

# Syntree Flosports | AWS Macie

## What is Amazon Macie?

Amazon Macie is a data security service that discovers sensitive data by using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks.

To help you manage the security posture of your organization's Amazon Simple Storage Service (Amazon S3) data estate, Macie provides you with an inventory of your S3 buckets, and automatically evaluates and monitors the buckets for security and access control. If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary.

Macie also automates discovery and reporting of sensitive data to provide you with a better understanding of the data that your organization stores in Amazon S3. To detect sensitive data, you can use built-in criteria and techniques that Macie provides, custom criteria that you define, or a combination of the two. If Macie detects sensitive data in an S3 object, Macie generates a finding to notify you of the sensitive data that Macie found.

In addition to findings, Macie provides statistics and other data that offer insight into the security posture of your Amazon S3 data, and where sensitive data might reside in your data estate. The statistics and data can guide your decisions to perform deeper investigations of specific S3 buckets and objects. You can review and analyze findings, statistics, and other data by using the Amazon Macie console or the Amazon Macie API. You can also leverage Macie integration with Amazon EventBridge and AWS Security Hub to monitor, process, and remediate findings by using other services, applications, and systems.

## Important Features of Amazon Macie:

- Automate the discovery of sensitive data
- Discover a variety of sensitive data types
- Evaluate and monitor data for security and access control
- Review and analyze findings
- Monitor and process findings with other services and systems
- Centrally manage multiple Macie accounts
- Develop and manage resources programmatically

## Start Creating Stack of CloudFormation:

### Step: 1

- Added Object URL of your S3 source Bucket in below

**Create stack**

Step 1: **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 ☐ Create template in Designer

**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://cf-templates-x4tk28lqib4-us-east-2.s3.us-east-2.amazonaws.com/macie/enable-macie.yaml

Amazon S3 template URL  
S3 URL: https://cf-templates-x4tk28lqib4-us-east-2.s3.us-east-2.amazonaws.com/macie/enable-macie.yaml

[View in Designer](#)

[Cancel](#) [Next](#)

## Step: 2

- Add parameters of CloudFormation Stack

**Specify stack details**

Stack name  
Stack name  
awsMacie  
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.

MacieMasterAccountId  
The AWS Account ID that will be configured as the Delegated Admin.  
785981945575

OrganizationId  
The Amazon Organizations ID for Control Tower.  
o-6c7qtp3db

RoleToAssume  
What role should be assumed in accounts to enable GuardDuty? The Default is AWSControlTowerExecution for a Control Tower environment.  
AWSControlTowerExecution

S3Key  
The S3 Path to the Lambda Zip File  
macie/macie.zip

S3SourceBucket  
The S3 Bucket that contains the Lambda Zip File.  
cf-templates-x4tk28lqib4-us-east-2

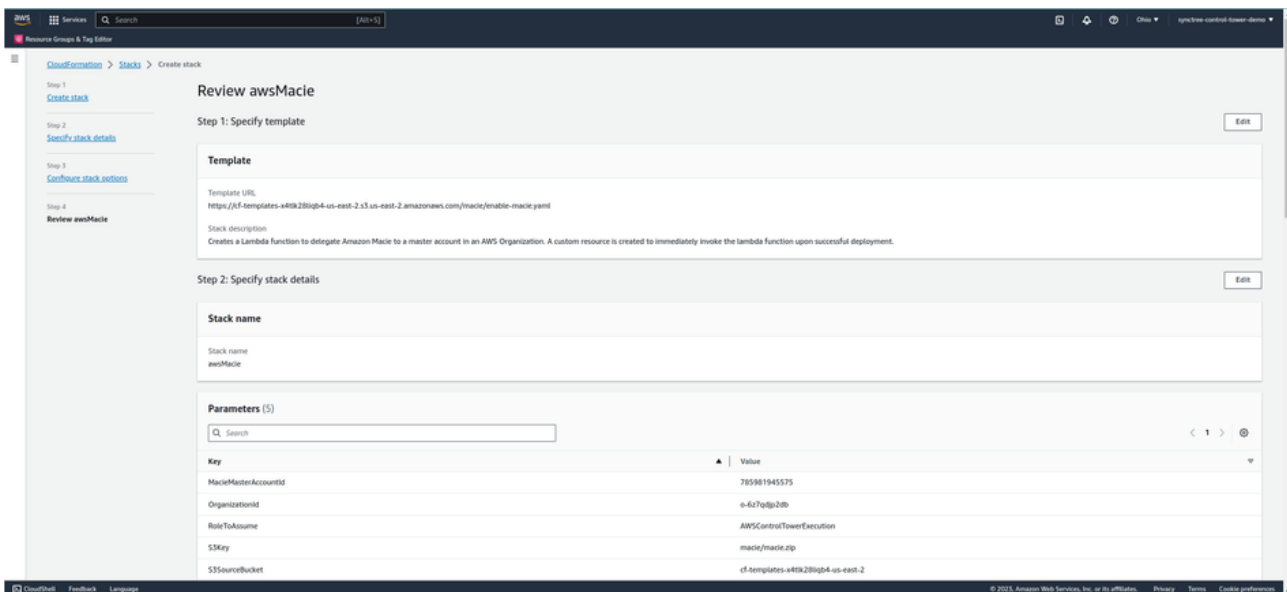
[Cancel](#) [Previous](#) [Next](#)

S3 key - Add lambda zip file of Macie

MacieMasterAccount - Add Audit account ID here

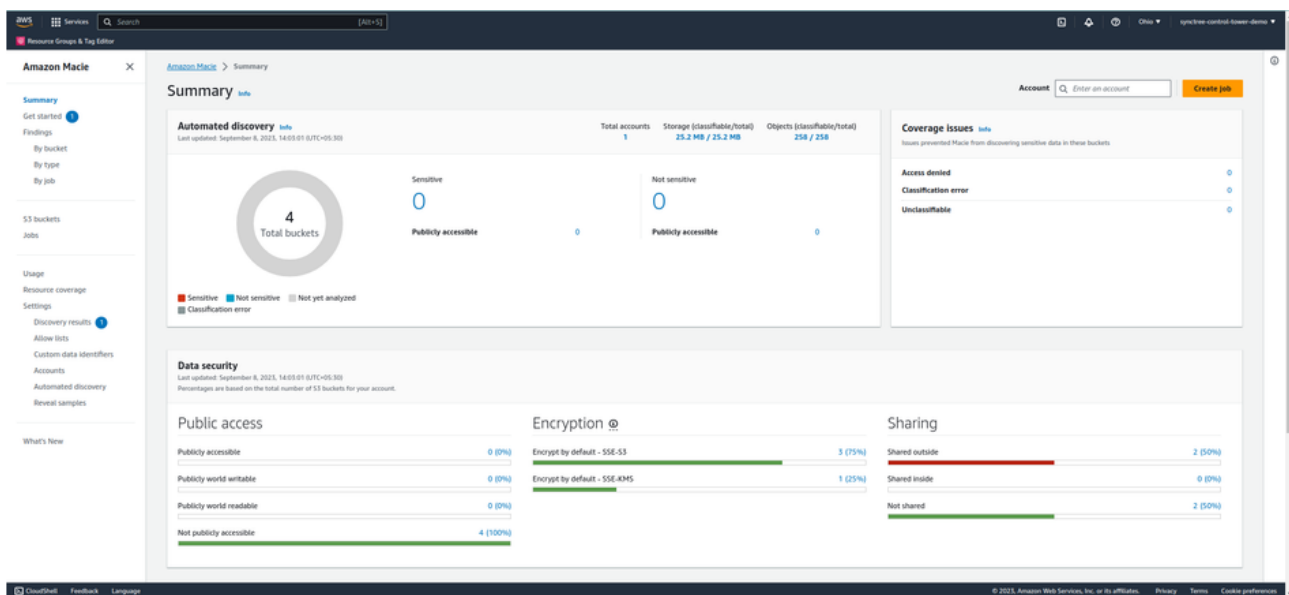
## Step: 3

- Once reviewed parameters of the stack and acknowledged enable after that click on submit.



## Step4:

- Go on AWS Macie dashboard and check it's working & showing your all S3 Bucket's.



Reference Link:

Repository: [CfCT-Amazon-Macie](#)