

# Generate Certificates with Hashicorp Vault

Here are steps to generate SSL certificates using HashiCorp Vault as an Intermediate CA.

NOTE: Be sure that you've setup a vault instance as an Intermediate CA.

See this page for how: [Vault as Intermediate CA](#)

Login to the web UI of your intermediate CA, such as: <https://vault02.ogsofttech.lan:8200/ui/>

If DNS is down, use this: <https://192.168.60.6:8200/ui/>

For the latest intermediate CA url, see this page: [Vault Services](#)

Find the issuing role by navigating to Secrets/PKI/Roles.

Secrets / pki



Overview **Roles** Issuers Keys Certificates Tidy Configuration

Create role +

🔍 [ogsofttech-dot-lan](#)



1-1 of 1 < 1 >

Select the role, and click Generate Certificate:

## PKI Role ogsofttech-dot-lan

	<a href="#">Delete</a> <a href="#">Generate Certificate &gt;</a> <a href="#">Sign Certificate &gt;</a> <a href="#">Edit &gt;</a>
<b>Role name</b>	ogsofttech-dot-lan
<b>Issuer</b>	e7c11c11-15da-d01e-772c-e202b986774c
<b>Issued certificates expire after</b>	4 years 11 months 30 days
<b>Issued certificate backdating</b>	30 seconds
<b>Max TTL</b>	0
<b>Generate lease with certificate</b>	<input checked="" type="checkbox"/> No

Fill in the Common name as: router.ogsofttech.lan.

Set the TTL to 1 year (365 days).

## Generate Certificate

**Common name** ⓘ

ogsofttech.lan

**User ID(s)** ⓘ

Add one item per row.

Add

**Not valid after**

The time after which this certificate will no longer be valid. This can be a TTL (a range of time from now) or a specific date.

**TTL**

43800

hours

**Specific date**

**Format** ⓘ

pem

**Private key format** ⓘ

der

Subject Alternative Name (SAN) Options

Generate

Cancel

Click Generate, to create the key and certificate, and you'll see this:

Secrets / pki / roles / ogsofttech-dot-lan / generate certificate

## View Generated Certificate

Download Revoke certificate

### Next steps

The `private_key` is only available once. Make sure you copy and save it now.

#### Certificate



##### PEM Format

```
-----BEGIN CERTIFICATE-----  
MIIDXCCAk5gAwIBAgIUW0jsUD3Eh9N8iukdKOKG...
```



#### Common name

router.ogsofttech.lan

#### Serial number

58:e8:ec:50:3d:c4:87:d3:7c:8a:e9:1d:28:e2:86:1e:d0:94:f0:fe

#### CA Chain



##### PEM Format

```
-----BEGIN CERTIFICATE-----  
MIID6jCCAtKgAwIBAgIUe5gwYSG4L92F2CJsZWh0...
```



#### Issuing CA



##### PEM Format

```
-----BEGIN CERTIFICATE-----  
MIID6jCCAtKgAwIBAgIUe5gwYSG4L92F2CJsZWh0...
```



#### Private key



##### PEM Format

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEpAIBAACAQEA7kj1Mtj+tJP/cH8csH1m3ifL...
```



#### Private key type

rsa

Download the private key as: router.ogsofttech.lan-key.pem

Download the certificate as: router.ogsofttech.lan-cert.pem

Download the CA chain as: router.ogsofttech.lan-cabundle.pem

**NOTE:** We are calling the downloaded CA chain file a “ca bundle”.

CA bundle is the standard naming convention for this file type.

Specifically, a cert is often concatenated with the CA bundle that signed it, to create a chain certificate file.

Now, you can copy the cert, ca bundle, and private key to the host, for usage.

If generating a pair for a linux host, you will need them as .crt and .key files.

Follow this: [Converting PEM to crt and key](#)

If generating a pair for an Nginx host, you will need

---

Revision #6

Created 1 September 2025 01:36:18 by glwhite

Updated 4 September 2025 03:24:34 by glwhite