

**AMAZON CLOUDFRONT SETUP GUIDE**

**The Below requirements are needed to establish a connection amazon cloudfront.**

**Prerequisites**

Prerequisiteslink  
To connect Amazon CloudFront to Fivetran, you need:  
  
An S3 bucket containing files with supported file types and encodings  
An AWS account with the ability to grant Fivetran permission to read from the bucket

**Setup Guide**

1. Configure CloudFront logging

* If you haven't already, configure CloudFront to store its log files in an S3 bucket according to
* Amazon's instructions.

1. Find external ID

* In the connector setup form, find the automatically-generated External ID and make a note of it. You will need it to create an IAM role in AWS.
* NOTE: The automatically-generated External ID is tied to your account. If you close and re-open the setup form, the ID will remain the same. You may wish to keep the tab open in the background while you configure your source for convenience, but closing it is also OK.

1. Create an IAM Policy for Fivetran

* This step will allow Fivetran to access your S3 bucket.
* Open your Amazon IAM console.
* Go to Policies, then select Create Policy.
* Go to the JSON tab.
* Copy the following policy and paste it in the JSON tab, replacing {your-bucket-name} with the name of the S3 bucket where you store CloudFront logs.

|  |
| --- |
| { "Version": "2012-10-17", "Statement": [  {  "Effect": "Allow",  "Action": [ "s3:Get\*", "s3:List\*"  ],  "Resource": "arn:aws:s3:::{your-bucket-name}/\*"  },  {  "Effect": "Allow",  "Action": [ "s3:Get\*", "s3:List\*"  ],  "Resource": "arn:aws:s3:::{your-bucket-name}"  }  ] } |

* content\_copy
* Click Review Policy.
* Name the policy "Fivetran-CloudFront-Log-Access".
* Click Create Policy.

1. Create an IAM role for Fivetran

* Go to Roles, then select Create New Role.
* Select Another AWS Account, then enter Fivetran's account ID, 834469178297, in the Account ID field. Select the Require external ID checkbox.
* Enter the External ID you found in Step 2.
* Click Next: Permissions.
* Select the "Fivetran-CloudFront-Access" policy that you created in Step 3.
* Click Next: Tags, which is optional.
* Click Next: Review.
* Name your new role "Fivetran".
* Click Create Role.
* Select the Fivetran role you just created.
* Find the Role ARN and make a note of it. You will need it to configure Fivetran.

1. Permissions (Optional)

* You can specify permissions for the Role ARN that you designate for Fivetran. Giving selective permissions to this Role will allow Fivetran to only sync what it has permissions to see.

1. Finish Fivetran Configuration

* Enter your chosen destination schema name in the connector setup form.
* Enter your S3 bucket.
* Enter the Role ARN you found in Step 4.
* Enter your folder path.
* Click Save & Test. Fivetran will take it from here and sync your CloudFront data from your AWS S3 bucket.

