The AWS S3 (Actions) destination enhances this capability by introducing configurable options to format and structure event data prior to storage. This new approach offers several key benefits:

- **Standardized Data Formatting**. AWS S3 (Actions) lets you define consistent output formats for your data, either CSV or TXT file formats, in a folder definition that you choose. The previous AWS S3 Classic Destination only allowed raw JSON payloads stored within a specific folder called `"segment-logs"`.
- **Configurable Data Translation**. AWS S3 (Actions) supports translation rules that can map raw event attributes to more meaningful or actionable representations. You can configure these rules to meet specific data schema requirements by either adding in custom columns or using the default ones.
- **Enhanced Delivery Controls**. The destination provides advanced options for batch size controls and file naming conventions. These controls can help optimize efficiency and simplify data retrieval workflows.

Supported Integrations

The AWS S3 (Actions) Destination supports the following Segment features as supported native Destination integration points:

- Reverse ETL
- Classic and Linked Audiences
- Connections

Getting started

Setting up the AWS S3 (Actions) destination is a straightforward process designed to help you configure and deploy standardized event data to your Amazon S3 bucket. Follow these steps to get started:

Prerequisites

Ensure you have the following in place before configuring the AWS S3 (Actions) destination:

- Amazon S3 Bucket: Create a bucket in your AWS account or use an existing one where you want to store the event data.
- AWS IAM Permissions: Verify that you have appropriate IAM roles with write access to the S3 bucket and permissions for the Segment connection.
- IAM Access IDs: Prepare your AWS IAM ARN ID and IAM External ID. These will be needed to authenticate and authorize Segment with your S3 bucket.

Step 1: Create an IAM role in the AWS console

To set up the IAM role to properly authorize Segment with the AWS S3 (Actions) destination:

1. Log in to your AWS account.
2. Create a new or use an existing bucket with `PutObject`, `GetObject`, `ListObject` access to the S3 bucket.
3. Navigate to **IAM > Roles > Create Role**.
4. Provide the following policy permissions for the IAM that was just created:

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Sid": "PutObjectsInBucket",
         "Effect": "Allow",
         "Action": [
             "s3:PutObject",
             "s3:PutObjectAcl"
         ],
         "Resource": "arn:aws:s3:::<YOUR_BUCKET_NAME>/*"
     }
 ]
}
```

5. Click on the Trust Relationships tab and edit the trust policy to allow the IAM user to assume the role. If a user is not already created, refer to the AWS documentation to create a user.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "AWS":
         "arn:aws:iam::595280932656:role/customer-s3-prod-action-destination-access"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "<YOUR_EXTERNAL_ID>"
      }
    }
  }
]
 }
```

Step 2: Add the AWS S3 (Actions) Destination in Segment

To finish the setup, enable the AWS S3 (Actions) Destination in your workspace:

1. Add the **AWS S3 (Actions)** destination from the Destinations tab of the catalog.
2. Select the data source you want to connect to the destination.
3. Provide a unique name for the destination.
4. Complete the destination settings:
   - Enter the name of the region in which the bucket you created above resides.
   - Enter the name of the bucket you created above. Be sure to enter the bucket's **name** and not URI.
   - Enter the ARN of the IAM role you created above. The ARN should follow the format `arn:aws:iam::ACCOUNT_ID:role/ROLE_NAME.`
   - Enter the IAM External ID, which is a value set in the Trust Relationship under your AWS IAM Role.
5. Enable the destination.

Available Actions

Build your own Mappings. Combine supported triggers with the following -supported actions:

> **Mapping limits per destination**
>
> Individual destination instances have support a maximum of 50 mappings.

Step 3: Configure the AWS S3 (Actions) Destination mappings

To finish the configuration, add mappings to your new AWS S3 (Actions) Destination:

1. Add a new **Sync to S3** Action into the destination.
2. Define the Event Trigger. If multiple types are accepted in the Event Trigger, the generated files will automatically be split by type in S3 (for example, you might have a Track events file and an Identify events file).
3. Configure the Column Mappings. If you don't need any of the default columns, leave the value blank. You can also choose to add new mapping fields to set up customized columns as needed.
4. Configure any additional settings as required.
5. Enable the Mapping.

6. Verify that Segment is sending data to your S3 bucket by navigating to `<your_S3_bucket>/` in the AWS console.

This page was last modified: 16 Dec 2024

Need support?

Questions? Problems? Need more info? Contact Segment Support for assistance!

Visit our Support page

Help improve these docs!

Edit this page

Request docs change

Was this page helpful?

Yes

No

Get started with Segment

Segment is the easiest way to integrate your websites & mobile apps data to over 300 analytics and growth tools.

Your work e-mail

Request Demo

or

Create free account