# **Cisco SD-WAN Automated Certificate Renewal Algorithm**

#### By: Rohan Dev, Consulting Engineer, Customer Experience (CX), Singapore

## Incumbent Process for Certificate Renewal Using 3rd Party Enterprise CA

A diagram of a software application

Description automatically generated

## Setting up 3rd Party (Windows-based) Enterprise CA

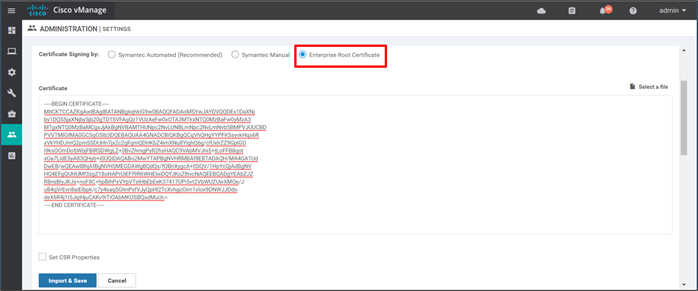
### Setup Windows Virtual Machine

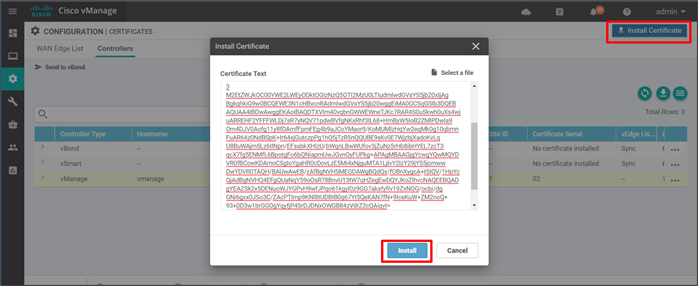
1. Microsoft Windows Server 2022 (64-bit): [Download Windows Server Virtual Machine ISO](https://info.microsoft.com/ww-landing-windows-server-2022.html)
2. [Creating Windows Server VM Reference Link](https://softwarekeep.com/help-center/windows-server-2022-installation-guide-step-by-step)
3. Register/Create VM on VMWare ESXi. The following is for the lab setup:
   1. vCPU: 2
   2. RAM: 8GB
   3. Hard Disk/Storage: 90GB
   4. Ensure that you proceed to install Windows Server 2022 (Desktop Experience) so that you can configure the VM with a GUI
4. Ensure there is a network leg to lab’s default gateway. The following is for the lab setup:
   1. Ethernet 0: inside (LAN), Ethernet 1: VM network (outside)
   2. Default GW: <IP>
   3. Network Mask: /26; 255.255.255.192
   4. Windows VM IPv4 Address: <IP>
5. Setup manual network proxy to point towards Cisco Singapore Office proxy server.

### Setup Windows Certificate Authority Server

1. [Building a Windows Certificate Authority for Lab](https://virtuallythere.blog/2018/04/24/making-things-a-bit-more-secure-part-1/)
2. At this stage, you should have generated the CA’s root certificate.

## Manual Certificate Renewal Procedure

1. [Configure SDWAN vManage with Enterprise Root Certificate Authority (CA)](https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert-deploy-guide.html#Option3EnterpriseRootCertificateAuthorityCA)
   1. Retrieve root certificate from CA server and insert into vManage
   2. 
   3. Verify the root certificate is inside vManage and has been distributed to vSmart and vBond by issuing the following command:   
      show certificate root-ca-cert | include Subject:  
      You should be able to see the CA root certificate inside. The following is for the lab:  
      A screenshot of a computer program

      Description automatically generated
   4. Generate Certificate Signing Request (CSR) from the controllers. Download the .crt file.
2. [Get the Certificate Signing Request (CSR) signed by the Certificate Authority](https://virtuallythere.blog/2018/04/27/making-things-a-bit-more-secure-part-2/)
3. At this stage, you should have exported the signed certificate to the server’s directory.
4. Copy contents of the signed certificate and paste into vManage as shown below:  
   
5. You have successfully installed the signed certificate and the controller has its certificate successfully renewed. The expiration date should have changed.

## Automated Certificate Renewal Process

- SSH into underlay switch first (ssh [admin@20.0.0.250](mailto:admin@20.0.0.250))

- SSH into C8200-R1 SDWAN Router (ssh -l admin -vrf Underlay 20.20.0.1)

1)

Copy root cert from server command:  
ssh into destination device (e.g., C8200)

copy scp://<source\_username>:<source\_password>@<source\_server\_IP>/<filename> bootflash://<filename> (optional: vrf <vrf name/number>)

example command:   
copy scp://admin:admin@20.20.0.2/root\_cert.cer bootflash://root\_cert.cer vrf 20

A screen shot of a computer

Description automatically generated

2)

Uninstall incumbent root-cert-chain inside cEdge router

request platform software sdwan root-cert-chain uninstall

A black background with white text

Description automatically generated

3)

Install new root-cert-chain

request platform software sdwan root-cert-chain install <directory>:<filename>

example command:

request platform software sdwan root-cert-chain install bootflash:root\_cert.cer

A screen shot of a computer

Description automatically generated

4) verify new root-ca-cert installation

example command:

show sdwan certificate root-ca-cert

A screen shot of a computer

Description automatically generated

5)

move file to bootflash/sdwan directory (cos apparently, any other path support will be deprecated)

copy <source\_directory>:<filename> <destination\_directory>

example command:

A screen shot of a computer

Description automatically generated

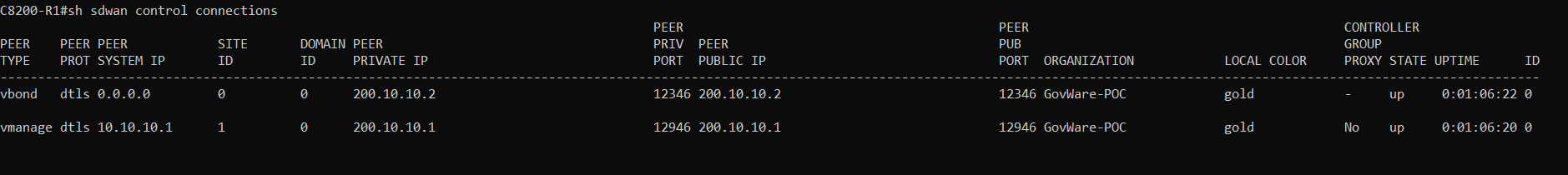
6)   
Assuming all requirements: site-ID, system-IP, organization-name, NTP, VPN0, connectivity, tunnel-interface configuration is present for cEdge to join vManage.

- Notice CSR icon indicating CSR was generated automatically

A screenshot of a computer

Description automatically generated

- Notice cEdge has not established vSmart tunnel



7) View and download CSR

A screenshot of a computer

Description automatically generated