



HashiCorp

# Vault PKI Secret Engine

1

## Enable the PKI Secret Engine



2

## Enable the Engine

### Enable PKI Certificates Secrets Engine

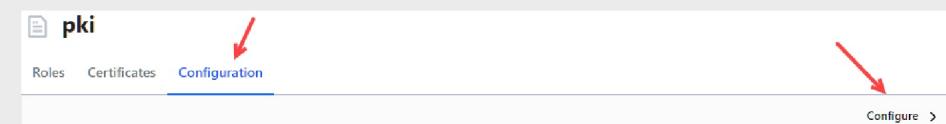
Path: pki

Method Options:

[Enable Engine](#) [Back](#)

3

## Configure the ROOT CA



## Configure PKI

[CA certificate](#) [URLs](#) [CRL](#) [Tidy](#)

This is the default CA certificate used in Vault. It is

[Configure CA](#)

[Set signed intermediate](#)



HashiCorp

# Vault PKI Secret Engine

4

## Configure CA Certificate

### Configure CA Certificate

**CA Type**

root

 Upload PEM bundle**Type**

internal

**Common name**

myvault.com

**Options****Address Options****Save****Cancel**

5

## Configure the TTL

[^ Hide Options](#)**DNS/Email Subject Alternative Names (SANs)****IP Subject Alternative Names (SANs)** TTL

Lease will expire after

87600

hours



After TTL Configuration click on  
save

6

## Configure the URL

[CA certificate](#) [URLs](#) [CRL](#) [Tidy](#)**Issuing certificates**<https://192.168.50.102:8200/v1/pki/ca>**CRL Distribution Points**<https://192.168.50.102:8200/v1/pki/crl>

enter the your vault server ip  
address



HashiCorp

# Vault PKI Secret Engine

7

create role

pki

Roles Certificates Configuration

Create role +

7.1

## Create a PKI Role

**Role name** ⓘ

myvault.com

**Key type** ⓘ

rsa

7.2

 Max TTL

Lease will expire after

0.02

hours



7.3

 Allow localhost ⓘ Allow bare domains ⓘ Allow subdomains ⓘ Allow glob domains ⓘ**Allowed domains** ⓘ

myvault.com



HashiCorp

# Vault PKI Secret Engine

8

## Generate Certificate

**PKI Role** myvault.com

[Delete role](#)[Generate Certificate >](#)

8.1

< pki < creds < myvault.com

### Issue Certificate

**Common name**

**Format**

**Options**

**Generate** **Cancel**

8.2

< pki < creds < myvault.com

### Issue Certificate

**Warning**  
You will not be able to access this information later, so please copy the information below.

<b>Certificate</b>	
<b>Common name</b>	server1.myvault.com
<b>Issuing CA</b>	
<b>Private key</b>	
<b>Private key type</b>	rsa
<b>Issue date</b>	Apr 12, 2022 11:38:18 AM
<b>Expiration date</b>	Apr 15, 2022 11:38:47 AM
<b>Serial number</b>	01:3d:d4:6f:ef:a3:d5:d9:ae:63:aa:2d:8a:62:e5:3b:d5:ce:fb:bc

**Copy credentials** **Back**



HashiCorp

# Vault PKI Secret Engine

9

## Configure the Intermediate CA



9.1

## Enable PKI Certificates Secrets Engine

Path

pki\_int

Method Options

Enable Engine

Back



Configure &gt;

9.2

## pki\_int

Roles Certificates Configuration



Configure &gt;

9.3

## Configure PKI

CA certificate URLs CRL Tidy

This is the default CA certificate used in Vault. It is not used for self-signed certificates or if you

Configure CA

Set signed intermediate





HashiCorp

# Vault PKI Secret Engine

9.4

Configure the Intermediate CA

9.5

Copy CSR

## Configure CA Certificate

**CA Type**

intermediate

 Upload PEM bundle**Type**

internal

**Common name**

myvault.com

[Options](#)[Address Options](#)**Save****Cancel**

## Configure PKI

[CA certificate](#)   [URLs](#)   [CRL](#)   [Tidy](#)

## Configure CA Certificate

**CSR****Common name**

myvault.com

[Copy CSR](#)[Back](#)



HashiCorp

# Vault PKI Secret Engine

10

copy CSR and visit root CA and paste CSR

The screenshot shows the 'Configure PKI' page with the 'Sign intermediate' tab selected. The 'CSR' section contains a large text area with a CSR (Certificate Signing Request) in PEM format. A red arrow points from the top-left towards this area. Another red arrow points from the bottom-left towards the 'Format' dropdown menu, which is set to 'pem\_bundle'. A third red arrow points from the bottom-left towards the 'TTL' input field, which contains the value '43800' and has a dropdown menu next to it. The 'Common name' and 'Use CSR values' fields are also visible.

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICChCCAwFjEUMBIGA1UEAxMLbXI2YXVsdC5jb20wggEiMA0GCSqGSIb3  
DQEBAQAAAIBDwAwggEKAoIBAQCkjdsZ1hHPvZ6lw62HHBUrW2YyckNs8CotbuFd  
Iew8T+/DeoYCSKEpacSSZrlinSf1Yflu+JOOBjNscqmdXStS6ICxNsAuCwAZt26  
qNS4u4rJQdLy4zjF02P6Doh8K572vAQydSPVlq3caAswIH12+2/cx585k/tizQPD
```

after these steps one more certificate generate please copy it sign the intermediate



HashiCorp

# Vault PKI Secret Engine

10.2

## Set Signed Intermediate

< pki\_int

### Configure PKI

View backend >

CA certificate URLs CRL Tidy

This is the default CA certificate used in Vault. It is not used for self-signed certificates or if you have a signed intermediate CA certificate with a generated key.

Replace CA Sign intermediate Set signed intermediate

< pki\_int

### Configure PKI

View backend >

CA certificate URLs CRL Tidy

This is the default CA certificate used in Vault. It is not used for self-signed certificates or if you have a signed intermediate CA certificate with a generated key.

[Download CA Certificate in PEM format](#)

[Download CA Certificate in DER format](#)

[Download CA Certificate Chain](#)

Replace CA Sign intermediate Set signed intermediate

< pki\_int

### Configure PKI

CA certificate URLs CRL Tidy

#### Set signed intermediate

Submit a signed CA certificate corresponding to a generated private key.

**Signed Intermediate Certificate**

```
K7VmeRB306tS5NIs4XAwGjSoiBX/3NCaVsf5H8tLy4xPtfhZInpUIMGNklZY6KN  
C+ilwGA9DJP5FdmOSJ3Y6gonr/qh2Pj8vV5rFAOyEmkrywzB/1gA9cn1GA8vWMan  
A8xO5OWUhluID0igCQW1tdBjvJRe3QMK/akid4WpbQEJzg/FbDT3xlAS92Ezd+T  
MJ+fsT1f6wQtV6k5Pg+9rB+6FMX5fgJX6CC3elZb2rfS4VV6Pqxh  
-----END CERTIFICATE-----
```

Save Cancel

Certificate are generated

Add your text here



HashiCorp

# Vault PKI Secret Engine

11

## Download ROOT CA and Intermediate CA Certificate In Import to ROOT and Intermediate Authority

### ROOT CA Certificate

< pk1

#### Configure PKI

CA certificate   URLs   CRL   Tidy

This is the default CA certificate used in Vault. It is not used for self-signed certificates.

[Download CA Certificate in PEM format](#)

[Download CA Certificate in DER format](#)

[Replace CA](#)   [Sign intermediate](#)   [Set signed intermediate](#)

### Intermediate Certificate

< pk1\_int

#### Configure PKI

CA certificate   URLs   CRL   Tidy

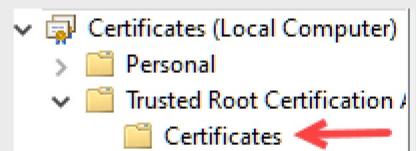
This is the default CA certificate used in Vault. It is not used for self-signed certificates.

[Download CA Certificate in PEM format](#)

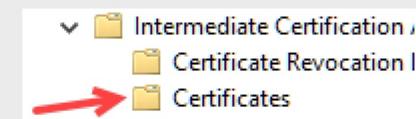
[Download CA Certificate in DER format](#)

[Download CA Certificate Chain](#)

[Replace CA](#)   [Sign intermediate](#)   [Set signed intermediate](#)



Import In window Certificate store





HashiCorp

# Vault PKI Secret Engine

12

Visit pki\_int/role click on generate certificate

The screenshot shows the HashiCorp Vault UI for the PKI Secret Engine. The URL path is visible in the top left: <secrets < pki\_int. A red arrow points to the 'pki\_int' part of the path. The main title is 'pki\_int'. Below it, there are three tabs: 'Roles' (which is selected and highlighted in blue), 'Certificates', and 'Configuration'. A search bar labeled 'Filter roles' is present. On the right side, there is a 'Create role +' button and a three-dot menu icon. In the center, a list item for 'myvault.com' is shown, with a red arrow pointing to its name. To the right of this list item is a vertical ellipsis menu with options 'Generate certificate' and 'Sign certificate', each preceded by a red arrow. At the bottom left, a callout box contains the text 'Rolename'.

Rolename



HashiCorp

# Vault PKI Secret Engine

13

## Generate the Certificate for the Website

```
vault write pki_int/issue/myvault.com ttl=31556952 common_name="server1.myvault.com" ip_sans="192.168.50.106" -format=json > client_certs.json
```

Note You Must install jq before execute command make Seperate folder and do these step to avoid confustion

```
cat client_certs.json | jq -r '.data.certificate' > client-cert.pem  
cat client_certs.json | jq -r '.data.private_key' > client-key.pem  
cat client_certs.json | jq -r '.data.issuing_ca' > ca.pem  
cat client_certs.json | jq -r '.data.ca_chain[]' > ca_chain.pem
```

Generate the pfx for windows server

```
openssl pkcs12 -export -in client-cert.pem -inkey client-key.pem -out certificate.pfx -certfile ca_chain.pem
```

Generate the pfx for windows server

copy generated pfx to windows server



HashiCorp

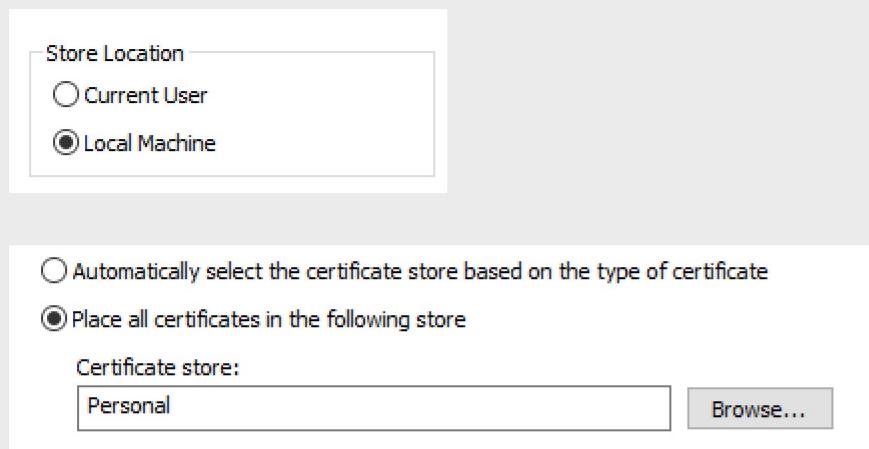
# Vault PKI Secret Engine

13

Bind the certificate in the IIS server

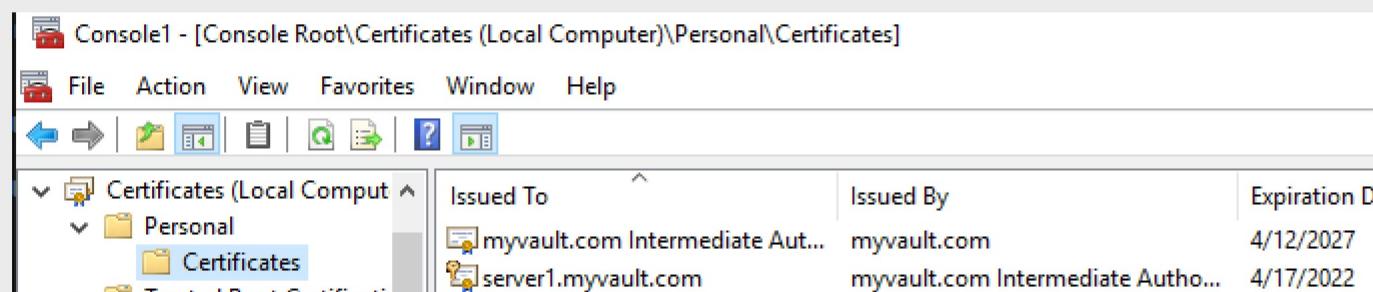
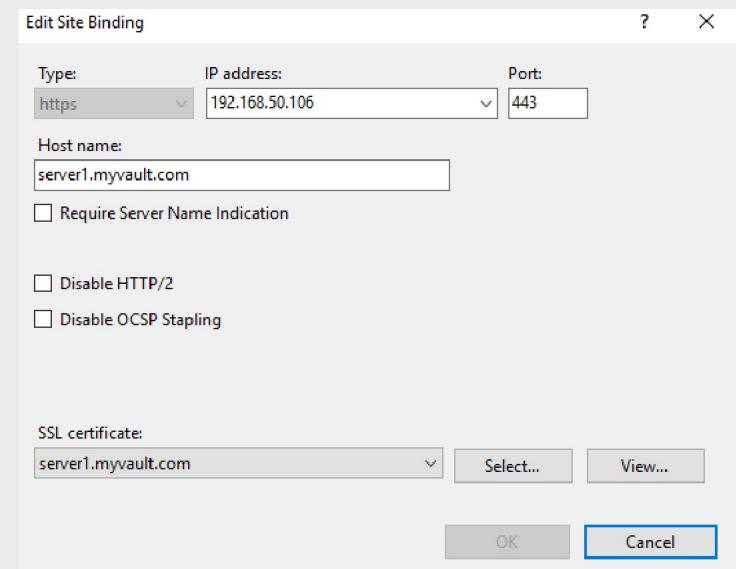
13.1

Install the certificate.pfx by double click



13.2

Bind the certificate in IIS



Make Entry in etc/hosts 192.168.50.106 server.myvault.com



HashiCorp

# Vault PKI Secret Engine

13

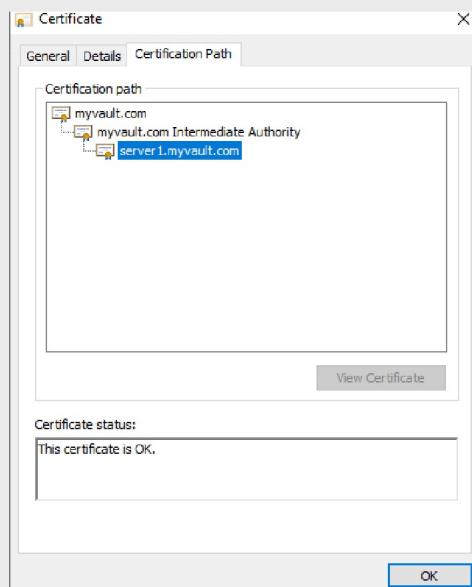
Bind the certificate in the IIS server

13.3

entry in /etc/hosts

Make Entry in etc/hosts 192.168.50.106 server.myvault.com

machine which try to access the website should have  
ROOT CA and Intermediate CA Certificate Imported  
According to Page Number 9



13.4

Access the Website

