AWS Private CA (PCA) Connector Integration Guide

This guide describes onboarding and using an existing AWS Private Certificate Authority as an agentless private 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 Private CA service endpoint, without TLS interception.

AWS Private CA

- A private CA already exists and is ACTIVE. A CA that was created but never activated cannot issue.
- You have the full CA ARN, in the form arn:aws:acm-pca:<region>:<account>:certificate-authority/<uuid>.
- The CA certificate's own expiry is comfortably beyond the validity you intend to issue.
- Revocation is already configured on the CA in AWS if you will need to revoke.

AWS Credentials

- An Access Key ID and Secret Access Key for a principal with the required AWS Private CA permissions. If you use temporary credentials, you will also need the Session Token.
- The credential is for the same AWS account and region as the CA. There is no cross-account role option.

Configuration Steps

Step 1: Gather the Connection Details

- The Access Key ID, Secret Access Key and, if applicable, the Session Token.
- The CA ARN and the region it lives in.
- Confirmation that the CA is ACTIVE and the credentials work.

Step 2: Add the AWS-PCA 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-PCA. The CA ARN field appears.
- Enter the Access Key and Secret Key, plus the Session Token if you are using temporary credentials.
- Paste the CA ARN.
- Select the Region - the same region as in the CA ARN.
- Add a Note if your change process expects one, then click Save.

- Expand the AWS-PCA 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 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.
- The CA certificate and chain are retrieved and displayed, along with its subject, key algorithm and validity dates.
- Confirm CA expiry alerting is in place. A CA that expires inside the validity window of the certificates it issues is a latent outage.

Step 4: Enroll, Then Operate

- Issue a test certificate for each template you intend to offer.
- Inspect the result and confirm the subject, SANs and key usages are what the requester expected.
- Work through your validation checklist before handing the connection to operators.