

Vault as Root CA

Here are steps you can follow to setup a vault instance as a Root CA.

NOTE: This page assumes that you have created a single-node vault instance to serve as your Root CA.

See this page for how to do that: [Hashicorp Vault Setup](#)

NOTE: These steps will create a root CA with one signing key.

You should create an intermediate CA, as well, that will perform the actual signing of certs. This will allow you to offline this root CA, once the intermediate CA is up.

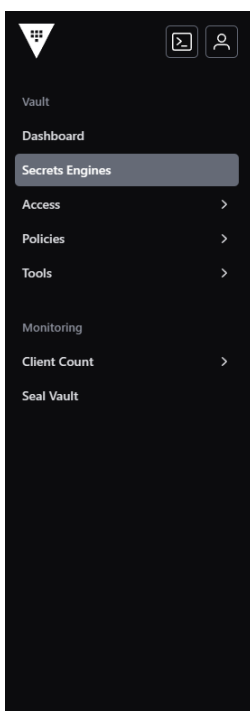
Starting the PKI Engine

NOTE: From here down, is steps for creating a Root CA.

If you are setting up an Intermediate CA, skip to 'Configure Intermediate CA'.

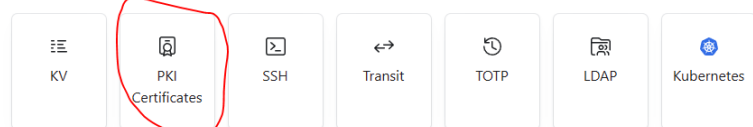
For Vault to serve as a root CA, you have to add the PKI secrets engine.

To do this, enable the pki secrets engine:

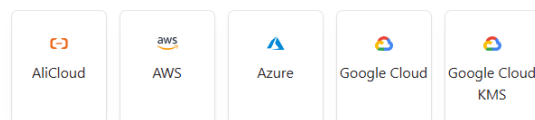


Enable a Secrets Engine

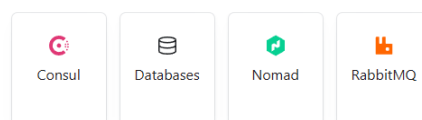
Generic



Cloud



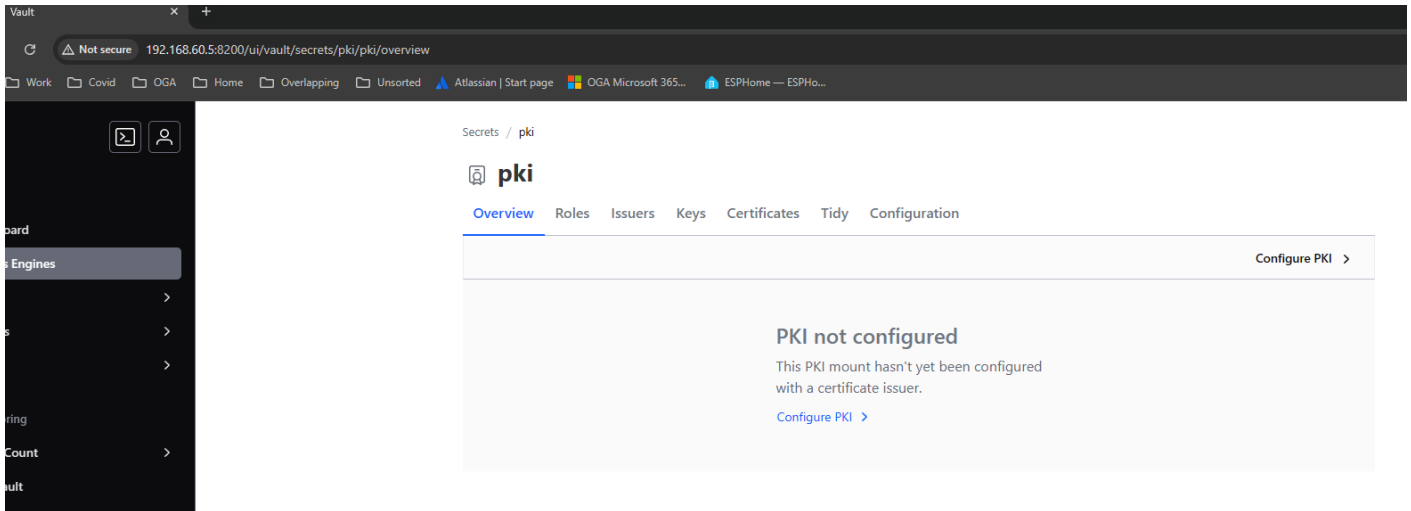
Infra



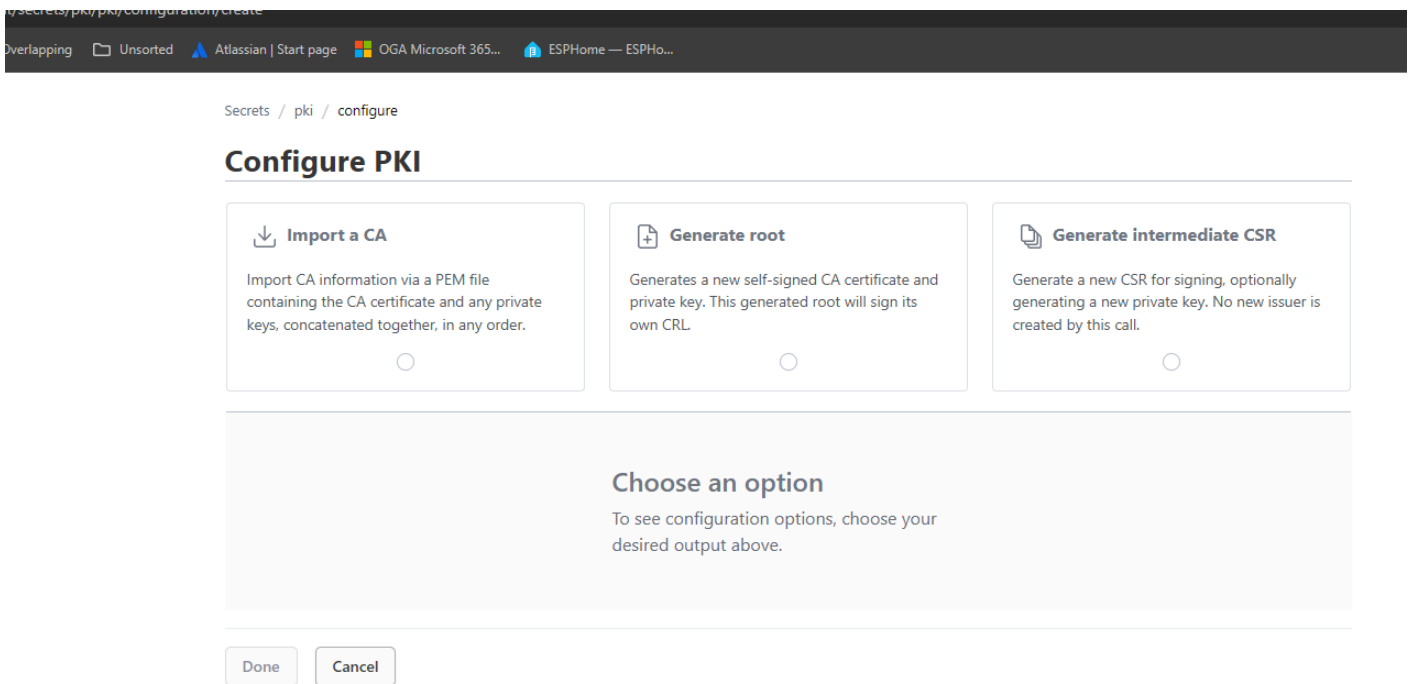
Cancel

For a Root CA, set the Max lease time to as long as possible, as the root CA will be offlined after generation.

Once initialized, it will look like this:



For a root CA, click Configure PKI to begin setup.



Choose the Generate Root option.




Set Type to Internal.

Set your Common name. Usually, this is a domain with a private TLD suffix.

Set the issuer name.

Set a TTL that is maxed out: 87600 hours.

Configure PKI

<p> Import a CA</p> <p>Import CA information via a PEM file containing the CA certificate and any private keys, concatenated together, in any order.</p> <p><input type="radio"/></p>	<p> Generate root</p> <p>Generates a new self-signed CA certificate and private key. This generated root will sign its own CRL.</p> <p><input checked="" type="radio"/></p>	<p> Generate intermediate CSR</p> <p>Generate a new CSR for signing, optionally generating a new private key. No new issuer is created by this call.</p> <p><input type="radio"/></p>
---	---	---

Root parameters

Type

internal ▼

Common name

ogsofttech.lan

Issuer name

leewhite187@gmail.com

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

87600 hours ▼

Specific date

Backdate validity

Also called the not_before_duration property. Allows certificates to be valid for a certain time period before now. This is useful to correct clock misalignment on various systems when setting up your CA.

Scroll down and fill in the issuer URLs, matching the origin for your root CA host:

Format

pem

Permitted DNS domains

Max path length

-1

- ✓ [Key parameters](#)
- ✓ [Subject Alternative Name \(SAN\) Options](#)
- ✓ [Additional subject fields](#)

Issuer URLs

Issuing certificates

The URL values for the Issuing Certificate field; these are different URLs for the same resource. Add one item per row.

http://192.168.60.5/v1/pki/ca

Add

CRL distribution points

Specifies the URL values for the CRL Distribution Points field. Add one item per row.

http://192.168.60.5/v1/pki/crl

Add

OCSP Servers

Specifies the URL values for the OCSP Servers field. Add one item per row.

http://192.168.60.5/v1/pki/ocsp





Add

Enable templating ⓘ

When finished, click Done, to generate the root CA key and certificate.

You will see a page like this:

View Root Certificate

<div style="background-color: #f0f0f0; height: 20px;"></div>	
Certificate	<div style="border: 1px solid #ccc; padding: 5px;">  PEM Format -----BEGIN CERTIFICATE----- MIIDPjCCAiaGAwIBAgIUH8d4nnRBH7Ntb+0NYXw3... </div>
Common name	ogsofttech.lan
Issuer ID	 2c371efc-4c5e-71b1-f61d-6fb0c6a57bc4
Issuer name	leewhite187
Issuing CA	<div style="border: 1px solid #ccc; padding: 5px;">  PEM Format -----BEGIN CERTIFICATE----- MIIDPjCCAiaGAwIBAgIUH8d4nnRBH7Ntb+0NYXw3... </div>
Key ID	 5608f114-66d2-40f9-9d19-682e2b6e46e2
Serial number	1f:c7:78:9e:74:41:1f:b3:6d:6f:ed:0d:61:7c:37:a8:9a:b1:dd:91
Private key	internal
Private key type	internal
Key usage	CertSign, CRLSign
Subject Alternative Names (SANs)	ogsofttech.lan

Copy out the root CA certificate, and save it to a file, named: `ogsofttech.lan_ca.crt`

Install it on all machines of the local network, so they will recognized the signed SSL certs of hosts.

Current Intranet Root CA Certificate

The current root CA for the local intranet can be found in the secure share at this path:

```
\SecureShare git\oga\ogsofttech.lan\rootCA
```

NOTE: This certificate should be installed on any host that will consume services signed by the root ca.

See this page for how to install it on an Ubuntu host: [How to Add Root CAs to Ubuntu](#)

Root CA Rotation

To make things easier, when it comes time to rotate your root CA key, add a role, now.

Click PKI.

Click Roles.

Click Create Role.

Give the new role a name that you will recognize as the root CA rotation role: CA_rotation_role

Leave the rest of the fields empty, and click Create.

Now, you have a working root CA key/cert for your network.

We will use it to sign the certificate of an Intermediate CA, that will do all the actual work.

And, we will offline the root CA.

Revision #7

Created 4 September 2025 02:55:37 by glwhite

Updated 23 September 2025 00:18:12 by glwhite