

## Manually Integrating AWS with Authomize - using *cross-account assumes a role*

This guide describes how to manually integrate Authomize, with *cross-account assumes a role*, (with your favorite tool).

Before proceeding make sure you have permission to create roles and assign policies to them.

### The process:

1. For each account that will be integrated, create a role with a trust policy for the Authomize user and attach the policies described below (in *Required Role Settings*).
2. Once the roles are installed on each account, go to the Authomize console and add the account numbers (of the accounts to be integrated).

### If you use the AWS Identity Center:

1. In the master account, add the following permission to the Authomize role:
  - a. AWSSSOReadOnly
  - b. AWSSSODirectoryReadOnly"
2. In the Authomize integration page, add the master account number to the list of accounts, and to the **Master Account** field

### Required Role Settings:

- **Role name:** AuthomizeCrossAccountTrustRole
- **Role policy:** aws:iam::aws:policy/SecurityAudit
- **Role trust policy:**
  - **Important:** the **ExternalID** should be copied from the Authomize AWS Integration dialog.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::291883359082:user/AuthomizeGlobalUser"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": {enter_unique_value}
        }
      }
    }
  ]
}
```

- If you are installing this role on the management account and wish to integrate AWS Identity Center as well, add the following policies to this role on top of the security audit policy:
  - `arn:aws:iam::aws:policy/AWSSSOReadOnly`
  - `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

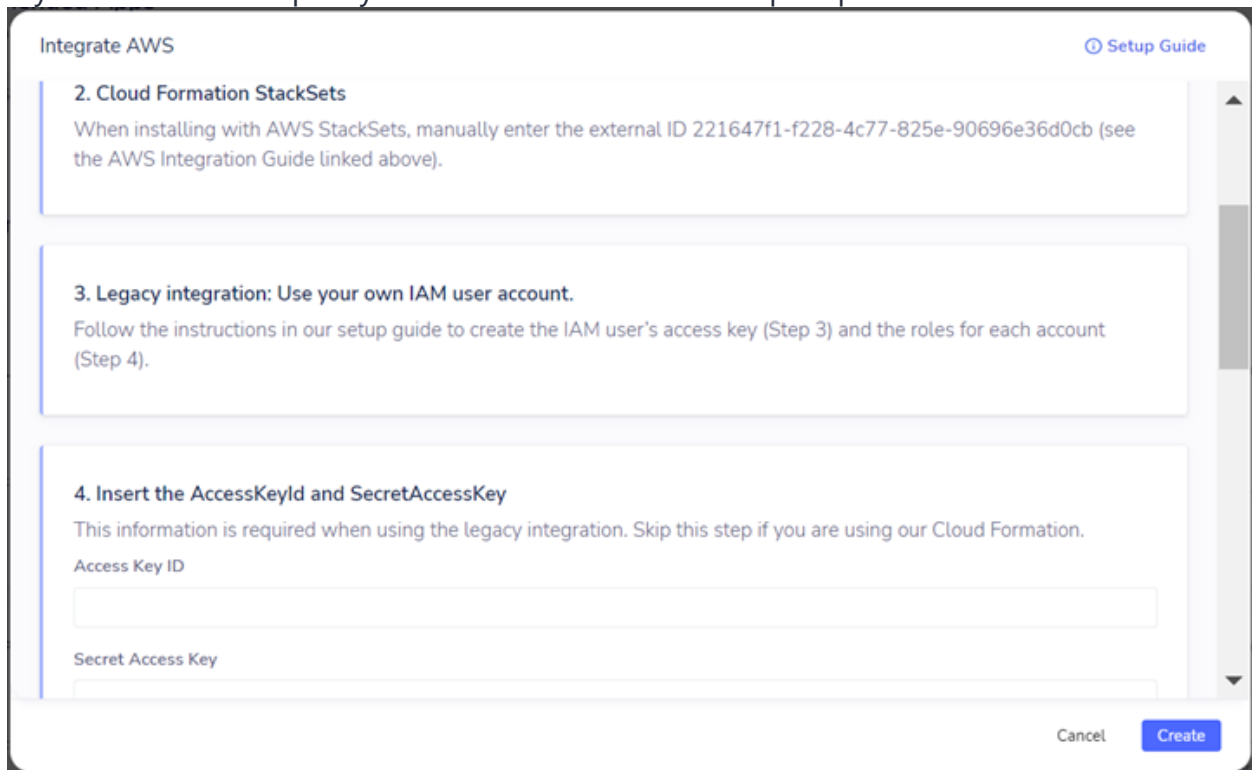
**Notes:**

1. If you update the role name, you must add the updated name in the integration dialog.
2. Do not change the trust policy principal.

## Complete the Integration

In the **Integrate AWS** dialog:

If you added a trust policy to the Authomize user – skip step 4



The screenshot shows the 'Integrate AWS' dialog box with a 'Setup Guide' link in the top right. It contains three main sections:

- 2. Cloud Formation StackSets**: When installing with AWS StackSets, manually enter the external ID 221647f1-f228-4c77-825e-90696e36d0cb (see the AWS Integration Guide linked above).
- 3. Legacy integration: Use your own IAM user account.**: Follow the instructions in our setup guide to create the IAM user's access key (Step 3) and the roles for each account (Step 4).
- 4. Insert the AccessKeyId and SecretAccessKey**: This information is required when using the legacy integration. Skip this step if you are using our Cloud Formation. It includes two input fields: 'Access Key ID' and 'Secret Access Key'.

At the bottom right, there are 'Cancel' and 'Create' buttons.

## Step 5:

- Insert the **Account Numbers** where this integration was installed
- Insert the **Management Account** number only if you want to integrate the AWS Identity Center.

This assumes:

- the role is installed on the management account
- the role includes AWS Identity Center permission.

If you insert a Management Account, that account number must be included (in comma-delimited format) in the **Account Number** field.

- Skip the **Assumed Role**, or enter a different name if you changed it.
- If you leave the **Regions** field empty, all regions (in your organization) will be included. If you specify one or more regions, data will be fetched only from those regions.

Integrate AWS [Setup Guide](#)

5. Insert the account IDs and relevant regions  
Visit our [setup guide](#) for more information

Account Numbers \*

577871520748

Management (master) Account Number (Optional for AWS Identity Provider)

577871520748

Assume Role

Regions

us-east-1, us-east-2

Cancel Create

**Step 6.** Enter an Integration name.

**Step 7.** Enter Owner's email.

Integrate AWS Setup Guide

us-east-1, us-east-2

**6. Set an integration Name**  
 If set, the integration will get a unique name  
 Integration name  
 Authomize-AWS-Integration

**7. Pick Owner**  
 The App Owner is considered the resource owner access review campaigns and security incidents  
 Contact email \*  
 sam@cheers.com

Cancel Create

Click Create.

If all goes well, you will see this:

**All set!**  
 We are fetching and processing data. This may take a while. We'll let you know when we're done.

**Recommended Apps**  
 Authomize has identified these apps in your organization

Dropbox + Ping Identity +

**My Connected Apps**  
 You have 31 connected apps

Search

<p><b>Authomize</b></p> <p>Status: Error</p> <p>Last sync: -</p> <p>Owner: peleg@authomize.com</p> <p>Type: Built by Authomize</p>	<p><b>AWS</b></p> <p>Status: Fetching</p> <p>Last sync: -</p> <p>Owner: sam@cheers.com</p> <p>Type: Built by Authomize</p>	<p><b>AWS SSO</b></p> <p>Status: Fetching</p> <p>Last sync: -</p> <p>Owner: sam@cheers.com</p> <p>Type: Built by Authomize</p>
--	--	--

Notice that AWS and AWS SSO were added to your Connected Apps.