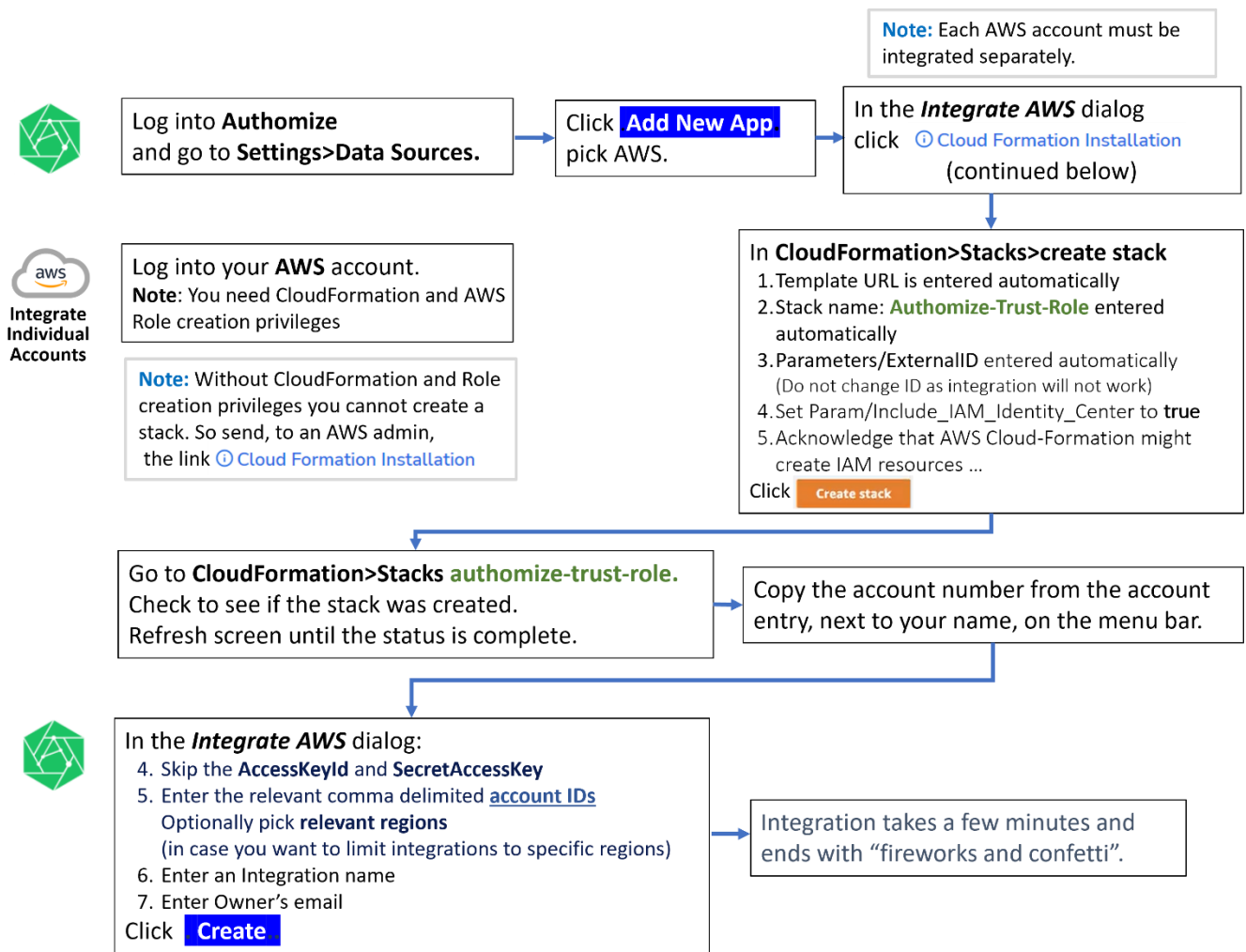


# AWS CloudFormation for individual accounts

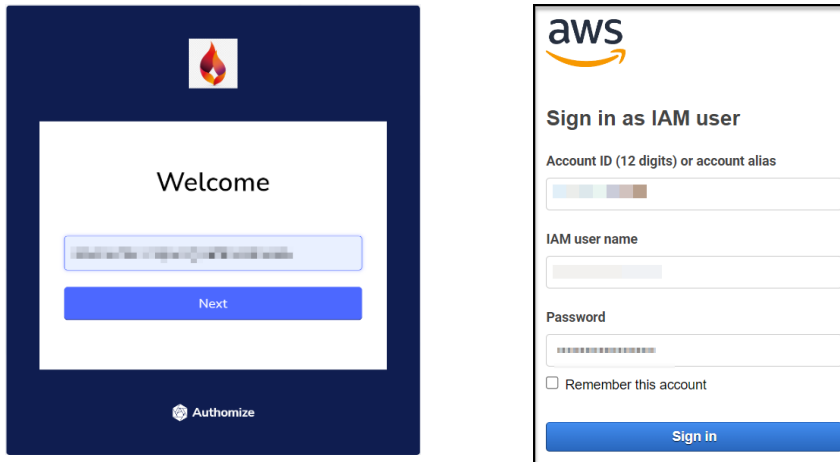
## Individual account integration workflow



**Note:** Only an AWS admin can create a role that can access connected Authomize accounts.

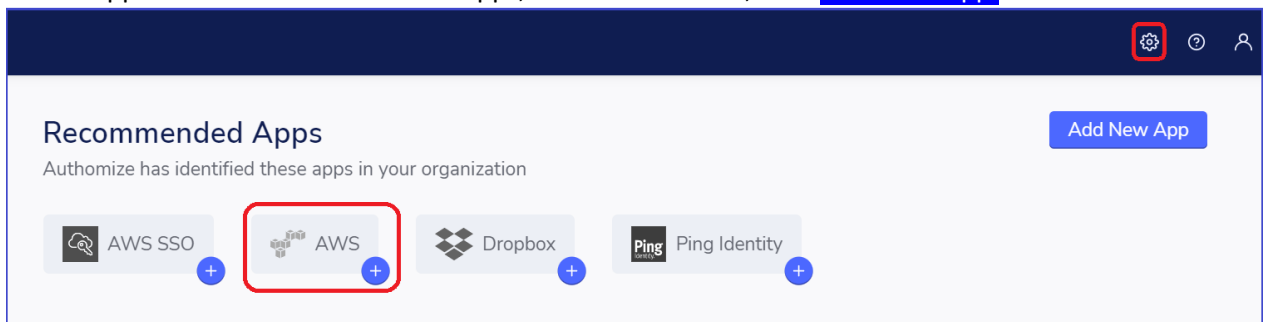
## Open both Authomize and AWS

- Log into **Authomize** and **AWS** in separate windows.
- In AWS you must have permissions to run CloudFormation and create new roles.

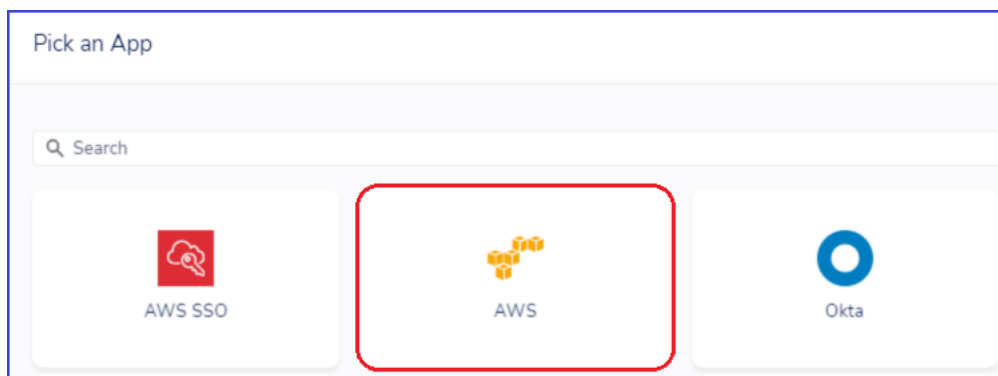


## Preparing the AWS Integration in Authomize

1. Go to **Settings > Data Sources**.
2. If AWS appears under Recommended Apps, click it. Otherwise, Click **Add New App**.



3. Select **AWS**.



**Note:** AWS IAM Identity Center (old AWS SSO) will be installed alongside AWS when the “*include SSO parameter*” is set in AWS.

- When the **Integrate AWS** dialog appears, click the [Cloud Formation Installation](#) button.  
If you do not have CloudFormation and Role creation privileges, send the link (along with a request to create an **Authomize-Trust-Role**) to your AWS admin.

**Note:** You can complete the **Integrate AWS** dialog after an **Authomize-Trust-Role** is available on AWS.

## Creating an Authomize-Trust-Role on AWS

Authomize communicates with AWS through an Authomize account (on AWS) with an **Authomize-Trust-Role**. Follow the steps below to create an account and an **Authomize-Trust-Role**.

- If you are already logged into AWS, the **CloudFormation>Stacks>Create stack** dialog will open in AWS after clicking on its link ([Cloud Formation Installation](#)).

CloudFormation > Stacks > Create stack

### Quick create stack

**Template**

Template URL  
https://authomize-cloud-formation.s3.amazonaws.com/authomize\_cloud\_formation.json

Stack description  
This stack is used to generate a cross account trust policy to integrate with Authomize. The stack generates a role with security audits permissions.

**Stack name**

Stack name  
Authomize-Trust-Role

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

ExternalId  
Your secret customer unique id - used internally by Authomize to connect you with our accounts - DO NOT CHANGE THIS  
a21416fe-c6cd-4617-a292-a701f6c2a213

IncludeAWSSSO  
Set to True to include AWS SSO integration  
true

**Capabilities**

**The following resource(s) require capabilities: [AWS::IAM::Role]**

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Cancel Create change set Create stack

Fill in the fields as follows:

**Template:**

- The Template URL is entered automatically. It is:  
`https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation.json`

**Stack name:**

- **Authomize-Trust-Role** entered automatically

**Parameters:**

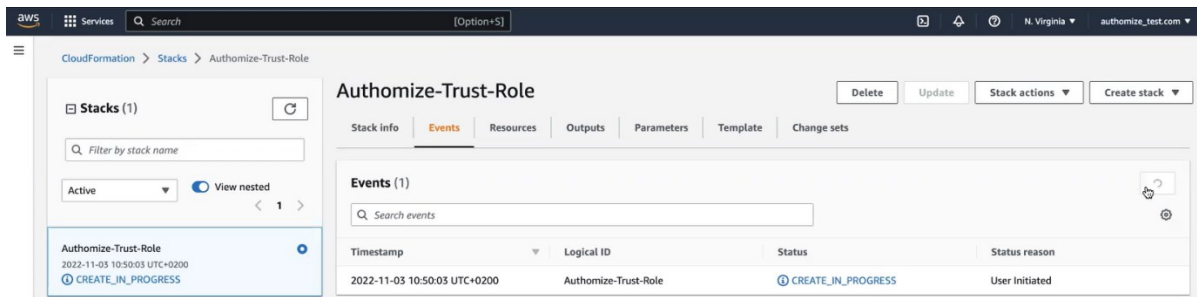
- **ExternalID** entered automatically  
(Do not change ID as the integration will not work)
- Set **IncludeAWSIdentityCenter** to **true** (so that AWS SSO will be integrated and installed alongside AWS).

**Capabilities:**

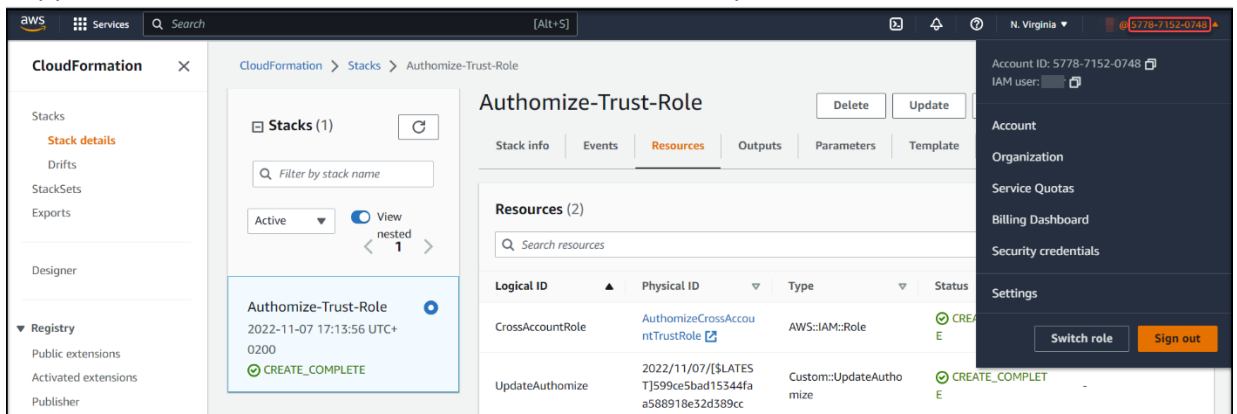
- Acknowledge that AWS Cloud-Formation might create IAM resources with custom names.

2. Click **Create stack**

3. In **CloudFormation/Stacks/Authomize-Trust-Role**, check to see if the stack creation was completed.



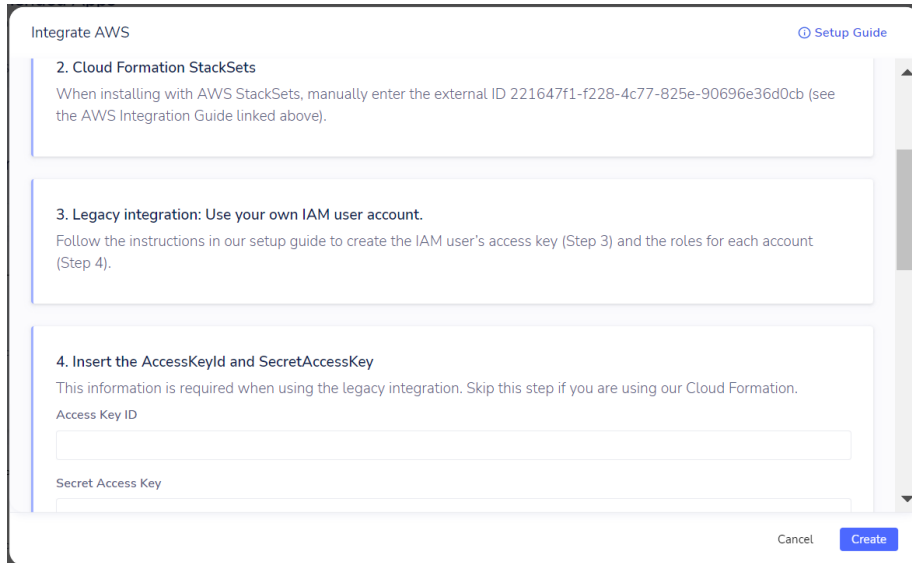
4. Copy the **Account** number from the account number next to your name on the Menu bar.



## Complete the Integration

In the *Integrate AWS* dialog:

- Skip step 4 if you used CloudFormation, otherwise insert the **AccessKeyId** and **SecretAccessKey** (for legacy integration).



The screenshot shows the 'Integrate AWS' dialog with three visible steps:

- 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.  
Access Key ID:   
Secret Access Key:

Buttons: Cancel, Create

- Insert the **Account Number**(copied from the **AWS** menu bar, as described above).

Insert the **Management Account** number only if you want to integrate the AWS Identity Center.

This assumes:

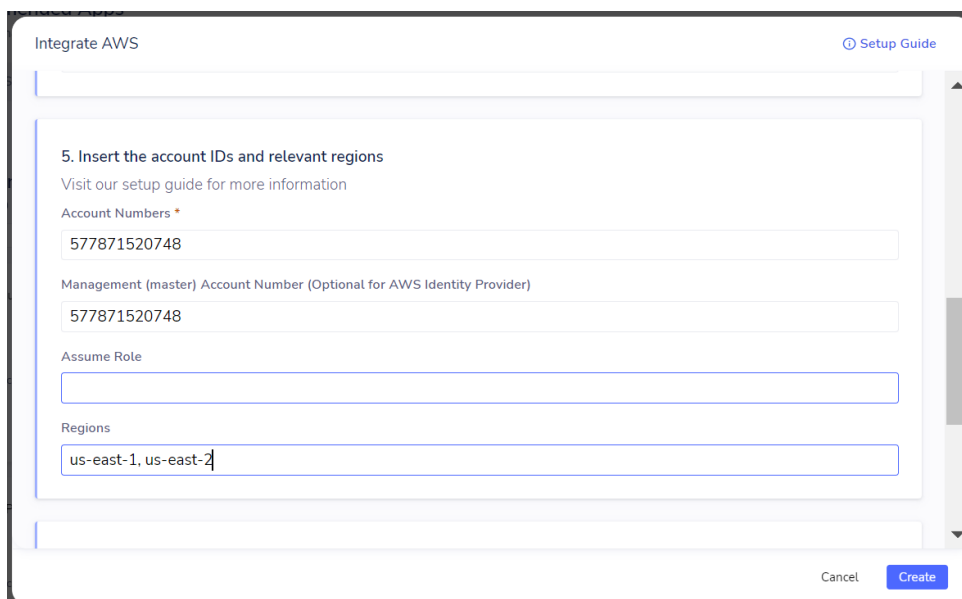
- the role is installed on the management account
- the role includes AWS Identity Center permission

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**.

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.



The screenshot shows the 'Integrate AWS' dialog with step 5:

- 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

Buttons: Cancel, Create

6. Enter an Integration name
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

App	Status	Last sync	Owner	Type
Authomize	Error	-	peleg@authomize.com	Built by Authomize
AWS	Fetching	-	ariel.zaretsky@authomize.com	Built by Authomize
AWS SSO	Fetching	-	ariel.zaretsky@authomize.com	Built by Authomize

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

# AWS IAM Identity Center

The AWS IAM Identity Center (previously known as AWS SSO) is an authentication solution that allows users to log in to multiple applications and websites with one-time user authentication.

- It is integrated with Authomize alongside AWS , when **IncludeAWSIdentityCenter** is set to **true** in the Specify StackSet Details page. It is only relevant if your organization uses *IAM Identity Center (AWS SSO)*
- If installed on an individual account, only mark as true in the management account.
- When checking this option Authomize requests two extra permissions:  
AWSSSOReadOnly,  
AWSSSODirectoryReadOnly
-