



HKEX Data Marketplace

Data Delivery Destination Configuration Guide – AWS S3

Version: 1.1

28 Apr 2025

@Copyright 2025 HKEX

All Rights Reserved

Document History

Version	Date of Issue	Comments
V1.0	18 Dec 2024	First distribution version
V 1.1	28 Apr 2025	<p>Section 2.1. AWS S3 bucket configuration under user's environment:</p> <p>Updated information on Access control lists (ACLs) and S3 Object Ownership Settings under AWS S3 Bucket Policy configuration.</p> <p>Added Section 2.1.2. AWS S3 default encryption</p>

DISCLAIMER

HKEX and/or its subsidiaries have endeavoured to ensure the accuracy and reliability of the information provided in this document, but do not guarantee its accuracy and reliability and accept no liability (whether in tort or contract or otherwise) for any loss or damage arising from any inaccuracy or omission or from any decision, action or non-action based on or in reliance upon information contained in this document.

Contents

1. Introduction	4
2. AWS S3 Delivery Location Configuration	4
2.1. AWS S3 bucket configuration under user's environment	4
2.1.1. AWS S3 Bucket Policy	4
2.1.2. AWS S3 default encryption	5
2.2. Delivery Destination setup for AWS S3 under Data Marketplace	6

1. Introduction

This document specifies the setup and configuration procedure for adding AWS S3 as a data product delivery destination in HKEX Data Marketplace.

The target audience of this document is the user admins who manage and operate the client's AWS S3 environment.

2. AWS S3 Delivery Location Configuration

To receive data files delivered to an AWS S3 bucket, configurations are required under both user's AWS S3 environment and HKEX Data Marketplace account settings.

2.1. AWS S3 bucket configuration under user's environment

2.1.1. AWS S3 Bucket Policy

User's AWS S3 bucket needs to be configured to allow HKEX Data Marketplace delivery service to write to the AWS S3 bucket; this is a one-off setup process.

Please run the following code snippet to apply the necessary permissions for the S3 bucket:

S3 bucket policy to be executed by Data Marketplace users:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDatahexS3Access",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::211125354333:role/venus-hkexprod-airflow-ec-
          AirflowTaskRoleWithUserSe-WHCZQtrzAmmC",
          "arn:aws:iam::211125354333:role/dhx-managed-s3-access-role-hkexprod"
        ]
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "<client-bucket-arn>/*",
        "<client-bucket-arn>"
      ]
    }
  ]
}
```

Please refer to [Adding a bucket policy by using the Amazon S3 console](#) under [AWS Documentation](#) for additional information.

Please note the following regarding setting up the S3 bucket policy:

1. **Action:** HKEX Data Marketplace will require `GetBucketLocation`, `PutObject` and `ListBucket` permissions as a minimum.
2. **Resource:** the Resource "`<client-bucket-arn>/*`" can also be limited to a sub-path if required, for example "Resource": ["`arn:aws:s3:::Bucket-name/Sub-path/*`"]
3. **Access control lists (ACLs) and S3 Object Ownership Settings:** as per AWS recommended best practices, Data Marketplace requires the bucket-level **Object Ownership** to be set to **ACLs disabled - Bucket owner enforced**.

To verify Object Ownership on an existing bucket using Amazon S3 console:

- 1) In the **Buckets** list, choose the name of the bucket selected as the data delivery destination.
- 2) Choose the **Permissions** tab.
- 3) Under **Object Ownership**, choose **Edit**.
- 4) Under **Object Ownership**, please ensure the following is selected:

ACLs disabled

- **Bucket owner enforced¹** – *ACLs are disabled, and the bucket owner automatically owns and has full control over every object in the bucket. ACLs no longer affect permissions to data in the S3 bucket. The bucket uses policies to define access control.*

Note: If ACLs is enabled, users will not be able to download the data files delivered with "Access Denied" error.

Please refer to [Setting Object Ownership on an existing bucket](#) under [AWS Documentation](#) for additional information.

2.1.2. AWS S3 default encryption

Data Marketplace can only support S3 buckets configured with server-side default encryption with **Amazon S3 managed keys (SSE-S3)**. Please note this is the automatic encryption applied by AWS.

To verify default encryption settings on a S3 bucket using Amazon S3 console:

- 1) In the left navigation pane, choose **Buckets**.
- 2) In the **Buckets** list, choose the name of the bucket.
- 3) Choose the **Properties** tab.
- 4) Under **Default encryption**, choose **Edit**.
- 5) Under **Encryption type**, please ensure the following is selected.
 - **Server-side encryption with Amazon S3 managed keys (SSE-S3)**

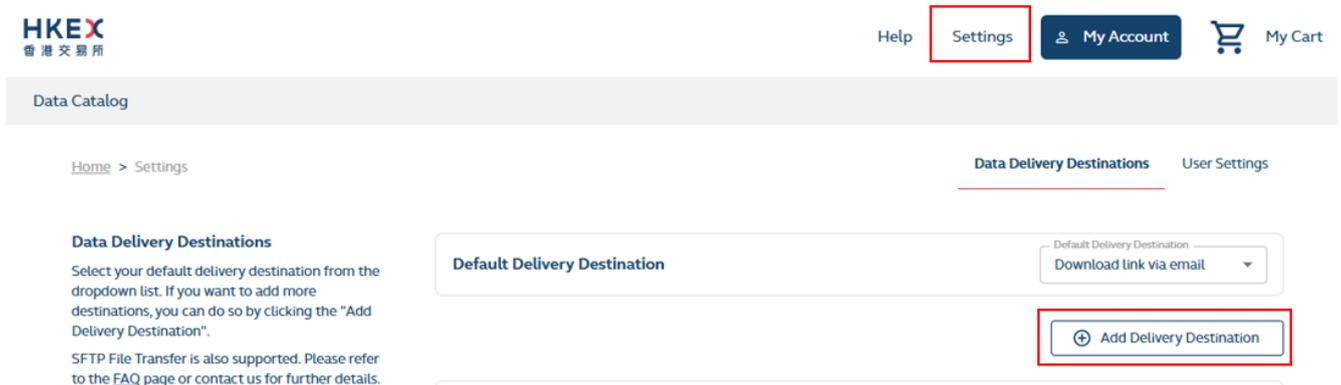
¹ Quoted from AWS documentation [Setting Object Ownership on an existing bucket](#).

Please refer to [Configuring default encryption](#) under [AWS Documentation](#) for additional information.

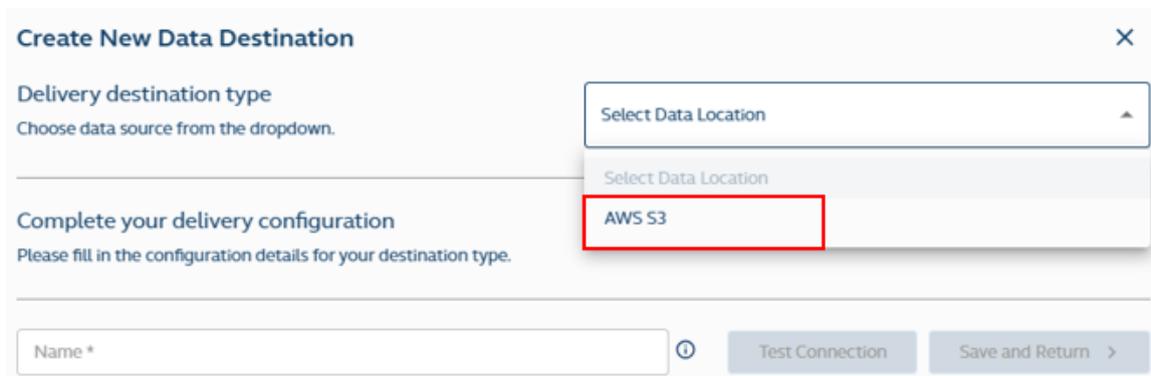
2.2. Delivery Destination setup for AWS S3 under Data Marketplace

Create a new data product delivery destination via the **Settings** tab in Data Marketplace platform:

1. After signing in, click **Settings** in the right top menu.
2. Under **Data Delivery Destinations** tab, click the **Add Delivery Destination** button.



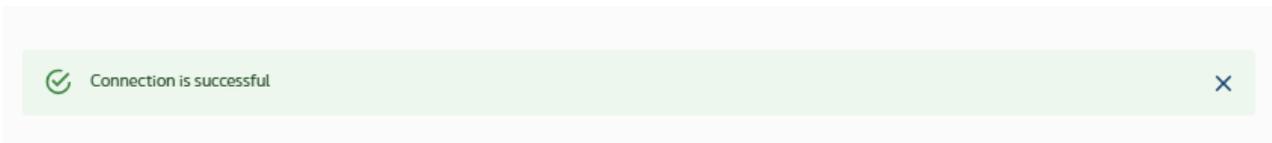
3. Under the **Create New Data Destination** pop-up window, select **AWS S3** from the dropdown list of **Delivery destination type**



4. Enter the additional information in the **Create New Data Destination** screen:
 - 1) **Bucket:** name of the target AWS S3 storage bucket (destination where the files will be delivered).
 - 2) **Prefix:** optional storage sub-path (subfolder name within the bucket for organising your data files). Please ensure to allow this sub-path under bucket policy **Resource** section if applied. Please refer to [2.1.1. AWS S3 Bucket Policy](#) – 2. Resource for details.
 - 3) **Region:** AWS region where the bucket is located (select from the drop-down list)
 - 4) **Name:** name of this delivery destination configuration (for your reference)

5. Test the connection by clicking the **Test Connection** button.

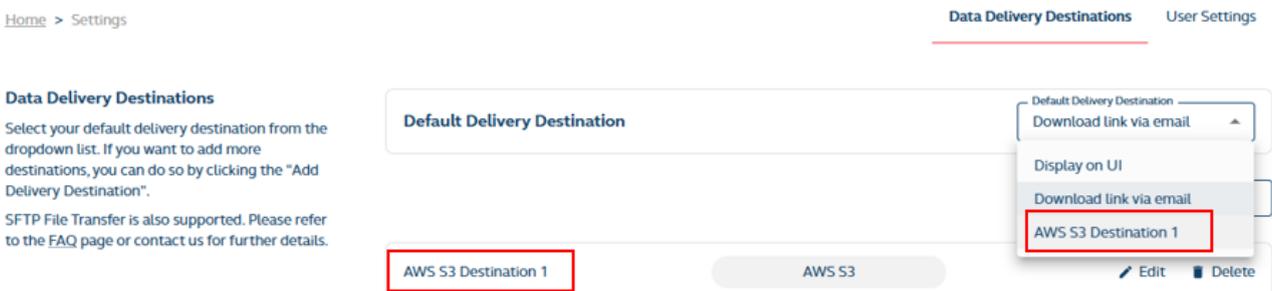
If the delivery configuration is valid - the bucket and prefix path (if applied) exist and has the required permissions, the platform will confirm the connection test was a success with a pop-up message "Connection is successful".



Otherwise, it will provide feedback on any errors encountered which need to be resolved before being able to establish connection.

The configuration can be saved by clicking the **Save and Return** button and will be displayed on the screen allowing user to Edit and Delete.

The list of saved delivery destinations will also appear in the **Default Delivery Destination** drop down list which can be selected as required.



Should you have any questions, please contact datamarketplace@hkex.com.hk for assistance.