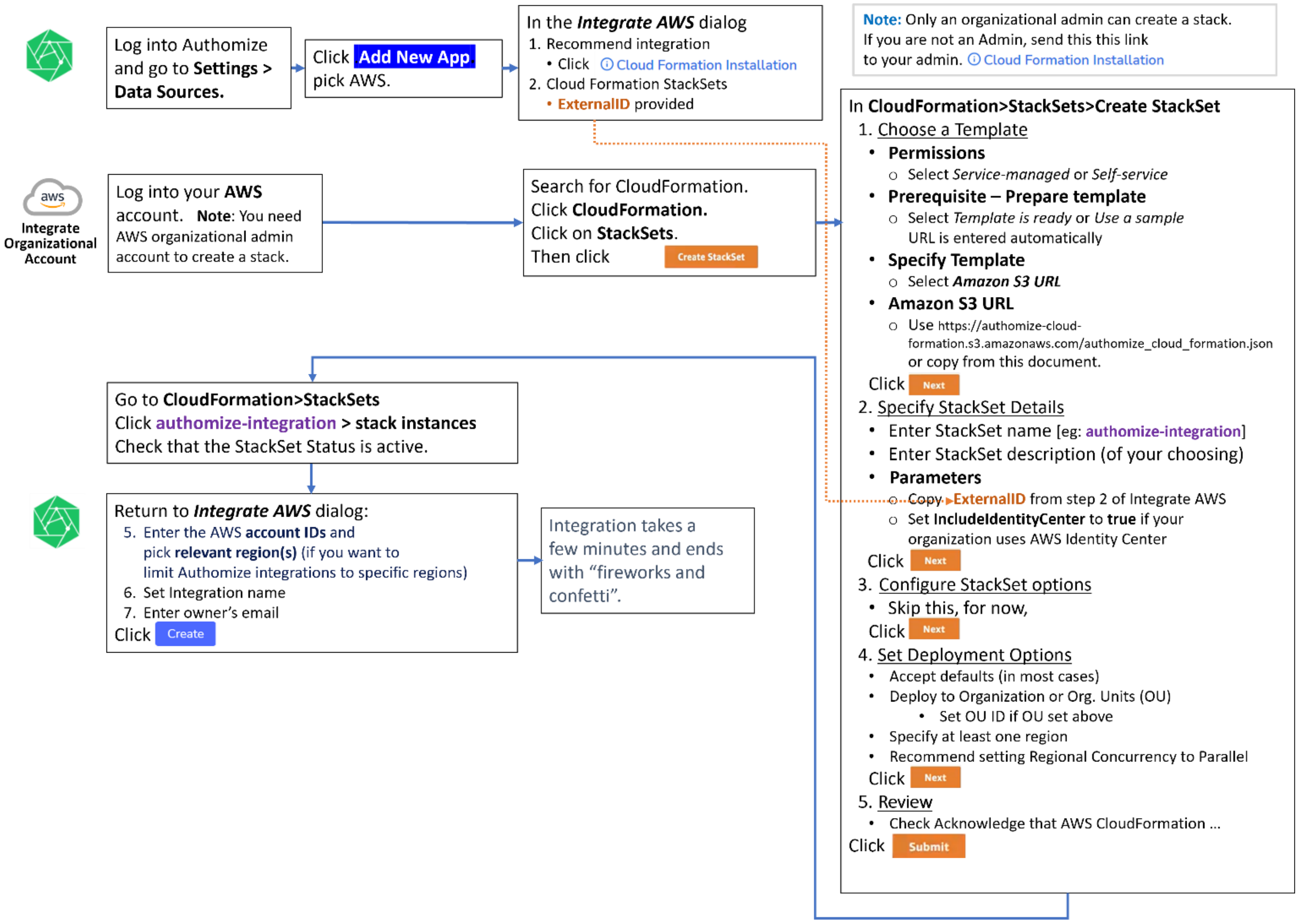
AWS CloudFormation for an organizational account

Organizational account integration workflow



Log into Authomize and go to **Settings > Data Sources.**

Click **Add New App** pick AWS.

In the ***Integrate AWS*** dialog
1. Recommend integration
   - Click ⓘ Cloud Formation Installation
2. Cloud Formation StackSets
   - **ExternalID** provided

Note: Only an organizational admin can create a stack. If you are not an Admin, send this this link to your admin. ⓘ Cloud Formation Installation

Integrate Organizational Account

Log into your **AWS** account. **Note:** You need AWS organizational admin account to create a stack.

Search for CloudFormation. Click **CloudFormation.** Click on **StackSets**. Then click Create StackSet

In **CloudFormation>StackSets>Create StackSet**
1. Choose a Template
   - **Permissions**
     - Select *Service-managed* or *Self-service*
   - **Prerequisite – Prepare template**
     - Select *Template is ready* or *Use a sample* URL is entered automatically
   - **Specify Template**
     - Select ***Amazon S3 URL***
   - **Amazon S3 URL**
     - Use https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation.json or copy from this document.

   Click Next
2. Specify StackSet Details
   - Enter StackSet name [eg: **authomize-integration**]
   - Enter StackSet description (of your choosing)
   - **Parameters**
     - Copy **ExternalID** from step 2 of Integrate AWS
     - Set **IncludeIdentityCenter** to **true** if your organization uses AWS Identity Center

   Click Next
3. Configure StackSet options
   - Skip this, for now,

   Click Next
4. Set Deployment Options
   - Accept defaults (in most cases)
   - Deploy to Organization or Org. Units (OU)
     - Set OU ID if OU set above
   - Specify at least one region
   - Recommend setting Regional Concurrency to Parallel

   Click Next
5. Review
   - Check Acknowledge that AWS CloudFormation …

Click Submit

Go to **CloudFormation>StackSets**
Click **authomize-integration > stack instances**
Check that the StackSet Status is active.

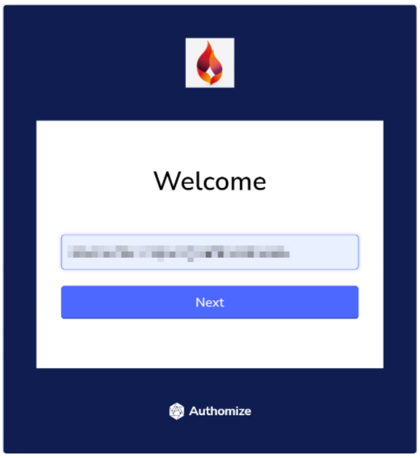
Return to ***Integrate AWS*** dialog:
5. Enter the AWS **account IDs** and pick **relevant region(s)** (if you want to limit Authomize integrations to specific regions)
6. Set Integration name
7. Enter owner's email

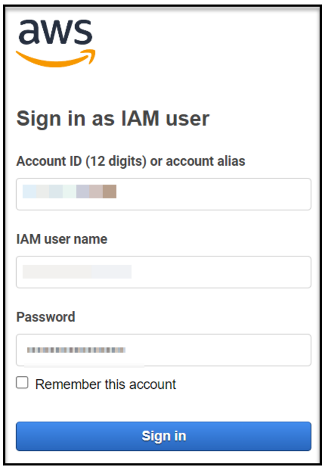
Click Create

Integration takes a few minutes and ends with "fireworks and confetti".

Open both Authomize and AWS

- Log into **Authomize** and **AWS** in separate windows.





Sign in as IAM user

Account ID (12 digits) or account alias

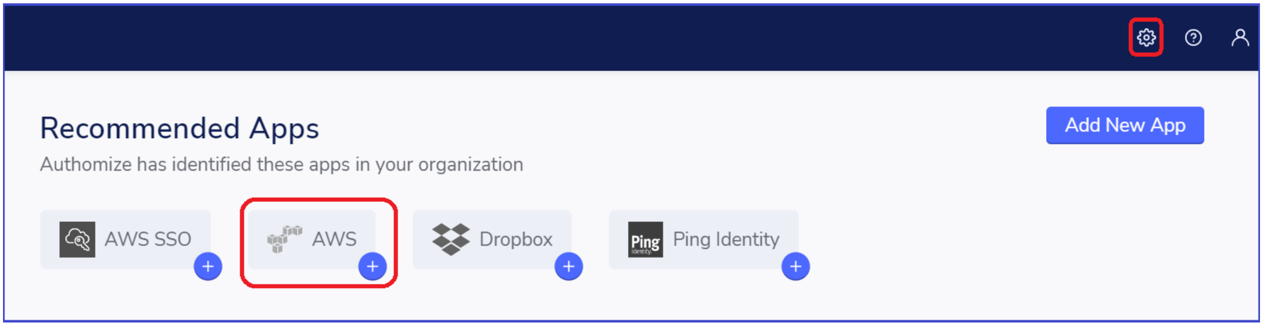
IAM user name

Password

□ Remember this account

Preparing the AWS Integration in Authomize

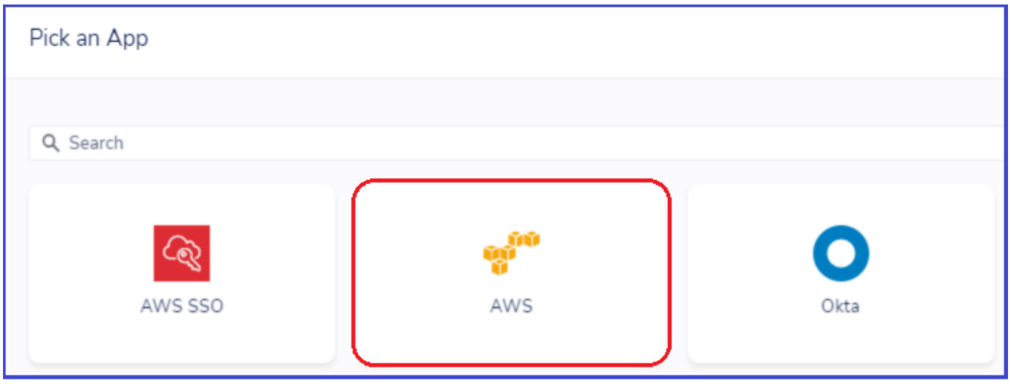
1. Go to **Settings > Data Sources**.
2. If AWS appears under Recommended Apps, click it. Otherwise, Click Add New App.



Recommended Apps

Authomize has identified these apps in your organization

3. Select **AWS.**



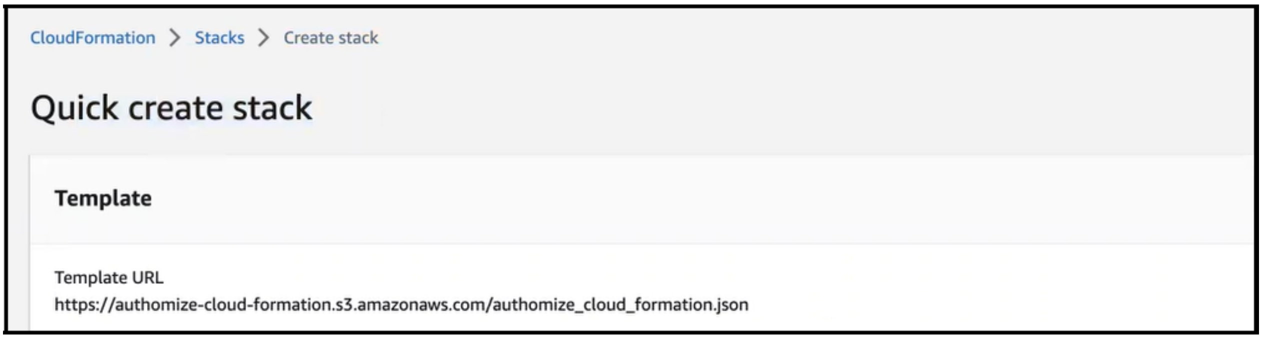
Pick an App

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

4. 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.

Creating an Authomize StackSet on AWS

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

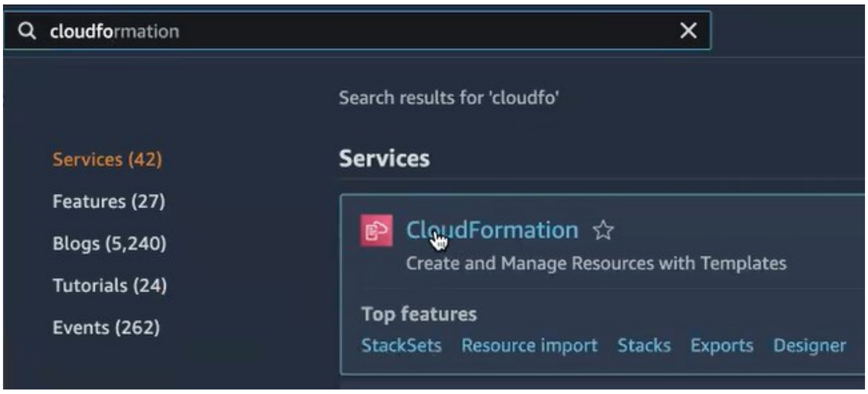
Quick create stack

Template

Template URL
https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation.json

The Template URL is entered automatically by Authomize. You will need this URL later:
`https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation.json`

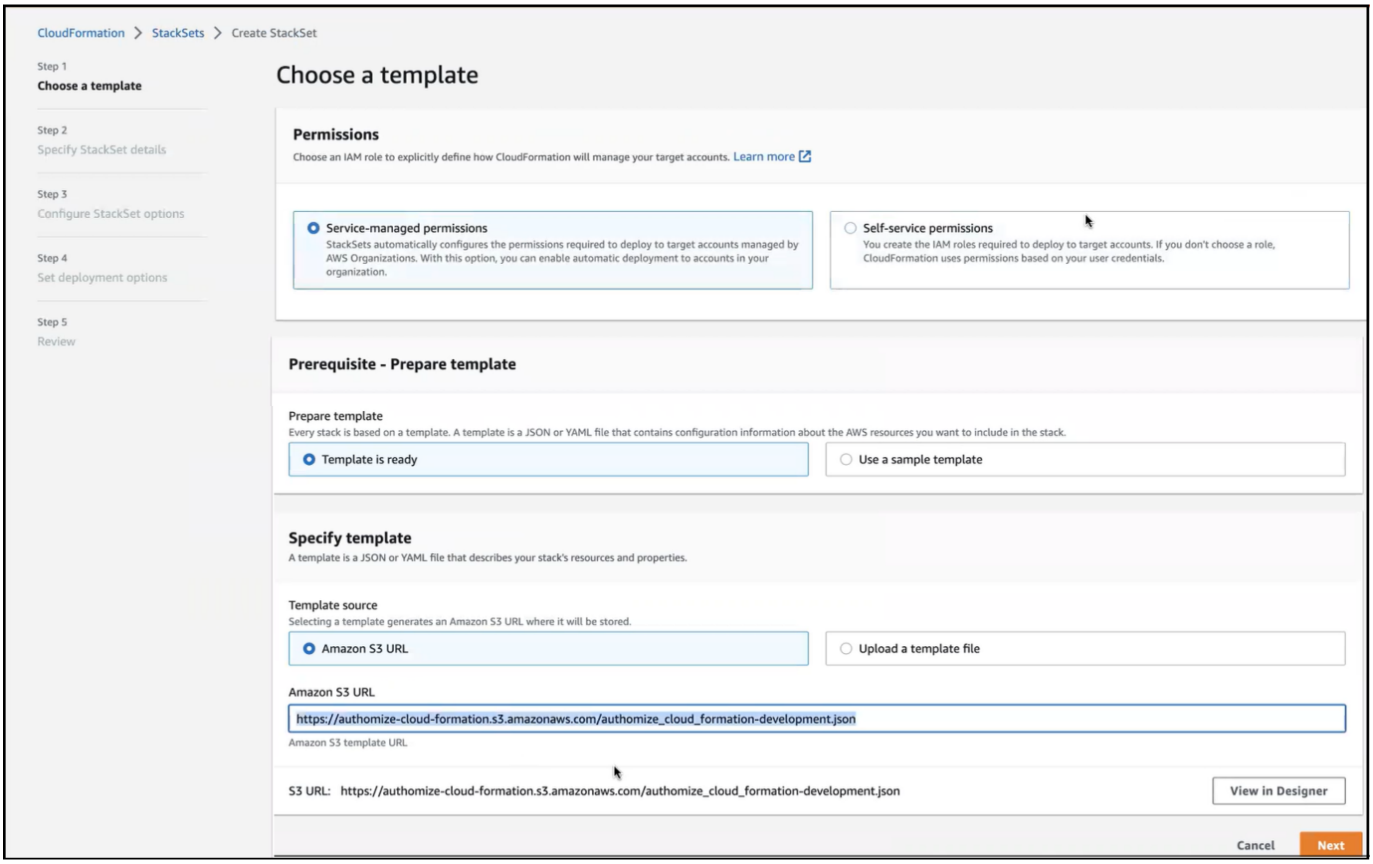
In the search field, on the menu bar, enter **CloudFormation.** Click CloudFormation then go to **StackSets**



Click Create StackSet.

Alternatively, go directly to click Create StackSet.

Follow the steps below to create an ***Authomize-Integration stackset*** *on AWS:*



CloudFormation > StackSets > Create StackSet

Step 1
Choose a template

Step 2
Specify StackSet details

Step 3
Configure StackSet options

Step 4
Set deployment options

Step 5
Review

Choose a template

Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. Learn more

● Service-managed permissions
StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization.

○ Self-service permissions
You create the IAM roles required to deploy to target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials.

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready　○ Use a sample template

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL　○ Upload a template file

Amazon S3 URL
https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation-development.json
Amazon S3 template URL

S3 URL: https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation-development.json

Fill in the fields as follows:

Step 1 Choose a Template

Permissions

Select either **Service-managed permissions** or **Self-service permissions.**

Prerequisite – Prepare template

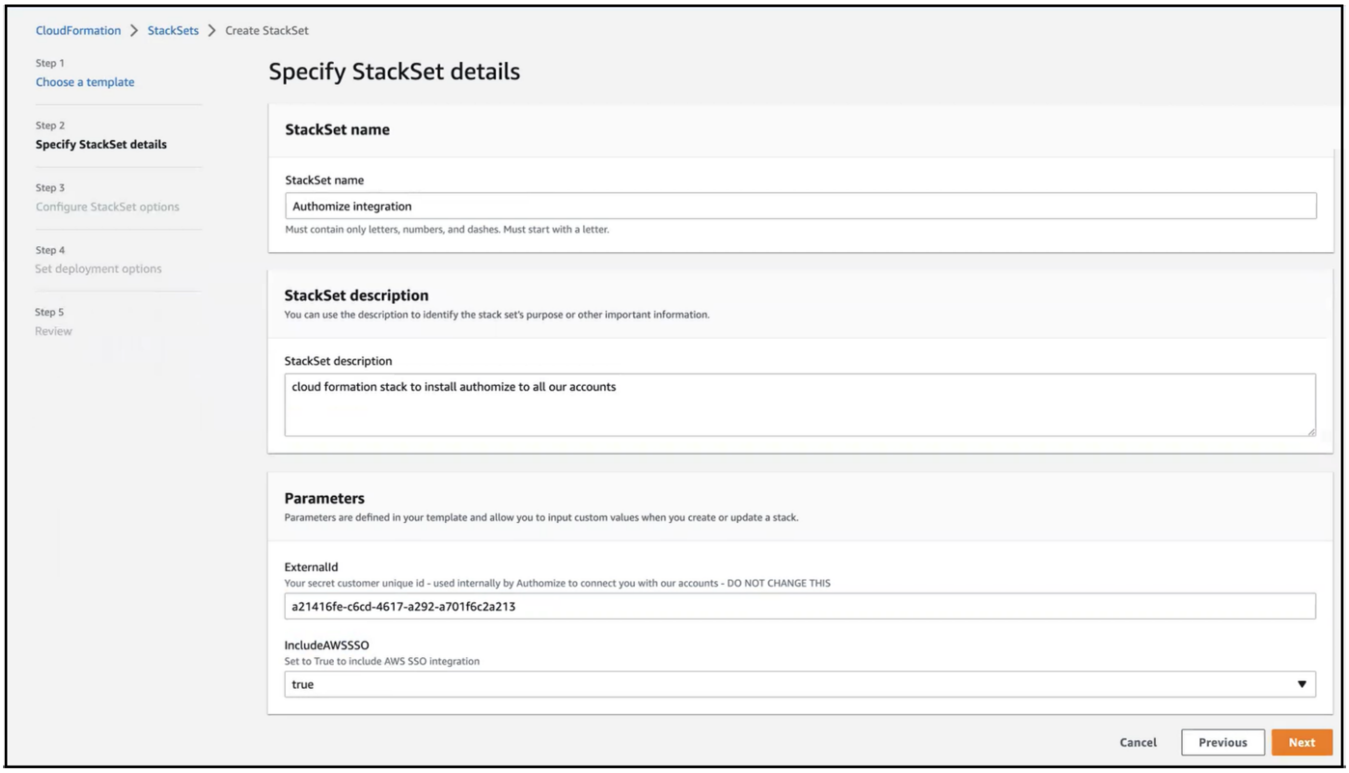
Select either **Template is ready** or **Use a sample template.**

Specify Template

Select **Amazon S3 URL.**

In the Amazon S3 URL field, enter the following URL:
`https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation.json`

Click Next to go to the **Specify StackSet details** section.



CloudFormation > StackSets > Create StackSet

Step 1
Choose a template

Step 2
Specify StackSet details

Step 3
Configure StackSet options

Step 4
Set deployment options

Step 5
Review

Specify StackSet details

StackSet name

StackSet name: Authomize integration

Must contain only letters, numbers, and dashes. Must start with a letter.

StackSet description

You can use the description to identify the stack set's purpose or other important information.

StackSet description: cloud formation stack to install authomize to all our accounts

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

Step 2 Specify StackSet details

StackSet name

Enter a StackSet name [such as **Authomize-integration**].

StackSet description

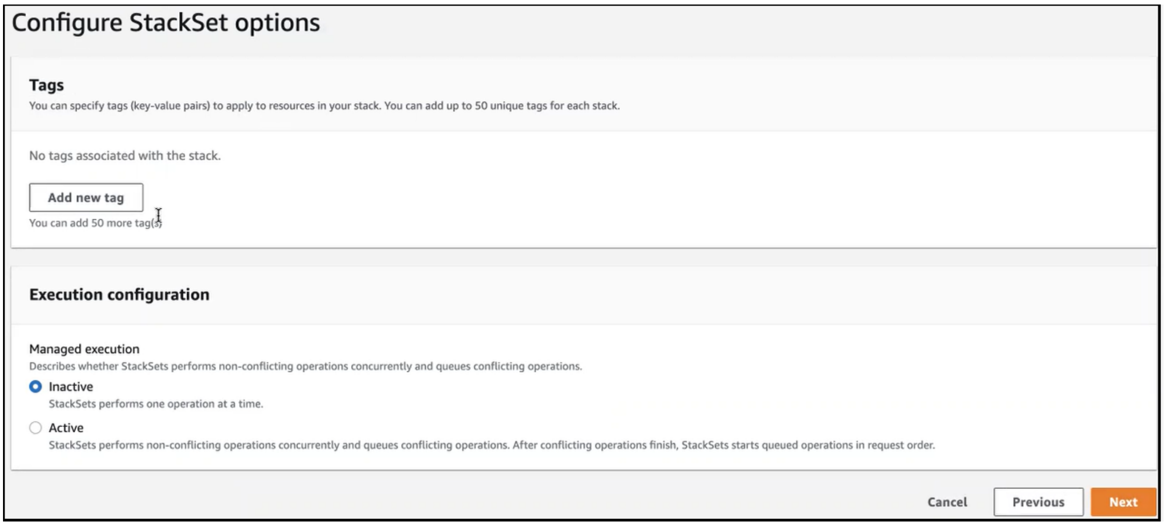
Enter a description of your choosing.

Parameters

Enter the **ExternalID** from Authomize's Integrate AWS page

Enter true in the **IncludeAWSSSO** field if your organization uses AWS Identity Center

Click **Next** to go to the **Configure StackSet options** section.



Configure StackSet options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack.

No tags associated with the stack.

You can add 50 more tag(s)

Execution configuration

Managed execution
Describes whether StackSets performs non-conflicting operations concurrently and queues conflicting operations.

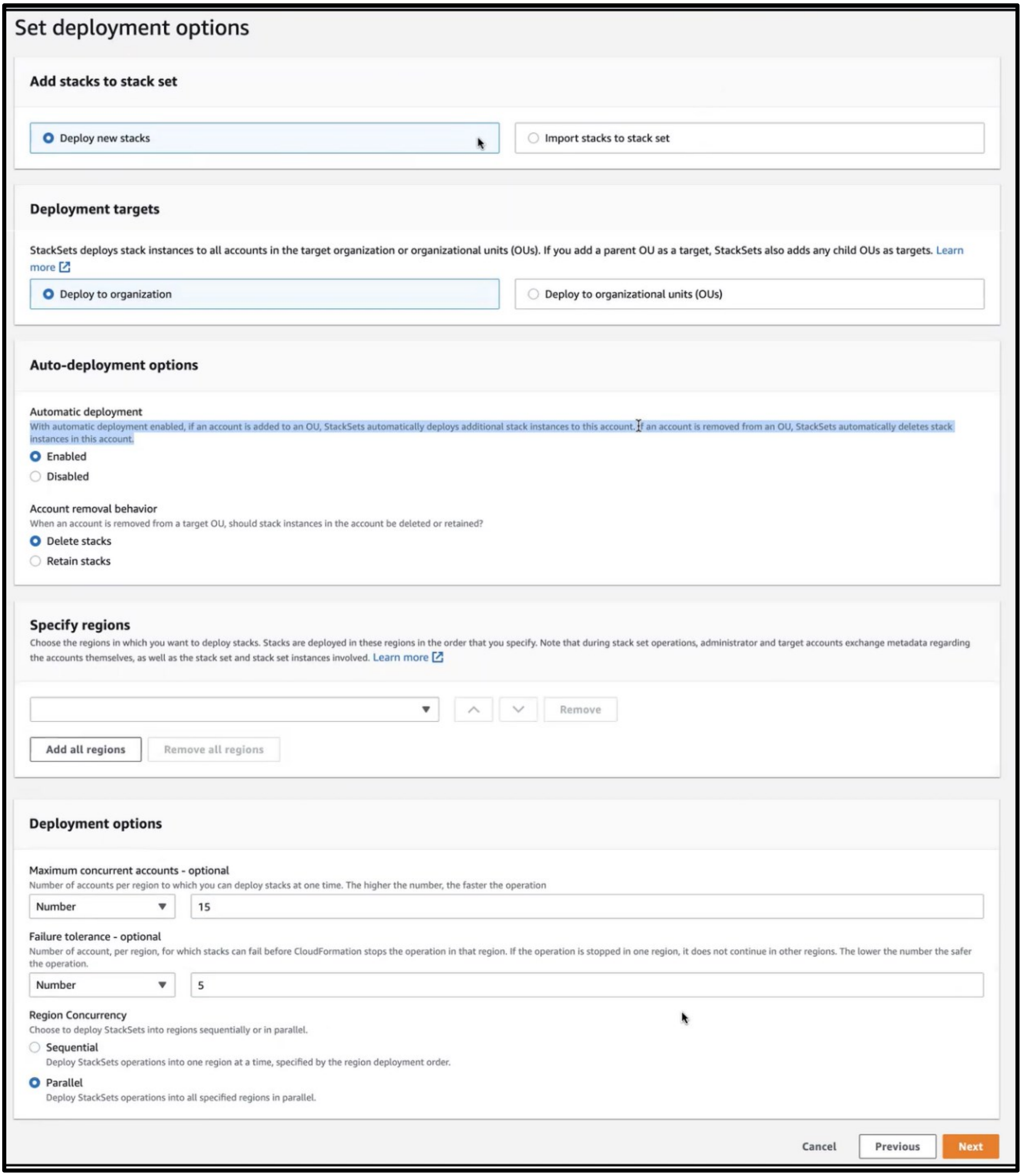
● Inactive
StackSets performs one operation at a time.

○ Active
StackSets performs non-conflicting operations concurrently and queues conflicting operations. After conflicting operations finish, StackSets starts queued operations in request order.

Step 3 Configure StackSet options

Skip step 3 for now.

Click **Next** to go to the **Set Deployment Options** section.



Set deployment options

Add stacks to stack set

● Deploy new stacks ○ Import stacks to stack set

Deployment targets

StackSets deploys stack instances to all accounts in the target organization or organizational units (OUs). If you add a parent OU as a target, StackSets also adds any child OUs as targets. Learn more

● Deploy to organization ○ Deploy to organizational units (OUs)

Auto-deployment options

Automatic deployment

With automatic deployment enabled, if an account is added to an OU, StackSets automatically deploys additional stack instances to this account. If an account is removed from an OU, StackSets automatically deletes stack instances in this account.

● Enabled

○ Disabled

Account removal behavior

When an account is removed from a target OU, should stack instances in the account be deleted or retained?

● Delete stacks

○ Retain stacks

Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify. Note that during stack set operations, administrator and target accounts exchange metadata regarding the accounts themselves, as well as the stack set and stack set instances involved. Learn more

Deployment options

Maximum concurrent accounts - optional

Number of accounts per region to which you can deploy stacks at one time. The higher the number, the faster the operation

Number 15

Failure tolerance - optional

Number of account, per region, for which stacks can fail before CloudFormation stops the operation in that region. If the operation is stopped in one region, it does not continue in other regions. The lower the number the safer the operation.

Number 5

Region Concurrency

Choose to deploy StackSets into regions sequentially or in parallel.

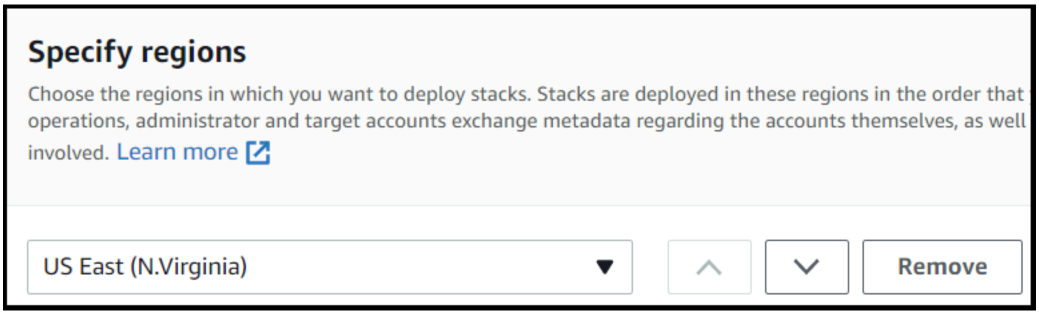
○ Sequential

Deploy StackSets operations into one region at a time, specified by the region deployment order.

● Parallel

Deploy StackSets operations into all specified regions in parallel.

For example:



Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that operations, administrator and target accounts exchange metadata regarding the accounts themselves, as well involved. Learn more

US East (N.Virginia)

Step 4 Set Deployment options

Add stacks to stack set

Select either **Deploy new stacks** or **Import stacks to stack set.**

Deployment targets

Select either **Deploy to organization** or **Deploy to organization units (OUs).**

If you picked **OUs**

Set the **OU ID** to [your account]

Auto-deployment options

Skip these options.

Specify Regions

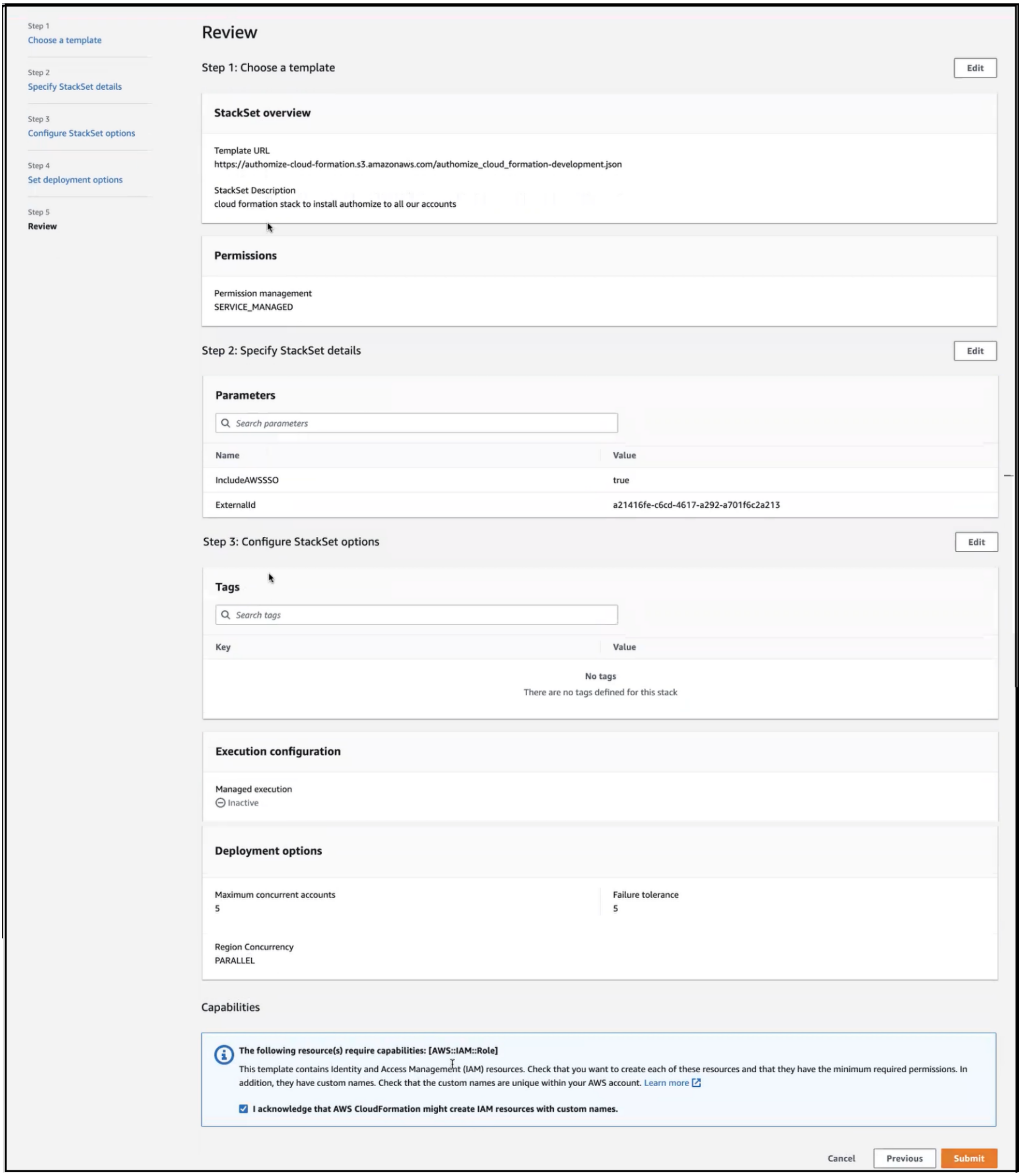
If you leave the regions field empty, all regions (in your organization) will be included.
If you specify one or more regions, data will be fetched only from those regions.
Note: Do **not** install Authomize CloudFormation on Africa (Cape Town), Asia Pacific (Hong Kong), Asia Pacific (Jakarta), Europe (Milan), Middle East (UAE), or Midde East (Bahrain).

Deployment options

Enter a number of concurrent accounts and failure tolerance.
Select parallel Region Concurrency for faster processing.

Click Next to go to the **Review** section.

Check the entries on the Review page to see if everything is correct.



Review

Step 1: Choose a template

StackSet overview

Template URL
https://authomize-cloud-formation.s3.amazonaws.com/authomize_cloud_formation-development.json

StackSet Description
cloud formation stack to install authomize to all our accounts

Permissions

Permission management
SERVICE_MANAGED

Step 2: Specify StackSet details

Parameters

Name	Value
IncludeAWSSSO	true
ExternalId	a21416fe-c6cd-4617-a292-a701f6c2a213

Step 3: Configure StackSet options

Tags

Key	Value

No tags
There are no tags defined for this stack

Execution configuration

Managed execution
⊖ Inactive

Deployment options

Maximum concurrent accounts
5

Failure tolerance
5

Region Concurrency
PARALLEL

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

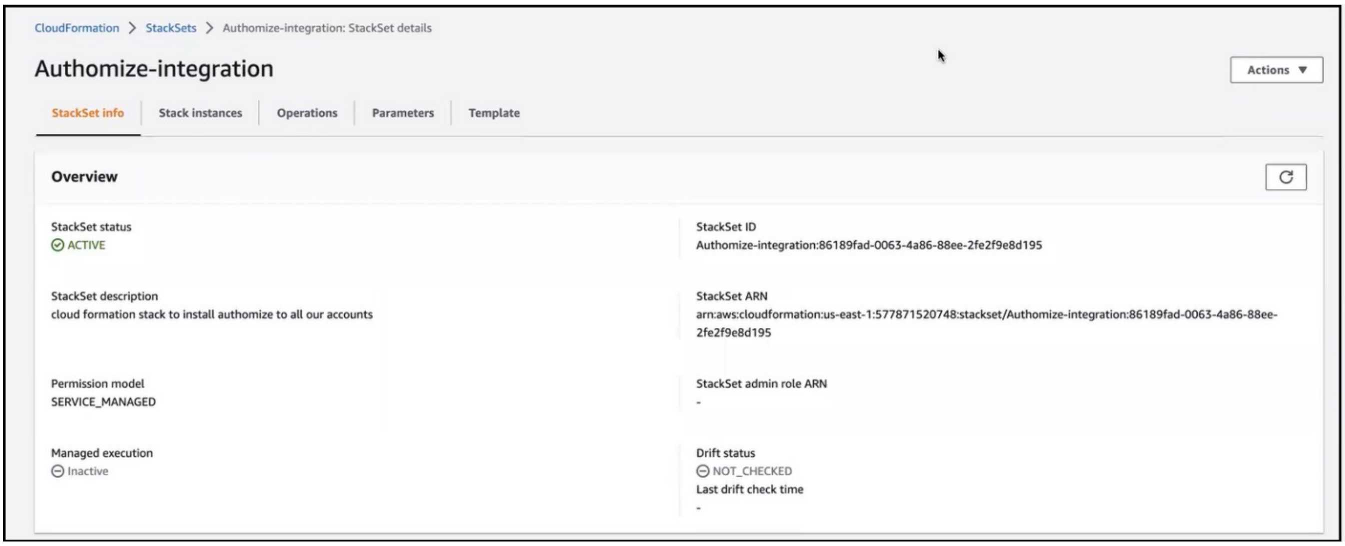
☑ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

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

Click Submit to create a StackSet.

Go to CloudFormation>StackSets options

Check if the Authomize-integration StackSet status is active (was created successfully).



CloudFormation > StackSets > Authomize-integration: StackSet details

Authomize-integration

Actions ▼
StackSet info
Stack instances
Operations
Parameters
Template

Overview

StackSet status
✓ ACTIVE

StackSet ID
Authomize-integration:86189fad-0063-4a86-88ee-2fe2f9e8d195

StackSet description
cloud formation stack to install authomize to all our accounts

StackSet ARN
arn:aws:cloudformation:us-east-1:577871520748:stackset/Authomize-integration:86189fad-0063-4a86-88ee-2fe2f9e8d195

Permission model
SERVICE_MANAGED

StackSet admin role ARN
-

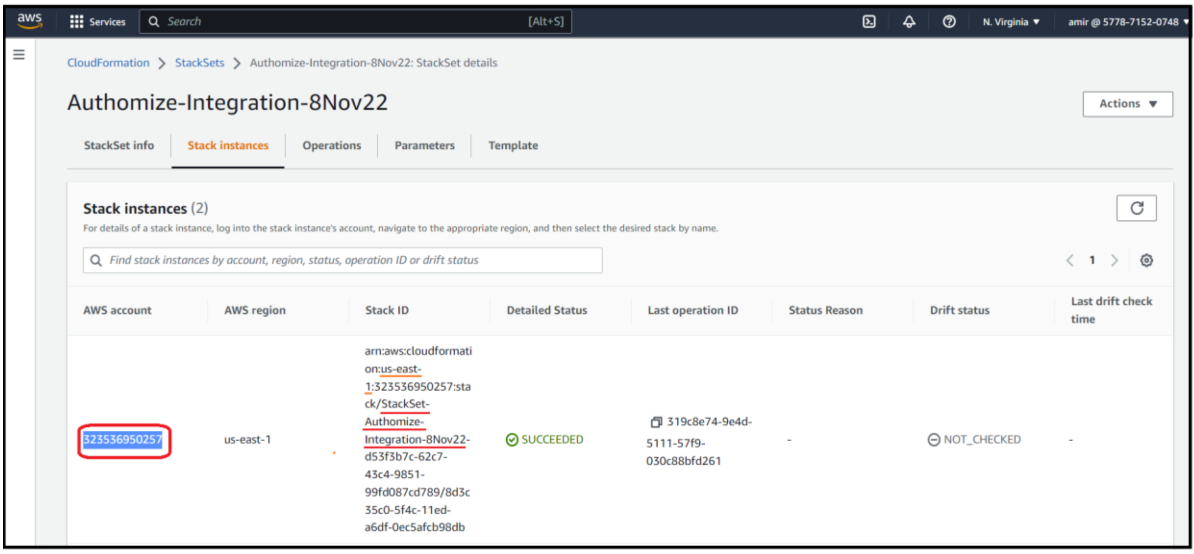
Managed execution
⊖ Inactive

Drift status
⊖ NOT_CHECKED
Last drift check time
-

Complete the Integration

In the ***Integrate AWS*** dialog:

5. Insert comma delimited **Account Numbers** (copied from Authomize-Integration StackSet) in the Account number field. The Management Account number goes in the Account **and** Management fields



aws
Services
Search
[Alt+S]
N. Virginia ▼
amir @ 5778-7152-0748 ▼
CloudFormation > StackSets > Authomize-Integration-8Nov22: StackSet details

Authomize-Integration-8Nov22

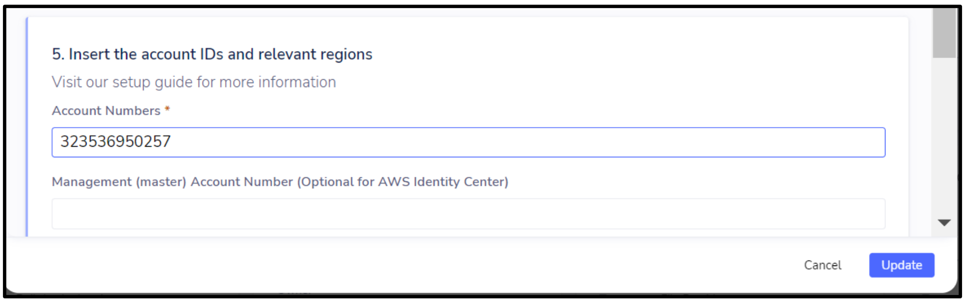
Actions ▼
StackSet info
Stack instances
Operations
Parameters
Template

Stack instances (2)

For details of a stack instance, log into the stack instance's account, navigate to the appropriate region, and then select the desired stack by name.

Find stack instances by account, region, status, operation ID or drift status
1

AWS account	AWS region	Stack ID	Detailed Status	Last operation ID	Status Reason	Drift status	Last drift check time
323536950257	us-east-1	arn:aws:cloudformation:us-east-1:323536950257:stack/StackSet-Authomize-Integration-8Nov22-d53f3b7c-62c7-43c4-9851-99fd087cd789/8d3c35c0-5f4c-11ed-a6df-0ec5afcb98db	✓ SUCCEEDED	319c8e74-9e4d-5111-57f9-030c88bfd261	-	⊖ NOT_CHECKED	-



5. Insert the account IDs and relevant regions

Visit our setup guide for more information

Account Numbers *

323536950257

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

4. Skip step 4.
5. Insert comma delimited **Account Numbers** (copied from Authomize-Integration StackSet) in the **Account Number** field.

   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.

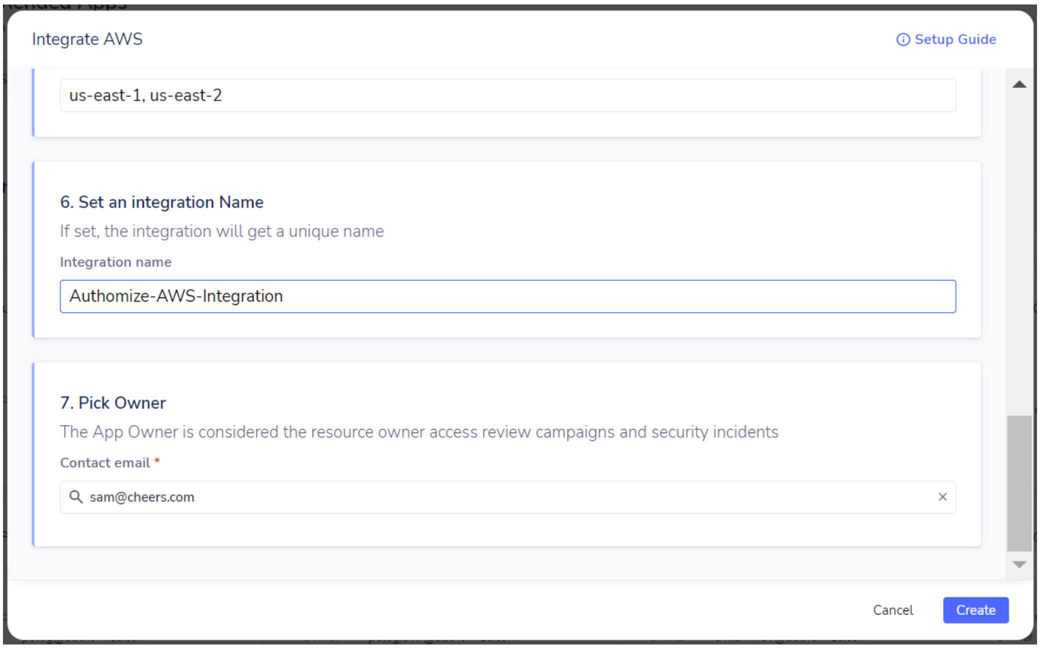
   If you insert a Management Account, that account number must be included (in comma delimited format) in the **Account Number** field.

   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.

   Skip the **Assumed Role**.

6. Enter an Integration name.

7. Enter Owner's email.



Integrate AWS

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

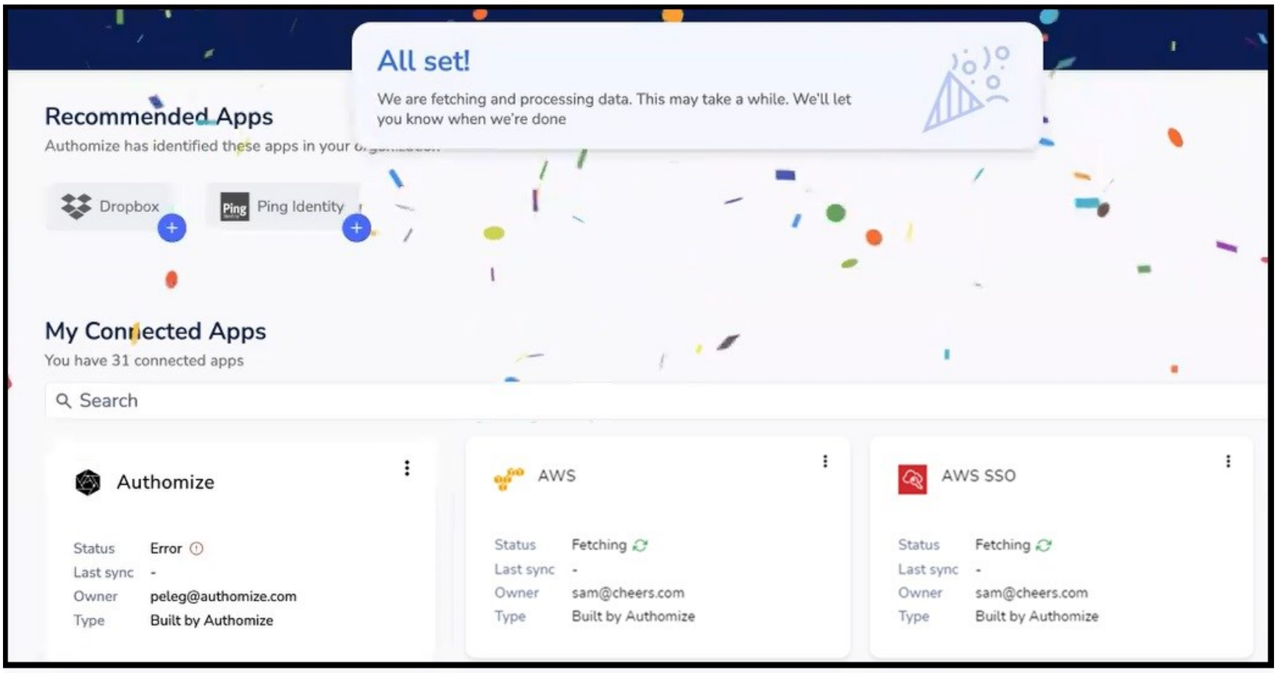
The App Owner is considered the resource owner access review campaigns and security incidents

Contact email *

sam@cheers.com

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 o...

My Connected Apps

You have 31 connected apps

Authomize

Status Error

Last sync -

Owner peleg@authomize.com

Type Built by Authomize

AWS

Status Fetching

Last sync -

Owner sam@cheers.com

Type Built by Authomize

AWS SSO

Status Fetching

Last sync -

Owner sam@cheers.com

Type 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 **IncludeAWSSSO** 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