Sectigo SCM CA Connector Integration Guide

This guide describes adding Sectigo Certificate Manager (SCM) as a CA connector in CertSecure Manager. Like other agentless connectors, the integration talks directly to Sectigo's REST API and requires no software installation on a separate host. Sectigo appears as a CA type alongside AWS Private CA, GlobalSign, EJBCA, HashiCorp Vault, Google CAS and Let's Encrypt.

Note: There is no ISO/installer step and no registration token. If Sectigo appears greyed/unconfigured on your tenant, it becomes selectable once the corresponding entitlement is enabled.

Prerequisites

- CertSecure Manager frontend and backend are fully operational.
- Your account has the "Manage Certification Authorities" permission.
- A Sectigo Certificate Manager (SCM) account with an admin-level API login (username + password) that has API access enabled.
- Your Sectigo account's Customer URI (the "customerUri" value).
- At least one Organization already created in SCM, and its numeric Organization ID.
- That organization is entitled to at least one SSL certificate profile/type in SCM.
- Target domain(s) registered and able to complete Domain Control Validation (DCV) in Sectigo – issuance will fail for any domain that has not passed DCV.
- Outbound HTTPS (443) connectivity from the CertSecure Manager backend to the Sectigo API endpoint (default https://cert-manager.com/api, or your dedicated SCM instance URL).

Connection Reference

Item	Requirement / Value
Profile name	Friendly name for this Sectigo credential profile in CertSecure Manager
Username	Sectigo SCM admin login
Password	Sectigo SCM admin password
Customer URI	Your Sectigo account's "customerUri" value
API base URL	Default https://cert-manager.com/api (override for a dedicated SCM instance)
Organization ID	Optional – numeric ID of the default SCM organization used for issuance
Certificate type ID	Optional – default SSL profile used as a fallback if none is specified at enrollment time
DCV mode	"auto" or "manual" – controls whether CNAME domain validation is automated (default: manual)

Configuration Steps

Step 1: Gather Sectigo SCM Connection Details

- Log in to Sectigo Certificate Manager and note: the admin username/password and your Customer URI.

- If this is your first integration, confirm with your Sectigo account manager that API access is enabled for the account – CertSecure Manager needs it to connect on your behalf.

Step 2: Add the Sectigo CA in CertSecure Manager

- Go to Administration > Certificate Authorities.
- Click Configure below Sectigo logo under Agentless CAs.
- Click on Add New Connection.
- Enter: Profile/CA Name, Username, Password, Customer URI, API Base URL (defaults to the standard Sectigo endpoint), Organization ID (optional), Certificate Type (optional default profile), and DCV Mode (Auto or Manual).
- Click Save.
- The Status should change from Pending to Enabled. The CA Agent Addition task can be monitored under Utilities > Task.

Step 3: Verify Connectivity and Sync

- CertSecure Manager validates the endpoint and credentials; on success the CA shows Online under Administration > Certificate Authorities > Manage CAs > Public CAs.

Step 4: Add, Activate, and Delete Domains

- Certificates can only be issued for domains registered under the CA's Domains. To add one: go to Administration > Certificate Authorities.
- Click Configure below Sectigo logo under Agentless CAs.
- Click on Manage Configs.
- Right-click on the CA config.
- Click on Manage Domains.
- To add a domain, click on Add Domain.
- Click Save. The domain is created in Sectigo in a Pending validation state.
- To remove a domain, right-click on the domain to delete it.

Step 5: Complete Domain Control Validation (DCV)

- Sectigo will not issue a certificate for a domain until that domain shows a validated DCV status. On the CA's config page:
- Right-click on the CA config.
- Right-click the target domain, hover over Validate With and choose a validation method: HTTP, HTTPS, CNAME, or Email.
- Repeat for every domain you plan to issue certificates for.

Step 6: Enroll / Renew / Revoke

- **Issue:** Enrollment > Generate Certificate (or CSR enrollment) in the CertSecure Manager UI → select the Sectigo CA, certificate template (the Sectigo certificate type) and fill all mandatory information → Submit. CertSecure Manager calls Sectigo to issue the certificate and the certificate can be downloaded later. The enrollment can be monitored under Utilities > Task.
- **Renew / Revoke:** performed from Inventory, the same as any other CA.

Troubleshooting

Symptom	Likely Cause	Fix
CA type greyed out	Entitlement/feature flag not enabled	Confirm license for Sectigo
"Connection failed" when saving the CA	Wrong Username/Password or Customer URI, or the SCM account lacks API access	Re-verify credentials in Sectigo SCM; confirm API access is enabled for the account
Enrollment rejected – domain not validated	Target domain has not completed Domain Control Validation in Sectigo	Complete DCV from the CA's DCV view (or directly in the Sectigo SCM portal) before enrolling
401 / 403 from the CA	Sectigo credentials were changed or revoked on the Sectigo side	Edit the CA in CertSecure Manager and re-enter the current Username/Password
Enrollment rejected on subject/SAN	Requested CN/SANs not permitted by the selected certificate profile	Align the request with the certificate type's allowed fields in Sectigo
TLS error	Corporate proxy or firewall intercepting TLS to the Sectigo API host	Allow outbound HTTPS 443 from the CertSecure Manager backend to the Sectigo API host without TLS interception