AWS Public CA (ACM) Connector Integration Guide

This guide describes onboarding and using AWS Certificate Manager (ACM) as an agentless public CA connector in CertSecure Manager.

Prerequisites

CertSecure Manager

- CertSecure Manager frontend and backend are operational.
- Your account has the Manage Certification Authorities permission.
- The AWS agentless CA entitlement is enabled on the tenant - the AWS tile is selectable, not greyed out.
- Outbound HTTPS (443) connectivity from the CertSecure Manager backend to the AWS ACM and Route 53 service endpoints, without TLS interception.

AWS

- An AWS account with ACM available in the target region.
- An Access Key ID and Secret Access Key for a principal with the required ACM permissions. If you use temporary credentials, you will also need the Session Token.
- The target region decided. ACM certificates that will front Amazon CloudFront must be issued in us-east-1.

Domains

- For automated DNS validation: the domain's zone is hosted in Amazon Route 53 in the same AWS account, and the credential has the required Route 53 permissions.
- For Email validation: one of the standard administrative addresses at the registered domain is monitored and reachable.
- No conflicting CAA record on the domain. If CAA records exist, Amazon must be a permitted issuer or issuance will fail.

Note: ACM requires domain validation: a public certificate is not issued until every domain name on the request has been validated. Plan for that before your first enrollment - both automated DNS and email validation methods are covered below.

Configuration Steps

Step 1: Gather the Connection Details

- The Access Key ID, Secret Access Key and, if applicable, the Session Token.
- The region, and the Validation Method this connection will use.
- Confirmation that the credentials work.

Step 2: Add the AWS-ACM Connection

- Go to Administration → Certificate Authorities.
- Under Agentless CAs, click Configure on the AWS tile. The AWS CA page opens with the AWS-PCA and AWS-ACM groups.
- Click Add New Connection to open the Configure AWS CA dialog.
- Enter the CA Name and an optional Description.
- Set CA Type to AWS-ACM.
- Enter the Access Key and Secret Key, plus the Session Token if you are using temporary credentials.

- Select the Region and the Validation Method.
- Add a Note if your change process expects one, then click Save.
- Expand the AWS-ACM group. The connection appears with a generated Connection ID, Connector = CertSecure Backend and Status = Enabled. The CA addition task can be monitored under Utilities → Task.

Step 3: Verify the Connection and First Sync

- Confirm Status = Enabled and, once the first job has run, Sync = Completed.
- The CA appears under Administration → Certificate Authorities → Manage CAs and becomes selectable in the Certificate Authority dropdown at enrollment.
- Existing ACM certificates for that account and region appear in Inventory with status, expiry, key algorithm, SANs and in-use associations.
- Spot-check a few records against the AWS console to confirm the inventory looks right.

Step 4: Enroll, Then Operate

- Issue your first certificate from Enrollment → Generate Certificate.
- Confirm expiry alerting and ownership metadata are working as expected for the new record.
- Work through your validation checklist before handing the connection to operators.