AWS Integration Guide

CBOM Secure · AWS Discovery Sensor

Overview

This guide describes the step-by-step procedure to configure AWS Identity and Access Management (IAM) so that the CBOM Secure AWS Discovery Sensor can successfully discover:

- AWS Certificate Manager (ACM) certificates
- IAM server certificates
- AWS KMS asymmetric keys (metadata only)

The procedure covers creating a least-privilege IAM policy, creating a dedicated IAM user, generating access credentials, and verifying permissions. It uses the AWS Management Console (GUI only) and does not require the AWS CLI.

Prerequisites

Before beginning, ensure the following:

- You have access to the AWS Management Console.
- You are signed in as the root user, or as an IAM user with permissions to manage IAM (for example, the IAMFullAccess policy).
- You have at least one AWS region enabled (for example, us-east-1).
- You have the CBOM Secure AWS Discovery Sensor package ready for configuration.

Step-by-Step Guide

Step 1: Open the IAM Service

- Sign in to the AWS Management Console.
- In the search bar, type IAM.
- Click IAM to open the Identity and Access Management console.

Step 2: Create the Discovery IAM Policy

- In the left navigation menu, click Policies.
- Click Create policy.
- Select the JSON tab and paste the policy document below exactly as shown.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSCertificateDiscovery",
```

```
    "Effect": "Allow",
    "Action": [
      "acm:ListCertificates",
      "acm:DescribeCertificate",
      "iam:ListServerCertificates",
      "iam:GetServerCertificate",
      "iam:ListRoles",
      "iam:ListUsers",
      "iam:ListRolePolicies",
      "iam:ListUserPolicies",
      "iam:GetRolePolicy",
      "iam:GetUserPolicy",
      "iam:ListAttachedRolePolicies",
      "iam:ListAttachedUserPolicies",
      "iam:GetPolicy",
      "iam:GetPolicyVersion",
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:DescribeKey",
      "kms:GetPublicKey",
      "kms:ListResourceTags"
    ],
    "Resource": "*"
  }
 ]
}
```

Note This policy grants read-only access required for discovery. No write, delete, or key-material export permissions are included.

Step 3: Name and Create the Policy

```
Policy name: CBOM-AWS-Certificate-Discovery
```

- Description: Read-only access for CBOM AWS certificate and key discovery

Click Create policy.

Step 4: Create a Dedicated IAM User

- In the IAM console, click Users.
- Click Create user.

```
Set the user name to cbom-aws-discovery, then click Next.
```

Step 5: Attach the Policy to the User

- Select Attach policies directly.

```
Search for CBOM-AWS-Certificate-Discovery and select it.
```

- Click Next, confirm the user name and attached policy, then click Create user.

Step 6: Generate Access Credentials

```
Open Users and click the user cbom-aws-discovery.
```

- Open the Security credentials tab and scroll to Access keys.
- Click Create access key, select Application running outside AWS, then click Next.

- (Optional) Skip tags, then click Create access key.

The Access key ID and Secret access key are now displayed. Download the .csv file or copy both values into a secure vault or password manager.

Note Important: The secret access key is displayed only once and cannot be retrieved later.

Step 7: Configure the CBOM Secure AWS Sensor

Use the generated credentials in the CBOM Secure AWS discovery configuration:

```
aws_access_key_id: "<AWS_ACCESS_KEY_ID>"
aws_secret_access_key: "<AWS_SECRET_ACCESS_KEY>"
region: us-east-1
services:
  - acm
  - iam
  - kms
scan_name: AWSDiscovery
```

Step 8: Validate Discovery

After configuration, run the AWS discovery task from CBOM Secure and confirm:

- The task completes successfully.

```
No AccessDenied errors appear.
```

- IAM server certificates are discovered (if present).

In AWS, open IAM → Users → Security credentials and confirm the access key shows a recent usage timestamp.

Step 9: Troubleshooting Common Errors

If discovery fails, check the error against the table below.

Error	Likely cause	Resolution
AccessDenied: iam:ListServerCertificates	Policy not attached, incorrect policy document, or a permission boundary is applied.	Re-check Steps 2, 4, and 5. Ensure the correct policy is attached to the correct user and no deny boundary exists.

Step 10: Security Recommendations (Optional)

For production environments:

- Use IAM roles with STS instead of long-term access keys.
- Restrict permissions further if IAM server certificates are not required.
- Rotate access keys periodically.
- Monitor CloudTrail for credential usage.