

## How to configure IAM on Quantum ANZ Secure Cloud to access only to a specific bucket using S3 Browser (GUI)?

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use AWS resources.

This document explains how to use S3 Browser to configure IAM settings, granting access only to a specific bucket on your Quantum ANZ Secure Cloud.

**Note: It is your responsibility to keep all the credentials secure for accessing your S3 account and the IAM user's account.**

### ➤ Install latest version of S3 Browser on Windows:

Follow the instructions on the following link to install the latest version of the S3 Browser.

[Download S3 Browser. Amazon S3 Client. Windows Client for Amazon S3.](#)

This document uses **S3 Browser Version 12.9.9**

### ➤ Custom IAM Endpoints:

Follow this link to setup Custom IAM Endpoint for your Root S3 Account.

<https://s3browser.com/s3-compatible-storage.aspx#custom-iam-endpoints>

### Custom IAM Endpoints

Please use the **REST Endpoint** field to specify the IAM endpoint.

Quantum ANZ Secure Cloud IAM Endpoint URL is **iam.quantum-anz.online**

The **;;** symbols must be used as separator.

For example : **s3-mel.quantum-anz.online;;iam.quantum-anz.online**



Display name:

Assign any name to your account.

### S3 Compatible Storage

Choose the storage you want to work with. Default is Amazon S3 Storage.

s3-mel.quantum-anz.online;;iam.quantum-anz.online

S3-compatible API endpoint, which can be found in the storage documentation. Example: s3.storage.com

[Download PDF of the book](#)

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

[illegible]

Turn this option on if you want to protect your Access Keys with a master password.

If checked, all communications with the storage will go through encrypted SSL/TLS channel

 Cancel

## ➤ Use IAM Manager

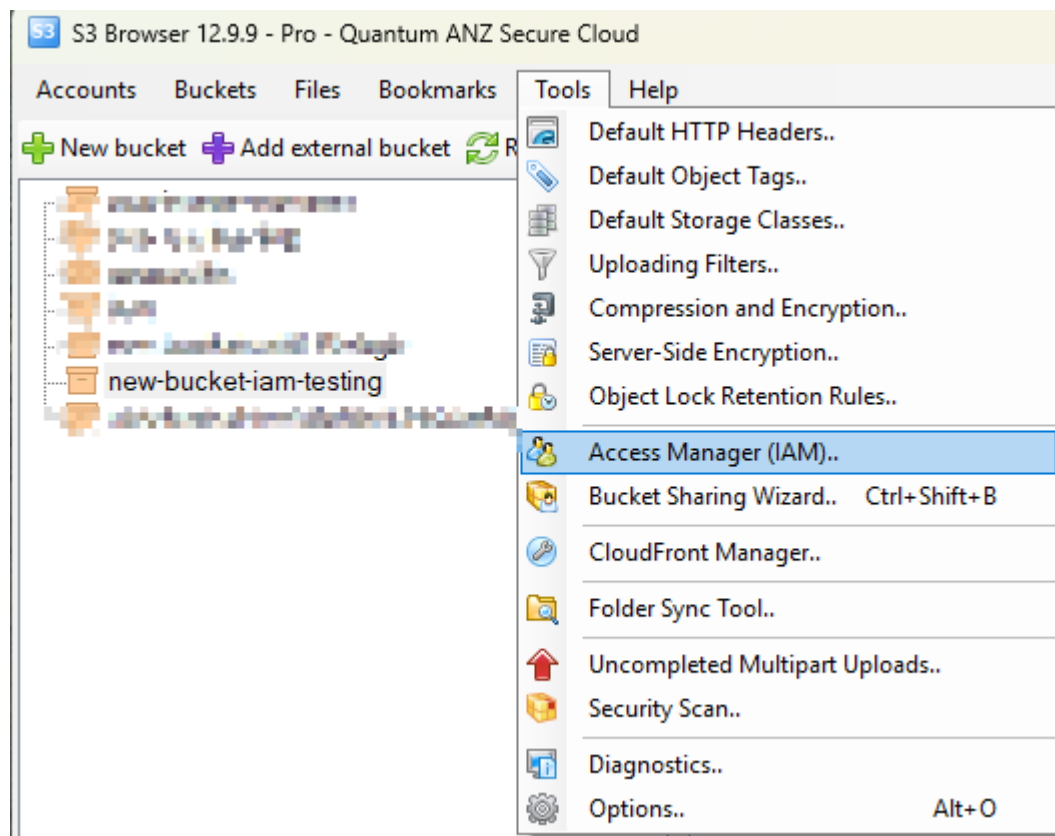
The below link is S3 Browser IAM user guide for your reference.

[Working with AWS Identity and Access Management \(IAM\). How to create IAM Users and Policies.](#)

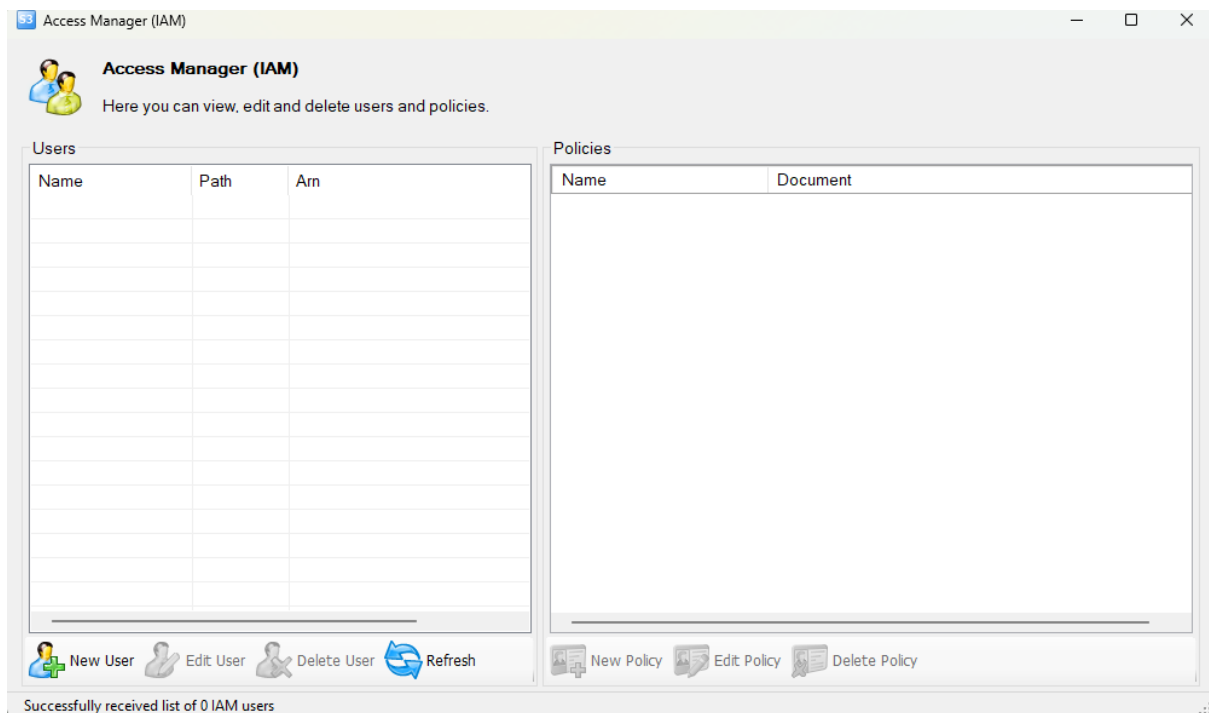
## The following steps are example using IAM with Quantum ANZ Secure Cloud

To Open IAM Manager

Click **Tools -> Access Manager (IAM)**



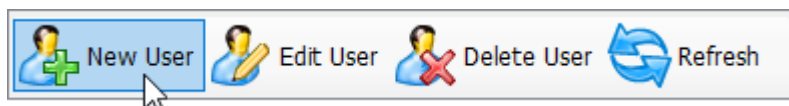
The **Access Manager (IAM)** dialog will open:



## Working with IAM Users - Create, Edit, Delete

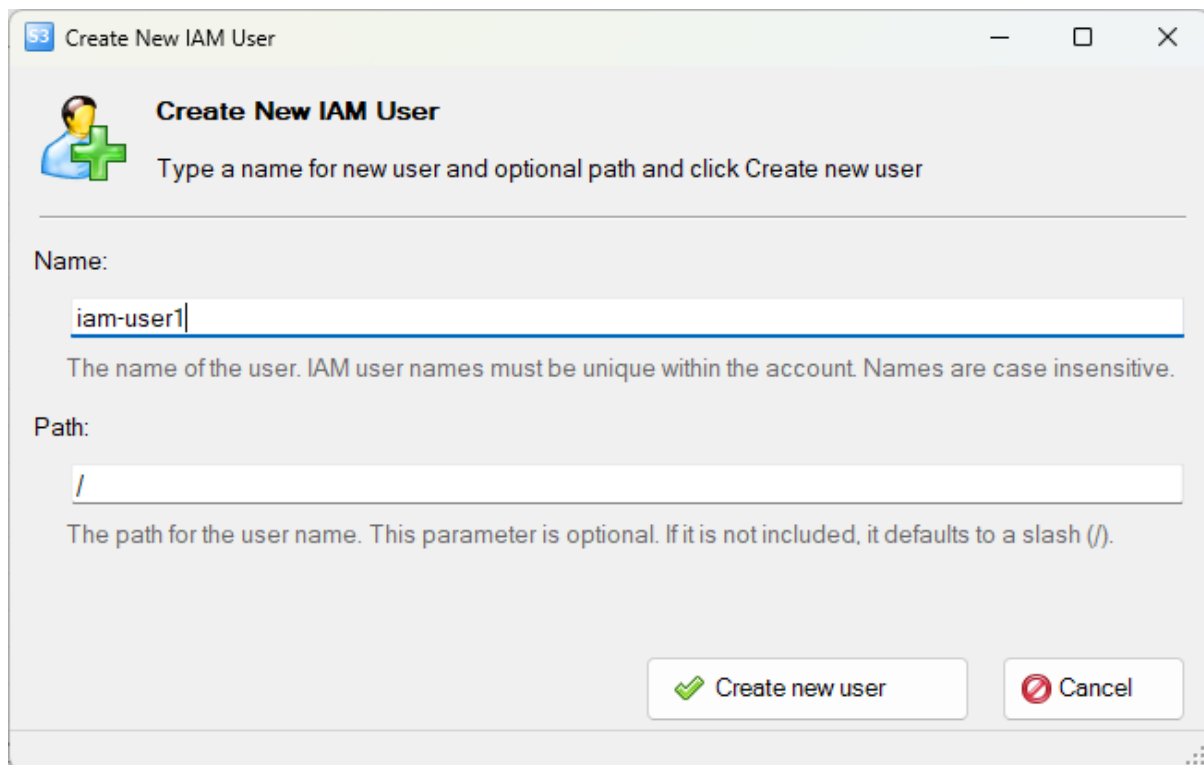
**To Create New IAM User:**

1. Click the **New User** button



**Click the New User button to add new IAM User**

The **Add New IAM User** dialog will open:



The screenshot shows a dialog box titled "Create New IAM User" with a user icon and a green plus sign. Below the title is the instruction: "Type a name for new user and optional path and click Create new user". There are two input fields: "Name:" with the text "iam-user1" and "Path:" with a single slash "/". Below each field is a descriptive note. At the bottom right are two buttons: "Create new user" (with a green checkmark icon) and "Cancel" (with a red circle and slash icon).

**Create New IAM User**

Type a name for new user and optional path and click Create new user

Name:

iam-user1

The name of the user. IAM user names must be unique within the account. Names are case insensitive.

Path:

/

The path for the user name. This parameter is optional. If it is not included, it defaults to a slash (/).

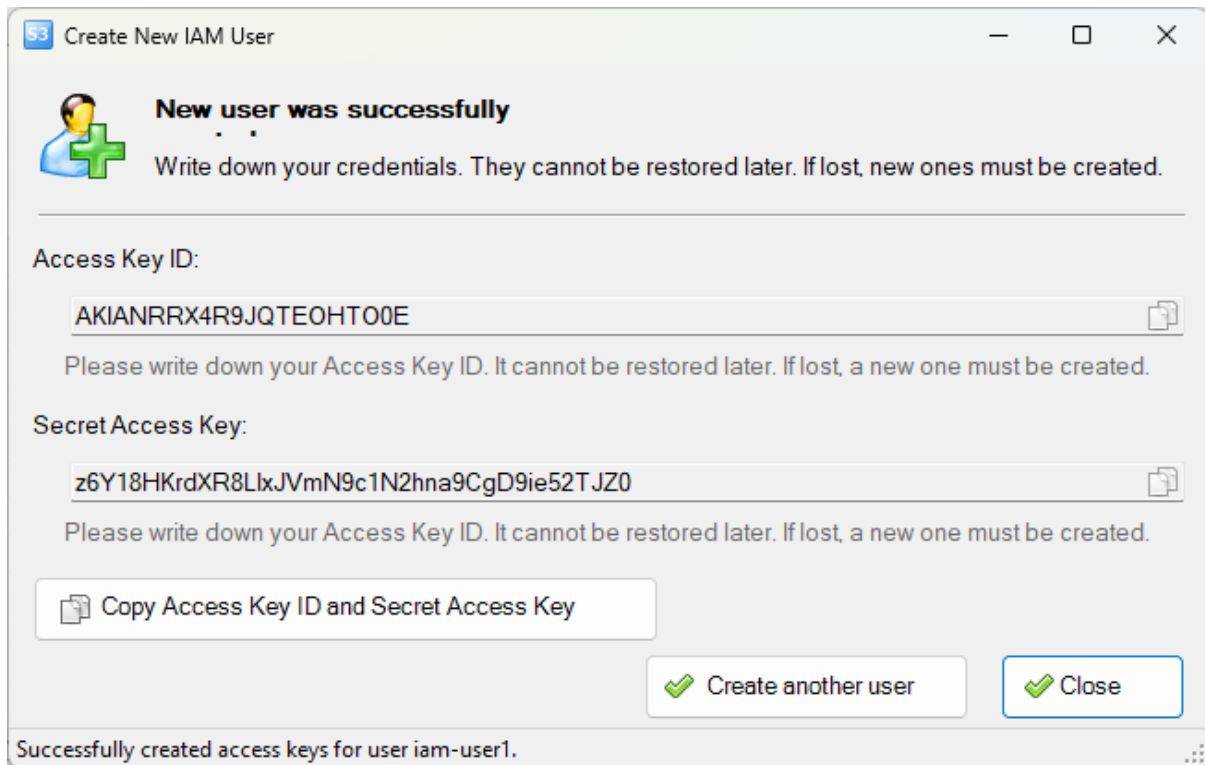
 Create new user  Cancel

### New IAM User dialog

2. Type a name of the user to create
3. Type a path for the new user (this field is optional)
4. Click **Create new user**

New IAM User will be created as well as Access Key ID and Secret Access Key.

The **New user created** page will open:



**New IAM User has been successfully created. Save Access Key ID and Secret Access Key.**

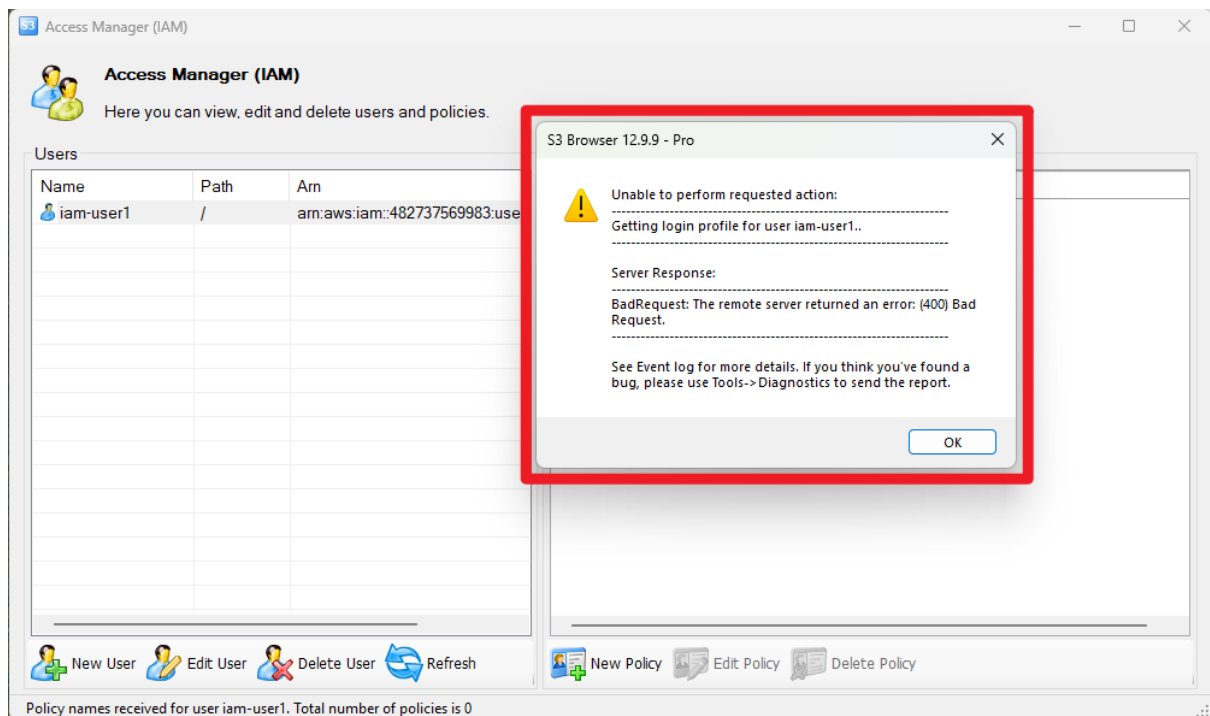
*Save Access Key ID and Secret Access Key. For security reasons there is no way to restore them later.*

Click **Copy Keys** to copy Access Key ID and Secret Access Key to clipboard.

Click **Create another user** if you would like to create more users and **Cancel** otherwise.

### **Special Note:**

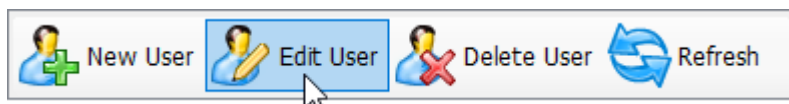
**Every time you click on the IAM users, S3 Browser will try to check the AWS Login Profile which is designed for AWS Management Console by default, and it is not compatible with Quantum ANZ Secure Cloud. So, it will pop-up this error message: (400) Bad Request.**



**Just click OK and ignore it. It will not affect using IAM function on your Quantum ANZ Secure Cloud services.**

### To Edit Existing IAM User:

1. Select the user to edit and click **Edit User**



**Click the Edit User button to edit existing IAM User**

The **Edit IAM User** dialog will open:

**Edit IAM User**

To edit existing user please update name or path and click Save changes

Name:

The name of the user. IAM user names must be unique within the account. Names are case insensitive.

Path:

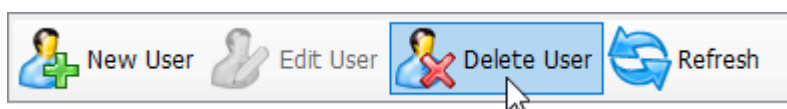
The path for the user name. This parameter is optional. If it is not included, it defaults to a slash (/).

### Edit IAM User Dialog

2. Type a new name for the user
3. Type a new path for the user (this field is optional)
4. Click **Save Changes**

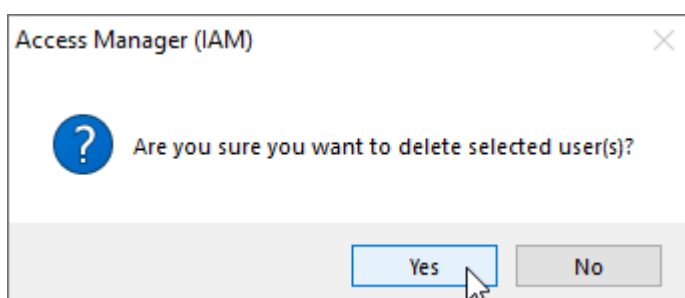
### To Delete IAM User(s):

1. Select user(s) you want to delete and click **Delete User(s)**



### Click the Delete User(s) button to delete IAM User(s)

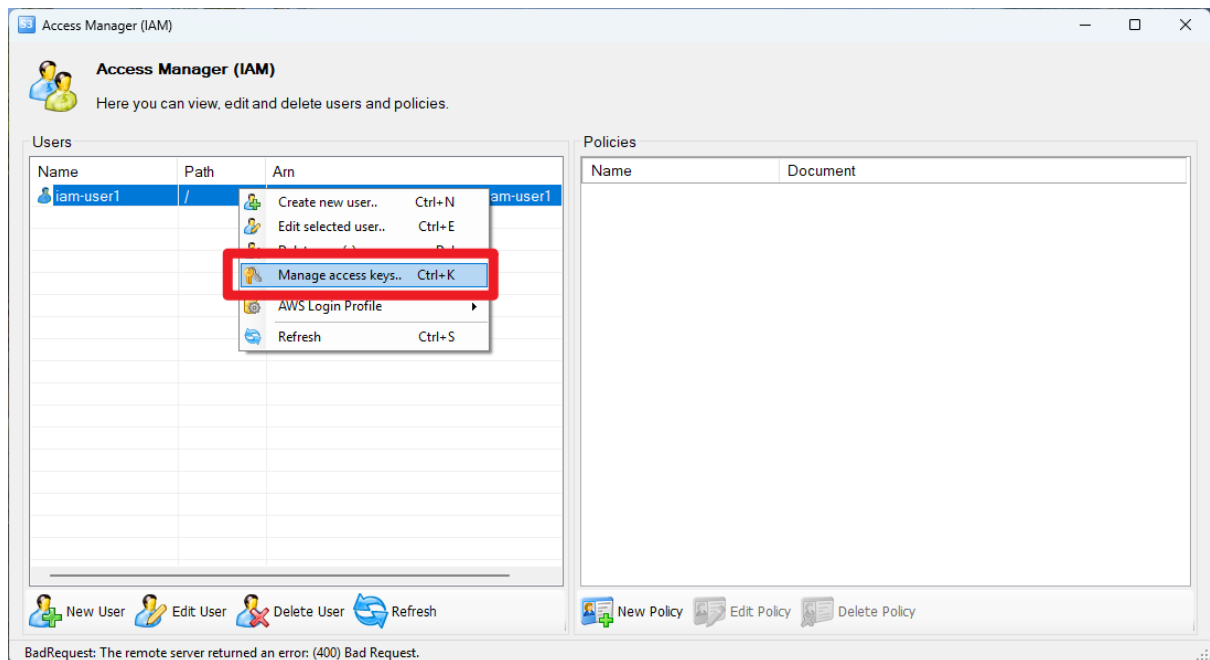
2. Confirm user(s) deletion



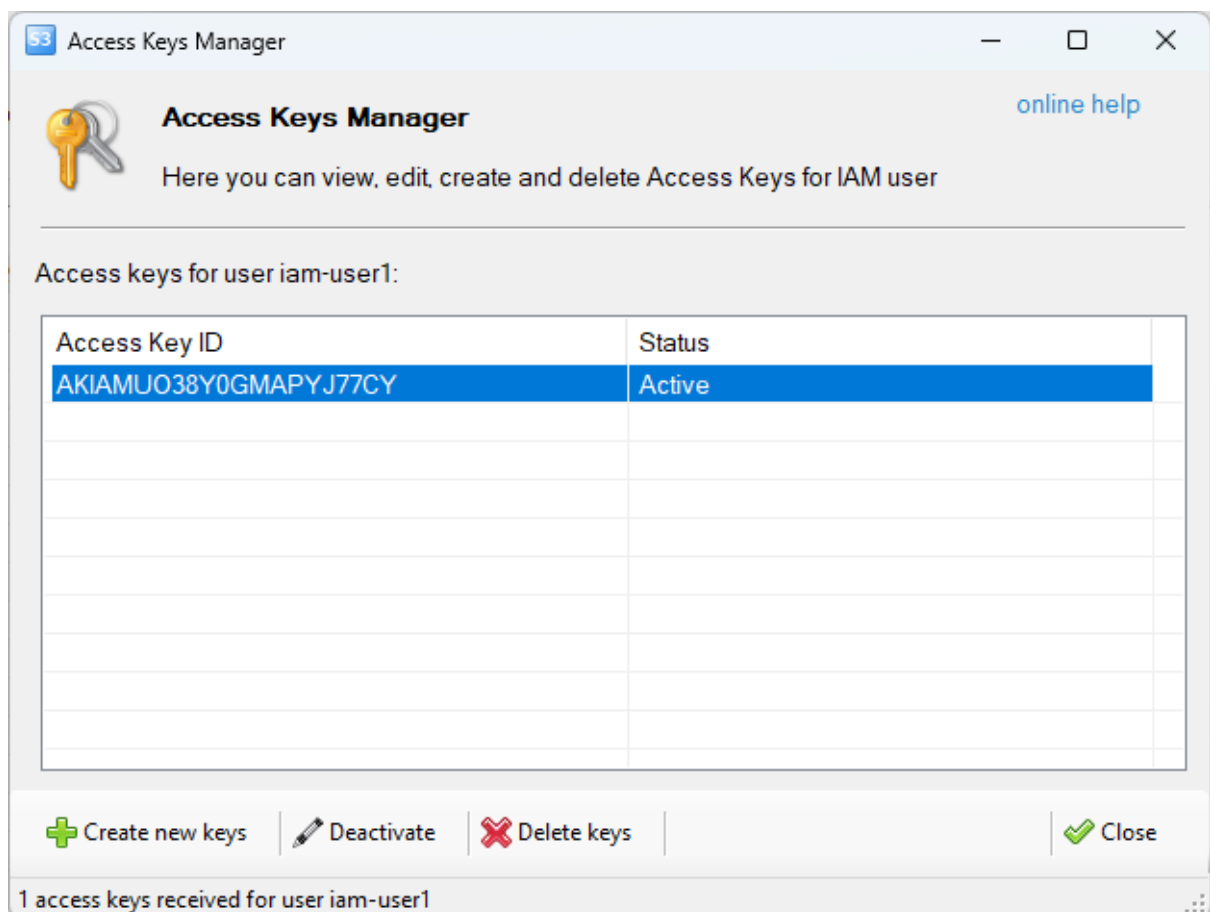
### Confirm IAM User(s) deletion

## Manage Access Keys for IAM User(s):

1. Right-click the IAM user you want to manage the access keys and click **Manage access keys**

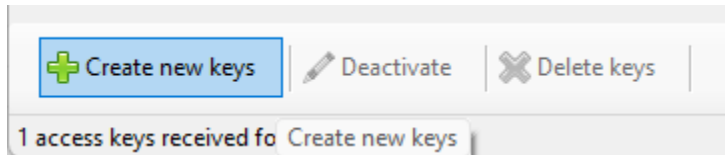


The **Access Keys Manager** dialog will open:



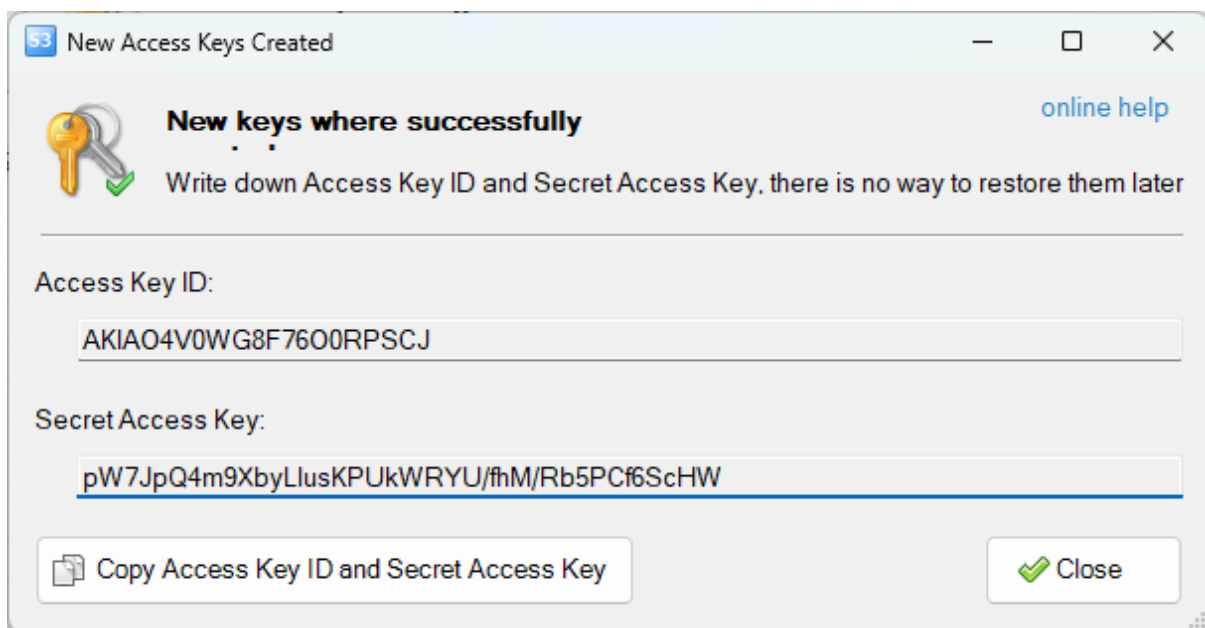
## To Create New Keys:

### 1. Click **Create new keys**



### Click the **Create new keys** button

The **New Access Keys Created** page will open:



**New keys were successfully created. Save Access Key ID and Secret Access Key.**

*Save Access Key ID and Secret Access Key. For security reasons there is no way to restore them later.*

Click **Copy Access Key ID and Secret Access Key** to copy Access Key ID and Secret Access Key to clipboard.

### 2. **Maximum 2 Access Keys can be created for one IAM user**

53

Access Keys Manager

— □ ×



**Access Keys Manager**[online help](#)

Here you can view, edit, create and delete Access Keys for IAM user

Access keys for user iam-user1:

| Access Key ID         | Status |
|-----------------------|--------|
| AKIAMUO38Y0GMAPYJ77CY | Active |
| AKIAO4V0WG8F76O0RPSCJ | Active |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |

Create new keys

Deactivate

Delete keys

Close

2 access keys received for user iam-user1

### To De-active Access Keys:

1. Select the Access Key you want to de-activate and click **Deactivate button**

53

Access Keys Manager

—

□

×



### Access Keys Manager

Here you can view, edit, create and delete Access Keys for IAM user

[online help](#)

Access keys for user iam-user1:

| Access Key ID         | Status |
|-----------------------|--------|
| AKIAMU038Y0GMAPYJ77CY | Active |
| AKIA2L3AWPYSPY6J14LT9 | Active |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |

Create new keys

Deactivate

Delete keys

Close

2 access keys received for user iam-u: Deactivate

2. The selected Access Key status will be **Inactive** now.

 Access Keys Manager

 **Access Keys Manager** [online help](#)

Here you can view, edit, create and delete Access Keys for IAM user

Access keys for user iam-user1:

| Access Key ID         | Status   |
|-----------------------|----------|
| AKIAMUO38Y0GMAPYJ77CY | Inactive |
| AKIAZL3AWP1SPT6574ET5 | Active   |
|                       |          |
|                       |          |
|                       |          |
|                       |          |
|                       |          |
|                       |          |
|                       |          |

 Create new keys |  Deactivate |  Delete keys |  Close

2 access keys received for user iam-user1

### To Activate Access Keys:

1. Select the Inactive Access Key you want to activate and click **Activate button**

 Access Keys Manager

 **Access Keys Manager** [online help](#)

Here you can view, edit, create and delete Access Keys for IAM user

Access keys for user iam-user1:

| Access Key ID         | Status   |
|-----------------------|----------|
| AKIAMU038Y0GMAPYJ77CY | Inactive |
| AKIA2L3AWPYSPY6J14LT9 | Active   |
|                       |          |
|                       |          |
|                       |          |
|                       |          |
|                       |          |
|                       |          |
|                       |          |
|                       |          |

 Create new keys  **Activate**  Delete keys  Close

2 access keys received for user iam-user1

2. The selected Access Key status will be **Active** again.

 Access Keys Manager

 **Access Keys Manager** [online help](#)

Here you can view, edit, create and delete Access Keys for IAM user

Access keys for user iam-user1:

| Access Key ID         | Status |
|-----------------------|--------|
| AKIAMUO38Y0GMAPYJ77CY | Active |
| AKIA2L3AWPYSPY6J14LT9 | Active |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |

 Create new keys |  Deactivate |  Delete keys |  Close

2 access keys received for user iam-user1

### To Delete Access Keys:

1. Select the Access Key you want to delete and click **Delete Keys button**

53

Access Keys Manager

—

□

×



**Access Keys Manager**[online help](#)

Here you can view, edit, create and delete Access Keys for IAM user

Access keys for user iam-user1:

| Access Key ID         | Status |
|-----------------------|--------|
| AKIAMUO38Y0GMAPYJ77CY | Active |
| AKIA2L3AWPYSPY6J14LT9 | Active |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |
|                       |        |

Create new keys

Deactivate

Delete keys

Close

2 access keys received for user iam-user1

Delete keys

## 2. Confirm key(s) deletion

Access Keys Manager

 Are you sure to delete selected key(s)?

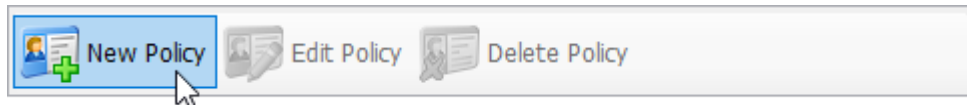
Yes

No

## Working with IAM Policies - Create, Edit, Delete

### To Add New IAM Policy:

1. Select the user and click the **New Policy** button



Click the **New Policy** button to add new IAM Policy for selected user

The **Add New Policy** dialog will open:



**New IAM Policy Dialog** allows you to specify iam policy name and policy document

2. Type a name of the new IAM Policy
3. Specify IAM Policy document
4. Click the **Add new policy** button

S3 Browser will add new IAM Policy for the selected user.

### Sample IAM Policy for access specific bucket:

**Policy name:** AccessBucket-@new-bucket-iam-testing

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBucketLevel",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::new-bucket-iam-testing"
      ]
    },
    {
      "Sid": "AllowObjectLevel",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource": [
        "arn:aws:s3:::new-bucket-iam-testing/*"
      ]
    }
  ]
}
```

```

    "Sid": "DenyAllOtherBuckets",
    "Effect": "Deny",
    "Action": "s3:*",
    "NotResource": [
        "arn:aws:s3:::new-bucket-iam-testing",
        "arn:aws:s3:::new-bucket-iam-testing/*"
    ]
}
]
}

```

This example IAM policy grants the user **full read/write access** to the bucket:

**new-bucket-iam-testing**

and **denies access to all other buckets** within the account.

### Key Capabilities Granted

- **List objects** in the bucket  
(s3:ListBucket)
- **Determine bucket location**  
(s3:GetBucketLocation)
- **Read, upload, overwrite, and delete objects**  
(s3:GetObject, s3:PutObject, s3:DeleteObject)
- **Perform multipart uploads**  
(s3:ListMultipartUploadParts, s3:AbortMultipartUpload)

### Isolation and Security Enforcement

The policy includes an explicit **Deny** rule that:

- Blocks **all S3 actions on any other bucket**
- Ensures the user cannot see or access buckets outside **new-bucket-iam-testing**, even if additional permissions are granted elsewhere

### Intended Use

This policy is designed for scenarios where a user must be **strictly restricted to a single S3 bucket**, ensuring strong isolation and preventing accidental or unauthorized access to other storage resources.

**Add New Policy**

Type a name for the new policy, enter policy document and click Add new policy

Policy name:

Policy document Policy Generator

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowBucketLevel",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": [
      "arn:aws:s3::new-bucket-iam-testing"
    ]
  },
  {
    "Sid": "AllowObjectLevel",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListMultipartUploadParts",
      "s3:AbortMultipartUpload"
    ],
    "Resource": [
      "arn:aws:s3::new-bucket-iam-testing/*"
    ]
  },
  {
    "Sid": "DenyAllOtherBuckets",
    "Effect": "Deny",
    "Action": "s3:*",
    "NotResource": [
      "arn:aws:s3::new-bucket-iam-testing",
      "arn:aws:s3::new-bucket-iam-testing/*"
    ]
  }
]
}
```

Copy and paste the sample policy to the IAM Policy document, make the necessary changes (Policy name and the bucket name in the policy) to suit your requirement.

Click the **Add new policy** button

**Access Manager (IAM)**  
Here you can view, edit and delete users and policies.

**Users**

| Name      | Path | Arn                                      |
|-----------|------|------------------------------------------|
| iam-user1 | /    | arn:aws:iam::123456789012:user/iam-user1 |

**Policies**

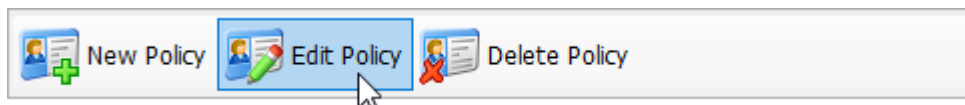
| Name                                 | Document                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AccessBucket-@new-bucket-iam-testing | <pre>{   "Version": "2012-10-17",   "Statement": [     {       "Sid": "AllowBucketLevel",       "Effect": "Allow",       "Action": [         "s3:ListBucket",         "s3:GetBucketLocation"       ],       "Resource": [         "arn:aws:s3:::new-bucket-iam-testing"       ]     },     {       "Sid": "AllowObjectLevel",       "Effect": "Allow",       "Action": [         "s3:GetObject",         "s3:PutObject",         "s3:DeleteObject",         "s3:ListMultipartUploadParts",         "s3:AbortMultipartUpload"       ],       "Resource": [         "arn:aws:s3:::new-bucket-iam-testing/*"       ]     },     {       "Sid": "DenyAllOtherBuckets",       "Effect": "Deny",       "Action": "s3:*",       "NotResource": [         "arn:aws:s3:::new-bucket-iam-testing",         "arn:aws:s3:::new-bucket-iam-testing/*"       ]     }   ] }</pre> |

New User Edit User Delete User Refresh New Policy Edit Policy Delete Policy

Successfully received policy AccessBucket-@new-bucket-iam-testing for user iam-user1

## To Edit Existing IAM Policy:

1. Select the user and policy you want to edit and click **Edit Policy**



Click the **Edit Policy** button to edit existing IAM Policy

The **Edit IAM Policy** dialog will open:

**Edit Policy**

Update policy document and click Save changes

Policy name:

new-policy-cb35428b

Policy document:

[Policy Generator](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadObjects",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::my-sample-bucket/*"
    }
  ]
}
```

Save changes Cancel

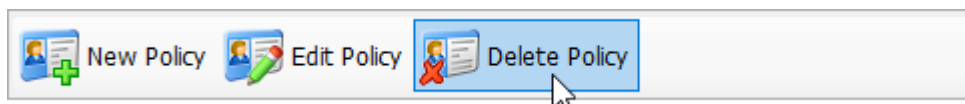
Successfully received policy new-policy-cb35428b for user new-user-cab69d86

### Edit IAM Policy Dialog

2. Make changes in the Policy Document and Click **Save Changes**

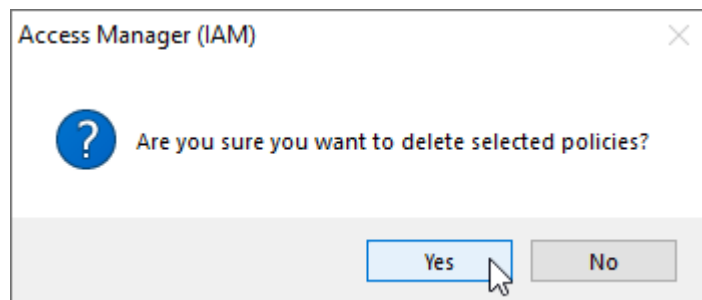
### To Delete IAM Policy:

1. Select the user and policy (or policies) you want to delete and click **Delete Policy**



**Click the Delete Policy button to delete IAM Policy or Policies.**

2. Confirm deletion:

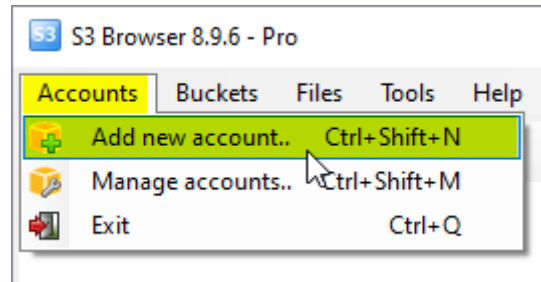


**Confirm IAM Policy deletion**

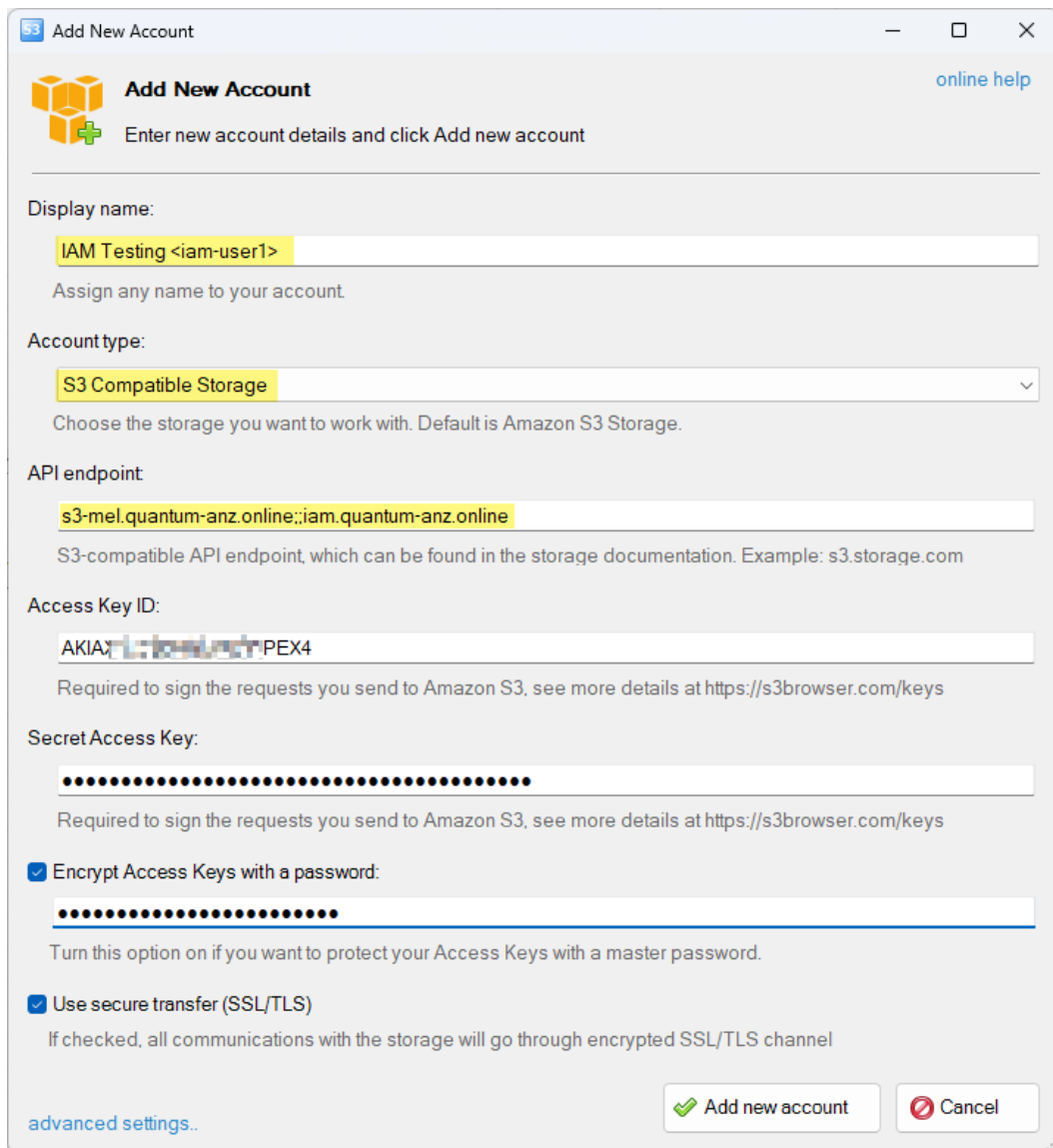
## ➤ Testing the IAM User “user1-iam” access in S3 Browser

**Note: Remember to use the Access Key ID and Secret Access Key during the step of Create New IAM User or Create Access Key**

1. Start S3 Browser and click **Accounts -> Add New Account**.



Click Accounts -> Add New Account



**Add New Account** [online help](#)

Enter new account details and click Add new account

Display name:  
  
Assign any name to your account

Account type:  
  
Choose the storage you want to work with. Default is Amazon S3 Storage.

API endpoint:  
  
S3-compatible API endpoint, which can be found in the storage documentation. Example: s3.storage.com

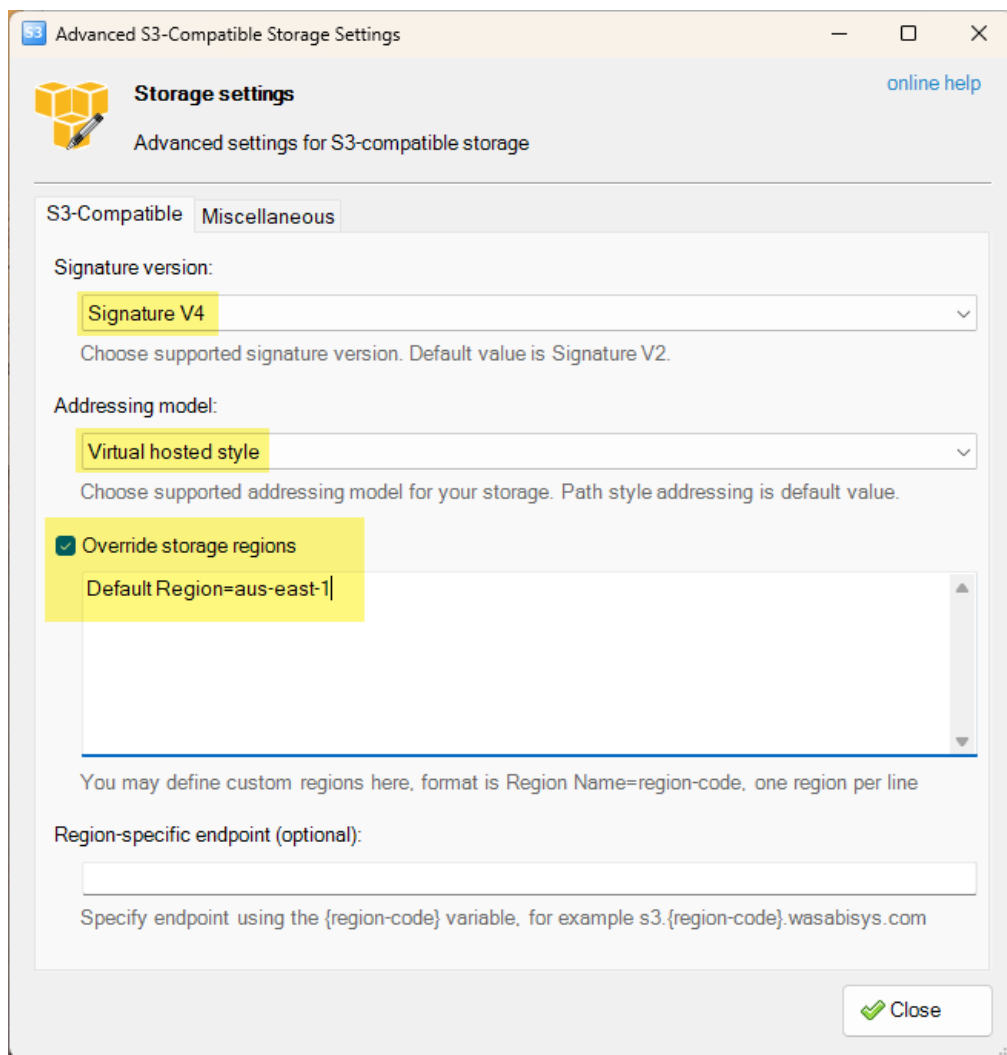
Access Key ID:  
  
Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

Secret Access Key:  
  
Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

☒ Encrypt Access Keys with a password:  
  
Turn this option on if you want to protect your Access Keys with a master password.

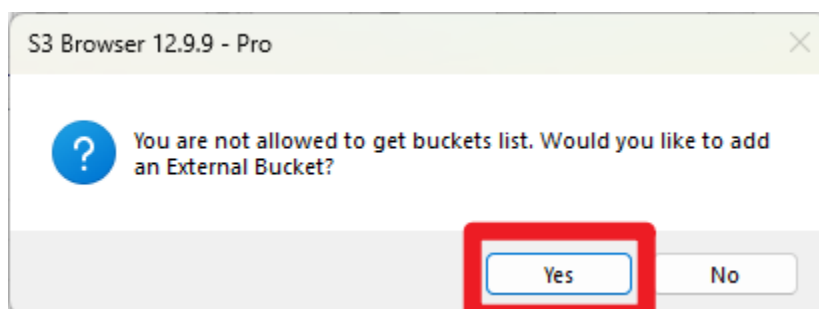
☒ Use secure transfer (SSL/TLS)  
If checked, all communications with the storage will go through encrypted SSL/TLS channel

[advanced settings..](#)



**Click Add new account button.**

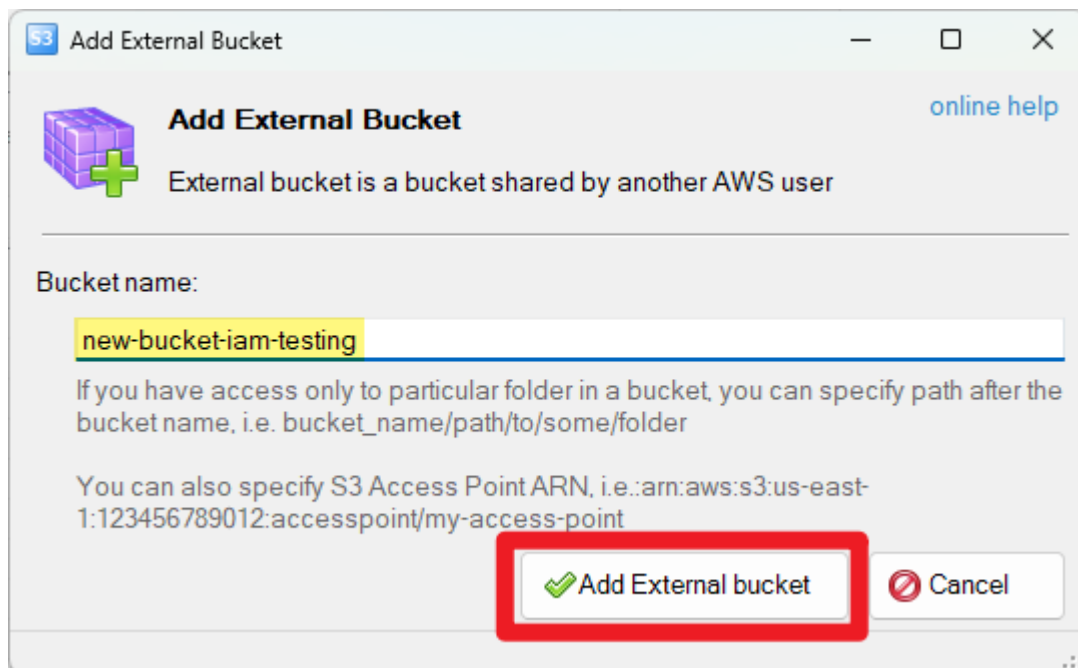
2. Select that account you just created in **Accounts**, you will see the pop-up window



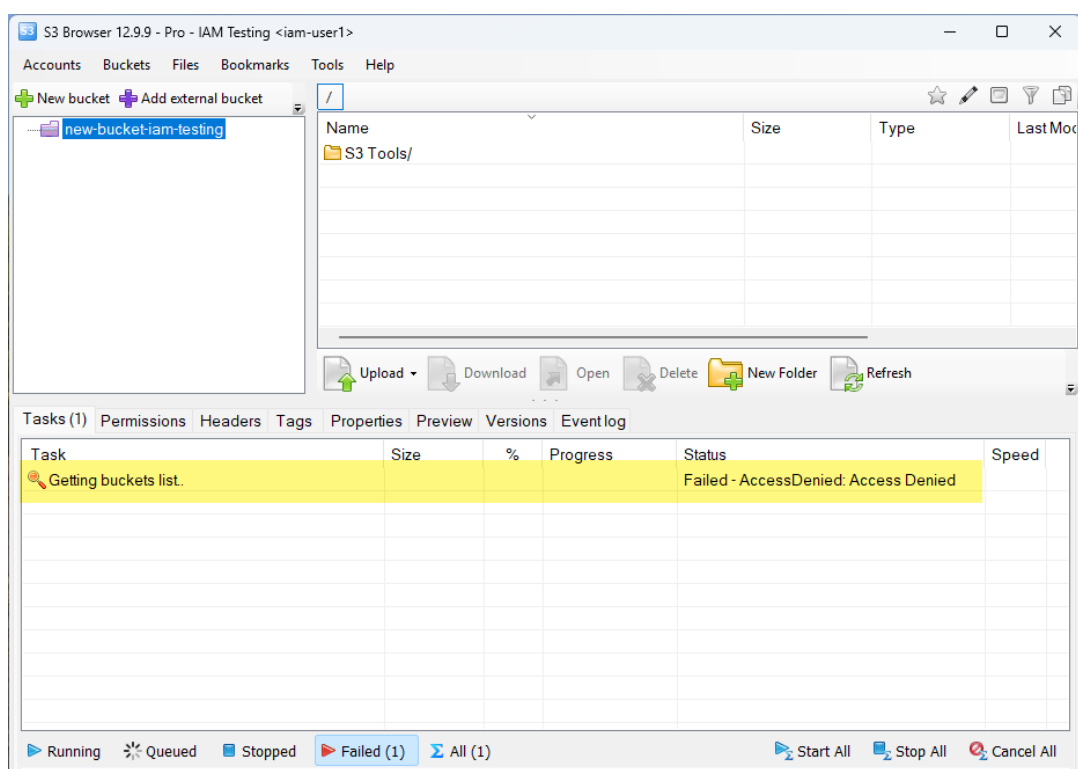
Because the policy limited this IAM user <iam-user1> just can access its own bucket *new-bucket-iam-testing*, and you are not allowed to get all the buckets list in the Root Account, so you need to add an External Bucket.

Click Yes button.

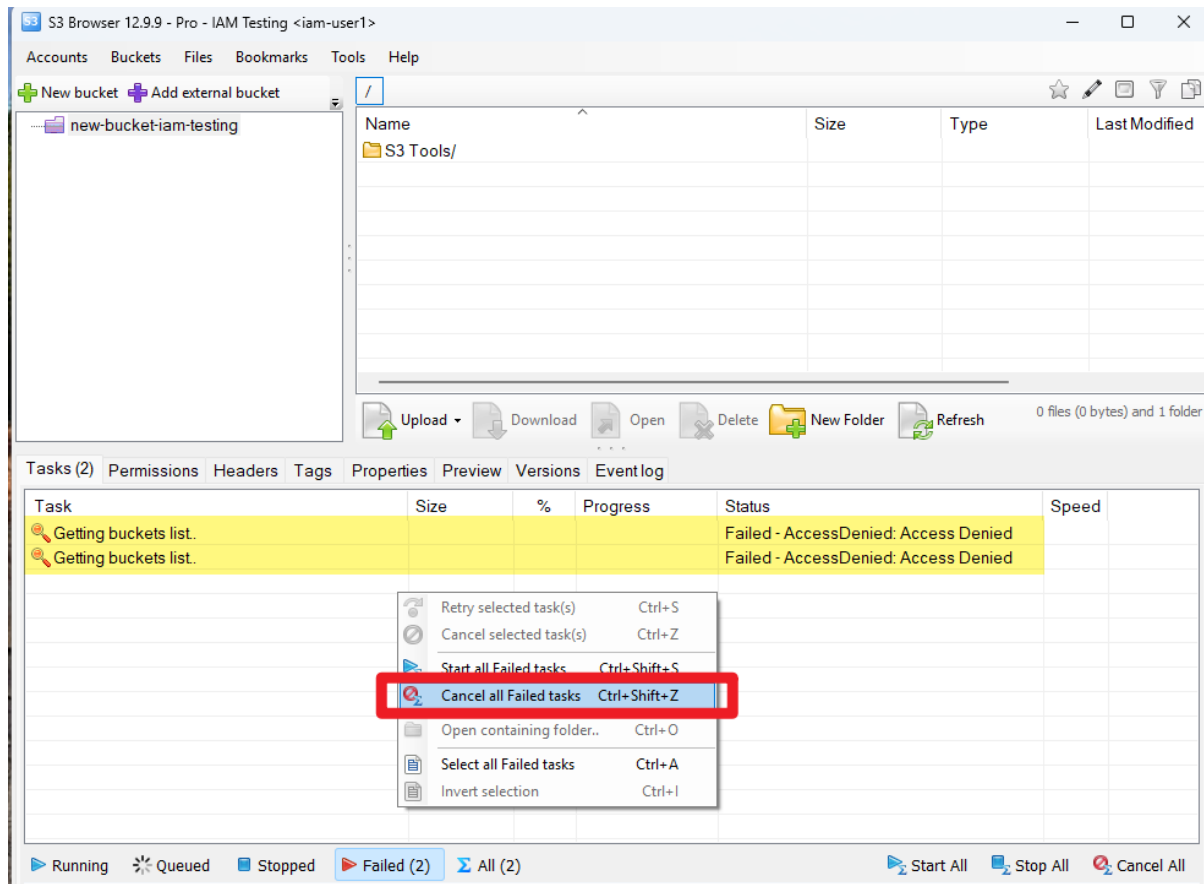
The **Add External Bucket** dialog will open:



Key in the bucket name *new-bucket-iam-testing* and click Add External bucket button.

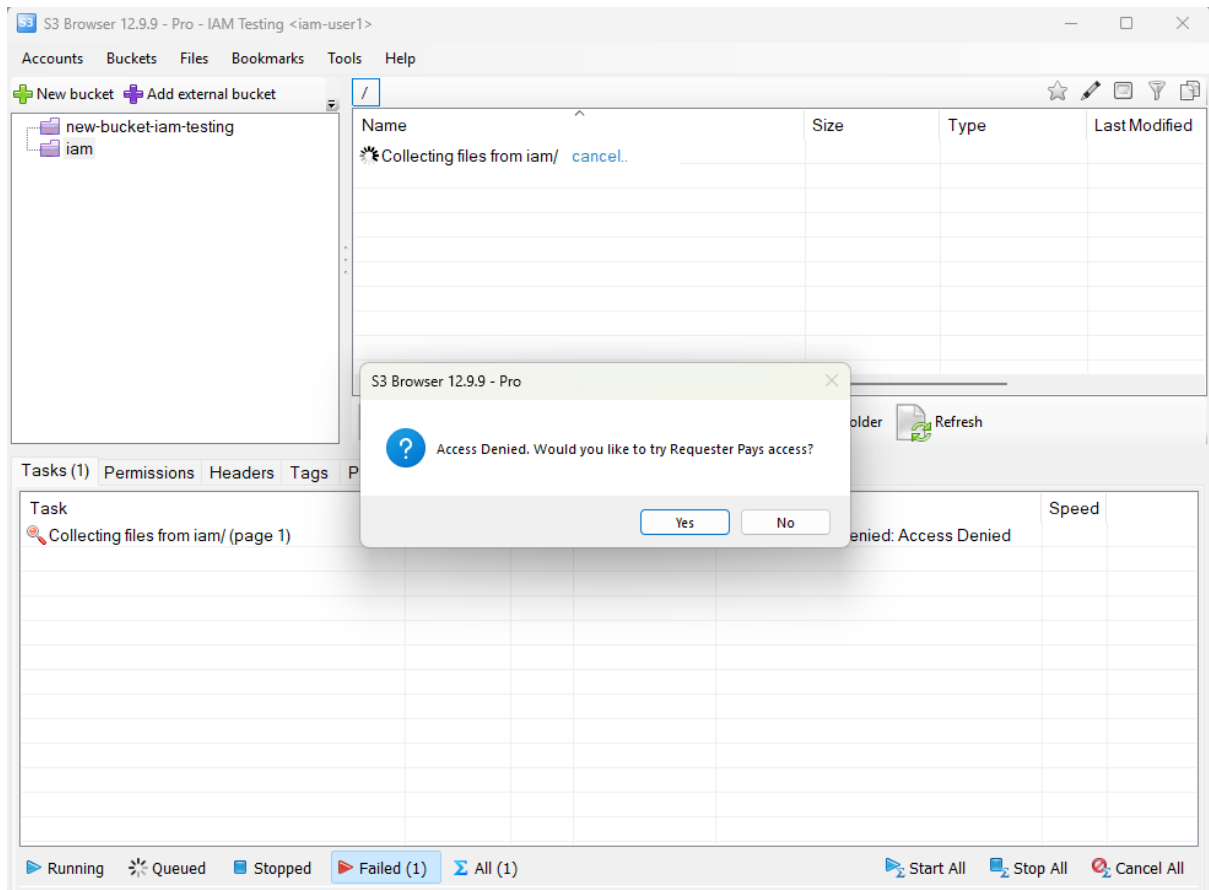


**Note: Because S3 Browser will try to get bucket list every time open the account, but this IAM user has not granted that permission. You will see many of the error message for Task: Getting bucket list Status Failed -Access Denied. Access Denied.**



**Just ignore those errors. Or right-click in the task window and cancel all failed tasks to clear them.**

**If you add other existing bucket in the root account, you will see Access Denied pop-up dialogue. The IAM policy don't give permission to access other bucket.**



**If click Yes, will see this pop-window with the Access Denied.**

