# EJBCA Agentless CA Connector Integration Guide

This guide describes adding EJBCA as an agentless CA connector in CertSecure Manager. Unlike agent-based connectors (which require installing a connector service via the ISO), the agentless integration is configured entirely from the CertSecure UI using EJBCA's REST API and requires no software installation on a separate host. EJBCA appears as a CA type alongside AWS Private CA, GlobalSign, HashiCorp Vault, Google CAS and Let's Encrypt.

**Note:** There is no ISO/installer step and no registration token. If EJBCA 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 reachable EJBCA instance with its REST API (and/or EST) enabled and the target CA online.
- Client credentials for EJBCA: an authorized client TLS certificate (mTLS) or username/password with rights to enroll and revoke on the target CA.
- The names of the EJBCA CA, End Entity Profile, and Certificate Profile to be used.
- Network connectivity from the CertSecure backend to the EJBCA API (default HTTPS 443/8443).

## Connection Reference

| Item | Requirement / Value |
|---|---|
| API endpoint | e.g. https://{URL}/ejbca/ejbca-rest-api |
| Auth type | Client cert + key (mTLS) or Basic |
| CA name | Target issuing CA in EJBCA |
| End Entity Profile | Governs subject/SAN and allowed fields |
| Certificate Profile | Governs key algo/size, validity, EKUs |

## Configuration Steps

### Step 1: Gather EJBCA Connection Details

- Base URL / API endpoint.
- Auth type and credential (client certificate + key, or basic).
- CA name, End Entity Profile, Certificate Profile, plus the key algorithm/size and validity permitted by the profile.

### Step 2: Add the EJBCA CA in CertSecure

- Go to Administration > CA Management → Add CA.
- Choose CA Type: EJBCA.
- Enter: Display/CA Name, API Base URL, Auth Type + credentials (upload client cert/key or enter basic), CA / End Entity Profile / Certificate Profile, and Renewal/Sync Interval.
- Click Save.

### Step 3: Verify Connectivity and Sync

- CertSecure validates the endpoint and credentials; on success the CA shows Online under Administration > CA Management (and Utilities > Connectors if surfaced).

**Step 4: Enroll / Renew / Revoke**

- **Issue:** Enrollment > Generate Certificate (or CSR enrollment) → select the EJBCA CA + template → Submit. CertSecure calls EJBCA REST to issue.
- **Renew / Revoke:** performed from Inventory as with other CAs.

## Troubleshooting

| Symptom | Likely Cause | Fix |
|---|---|---|
| CA type greyed out | Entitlement/feature flag not enabled | Confirm license for EJBCA |
| 401 / 403 | Client cert not authorized, or End Entity Profile access rule | Check EJBCA admin roles and profile access |
| Enrollment rejected | Subject/SAN violates Certificate Profile constraints | Align template with the EJBCA profile |
| TLS error | EJBCA server / client cert chain not trusted | Fix trust stores on both ends |