HashiCorp Vault – Certificate Lifecycle Management (CLM) Integration Guide

Overview

This guide describes how to integrate a HashiCorp Vault PKI secrets engine with CertSecure Manager as an agentless CA connector, enabling end-to-end certificate lifecycle management — mount configuration, PKI role discovery, issuance, renewal, and revocation — with automatic ingestion and synchronization of issued certificates into the CertSecure inventory, including ownership transfer.

Note: Unlike the agent-based connector, Vault is integrated over its HTTP API. There is no ISO installer or connector service to deploy on a separate host — the CA is configured entirely from the CertSecure UI.

Prerequisites

- CertSecure Manager frontend and backend are fully operational.
- Your CertSecure Manager account has the "Manage Certification Authorities" permission.
- A reachable HashiCorp Vault cluster with the PKI secrets engine enabled at a known mount path, backed by a signing/intermediate CA.
- At least one PKI role configured on the mount (roles define allowed domains, key type/size, and TTL).
- A Vault auth credential for CertSecure — a token or AppRole bound to a policy permitting the required PKI operations (see below).
- Network connectivity from the CertSecure backend to the Vault API (default TCP 8200 / HTTPS).
- The Vault API address, PKI mount path, and namespace (Vault Enterprise only, if used).

Access Requirements

Item	Requirement / Value
Vault API	HTTPS, default TCP 8200 (reachable from CertSecure backend)
Auth method	Token or AppRole (`role_id` / `secret_id`)
PKI mount path	e.g. `pki_int`
Namespace	Vault Enterprise only (optional)
TLS trust	Vault server certificate must be trusted by the CertSecure backend

Minimum Vault Policy for the CertSecure Credential

Grant only what the CLM connector calls:

```
# certsecure-pki.hcl
path "<mount>/roles" { capabilities = ["list"] }
path "<mount>/roles/*" { capabilities = ["read"] }
path "<mount>/issue/*" { capabilities = ["create","update"] }
path "<mount>/revoke" { capabilities = ["create","update"] }
path "<mount>/certs" { capabilities = ["list"] }
path "<mount>/cert/*" { capabilities = ["read"] }
path "<mount>/config/urls" { capabilities = ["read"] }
```

Note: Confirm the exact paths/capabilities above against the connector's actual API calls before publishing this guide externally.

Configuration Steps

Step 1: Prepare the Vault PKI Secrets Engine

- Confirm the PKI engine is enabled at the mount and a signing/intermediate CA is configured.
- Confirm at least one PKI role exists — CertSecure lists these roles for template binding and enrollment.

CLI reference:

```
vault secrets enable -path=pki_int pki
vault list pki_int/roles
vault read pki_int/roles/<role>
```

Step 2: Create the CertSecure Auth Credential in Vault

- Apply the policy above, then issue a token or configure an AppRole for CertSecure.

```
vault policy write certsecure-pki certsecure-pki.hcl

# Option A — periodic token
vault token create -policy=certsecure-pki -period=768h

# Option B — AppRole (recommended for unattended renewal)
vault auth enable approle
vault write auth/approle/role/certsecure token_policies=certsecure-pki \
  token_period=768h
vault read auth/approle/role/certsecure/role-id
vault write -f auth/approle/role/certsecure/secret-id
```

Note: Prefer AppRole with a periodic token so the connector can renew unattended without manual token rotation.

Step 3: Add the Vault CA in CertSecure Manager

- Go to Administration > CA Management, click Add CA.
- Choose CA Type: HashiCorp Vault.
- Enter: Display/CA Name, Vault Address (`https://…:8200`), PKI Mount Path, Namespace (if any), Auth Method (Token/AppRole), and the corresponding credential.
- Set Renewal / Sync Interval (e.g. 30 = sync every 30 minutes) → Save.

Step 4: Sync and List PKI Roles

- After the first sync (allow approximately 15–30 minutes, depending on the configured interval), CertSecure lists the Vault PKI roles under the CA.
- Roles become available for template binding and enrollment.

Step 5: Certificate Operations — Issue / Renew / Revoke

- Issue: Enrollment > Generate Certificate → select the Vault CA and a role-bound template → supply subject/SANs → Submit. CertSecure calls Vault's `<mount>/issue/<role>` endpoint and returns the certificate and chain.
- Renew: from Inventory, select the certificate → Renew. CertSecure re-issues through the same role.

- Revoke: select the certificate → Revoke. CertSecure calls `<mount>/revoke` by serial. CRL/OCSP behaviour follows the Vault mount's `config/urls` and CRL settings.

Note: HashiCorp Vault does not expose named certificate templates the way an internal CA does — the PKI role is the policy anchor. CertSecure templates bind to a role so you don't re-enter request details each time.

Troubleshooting

Symptom	Likely Cause	Fix
Roles not listing	Policy missing `list` on `<mount>/roles`, or wrong mount path	Grant `list`; verify the exact PKI mount path.
403 on issue	Policy missing `create` on `<mount>/issue/*`, or role name mismatch	Align policy and role name.
TLS handshake fails	Vault server certificate not trusted by CertSecure backend	Add the Vault CA chain to the backend trust store.
New certs not syncing	Interval too long, or token/AppRole expired	Shorten the interval; renew the AppRole / periodic token.