**✅ Manual Certificate Installation on Cisco vEdge via Local CA Server**

**📘 Introduction:**

In Cisco SD-WAN deployments, every vEdge router must possess a **valid identity certificate** signed by a trusted **Certificate Authority (CA)**. This certificate allows the vEdge to securely join the SD-WAN fabric and authenticate with vBond/vSmart.

This guide describes the **manual certificate installation process** using a **local CA server** and TFTP. It includes downloading the CA root certificate, generating a CSR, signing it using the CA, and installing the signed certificate on the vEdge.

**🔧 Step-by-Step Procedure**

**1️⃣ Download the CA Root Certificate to vEdge**

bash

CopyEdit

tftp -g -r PKI.ca <ca-server-ip>

* -g: Download (get) mode
* -r PKI.ca: Name of the CA certificate file on the CA server
* <ca-server-ip>: IP address of your CA server

✅ This downloads the **root certificate** from your CA to the local vEdge.

**2️⃣ Install the CA Root Certificate on vEdge**

bash

CopyEdit

request root-cert-chain install /home/admin/PKI.ca

✅ This installs the CA’s public certificate into the vEdge trust store.  
It’s required so vEdge can later **verify the signed certificate** issued by this CA.

**3️⃣ Generate the CSR (Certificate Signing Request) on vEdge**

bash

CopyEdit

request csr upload /home/admin/csr.txt

✅ This generates a new CSR file (csr.txt) which includes:

* vEdge's public key
* Identity info (like system IP, UUID, org)

**4️⃣ View and Copy the CSR Content**

bash

CopyEdit

more /home/admin/csr.txt

✅ Use this command to **open and copy** the CSR content.  
You will **paste it into the CA server** in the next step.

**5️⃣ On the CA Server: Sign the CSR**

On the CA server, enter:

bash

CopyEdit

crypto pki server <server-name> request pkcs10 terminal

✅ After you paste the CSR content, press Enter.  
The CA will generate a **signed certificate** and print it to the terminal.

🔁 Copy this **signed certificate output**.

**6️⃣ On vEdge: Create a File for the Signed Certificate**

bash

CopyEdit

cat <<"EOF" > /home/admin/cert.txt

<PASTE\_THE\_SIGNED\_CERTIFICATE\_CONTENT\_HERE>

EOF

✅ This saves the signed certificate into a file (cert.txt) on the vEdge.

**7️⃣ Install the Signed Certificate on vEdge**

bash

CopyEdit

request vedge install certificate /home/admin/cert.txt

✅ This installs the final, **CA-signed identity certificate** on vEdge.  
The vEdge can now participate in the SD-WAN control plane securely.

**✅ Summary of Commands (Quick Reference)**

bash

CopyEdit

# Download CA root certificate

tftp -g -r PKI.ca <ca-server-ip>

# Install CA root certificate

request root-cert-chain install /home/admin/PKI.ca

# Generate CSR

request csr upload /home/admin/csr.txt

# View CSR

more /home/admin/csr.txt

# (On CA Server) Sign CSR

crypto pki server <server-name> request pkcs10 terminal

# (Back on vEdge) Save signed certificate

cat <<"EOF" > /home/admin/cert.txt

<PASTE\_SIGNED\_CERT\_HERE>

EOF

# Install signed certificate

Request certificate install home/admin/cert.txt

**Or**

request vedge install certificate /home/admin/cert.txt

Finally use this command to get the certificate

# show certificate serial number   
  
copy the chassis number and serial number and use the below command on both vBond and vManage

# request vedge add chasis-num (put chasis number here ) serial-num (put serial number here)