



## Taks1: Setup vManage web management

- Setup IP web management for vManage:

### Console to vManager

```
vmanage login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
Available storage devices:
hdb      100GB
hdc      3GB
1) hdb
2) hdc
Select storage device to use: 1
Would you like to format hdb? (y/n): y
```

**Waiting 5-10min for vManage booting again.**

```
config t
vpn 512
 interface eth0
   ip address 192.168.10.11/24
   no shutdown
!
 ip route 0.0.0.0/0 192.168.10.1
commit
```

If it logs commit failed due to:

**Aborted: values are not unique: eth0**

**'vpn 0 interface eth0 if-name'**

**'vpn 512 interface eth0 if-name'**

→ Let delete eth0 on vpn 0 by command:

```
vpn 0
 no interface eth0
commit
```

Click to User icon -> login vManage web with ip address: 192.168.10.11. Login with account: **admin/admin**

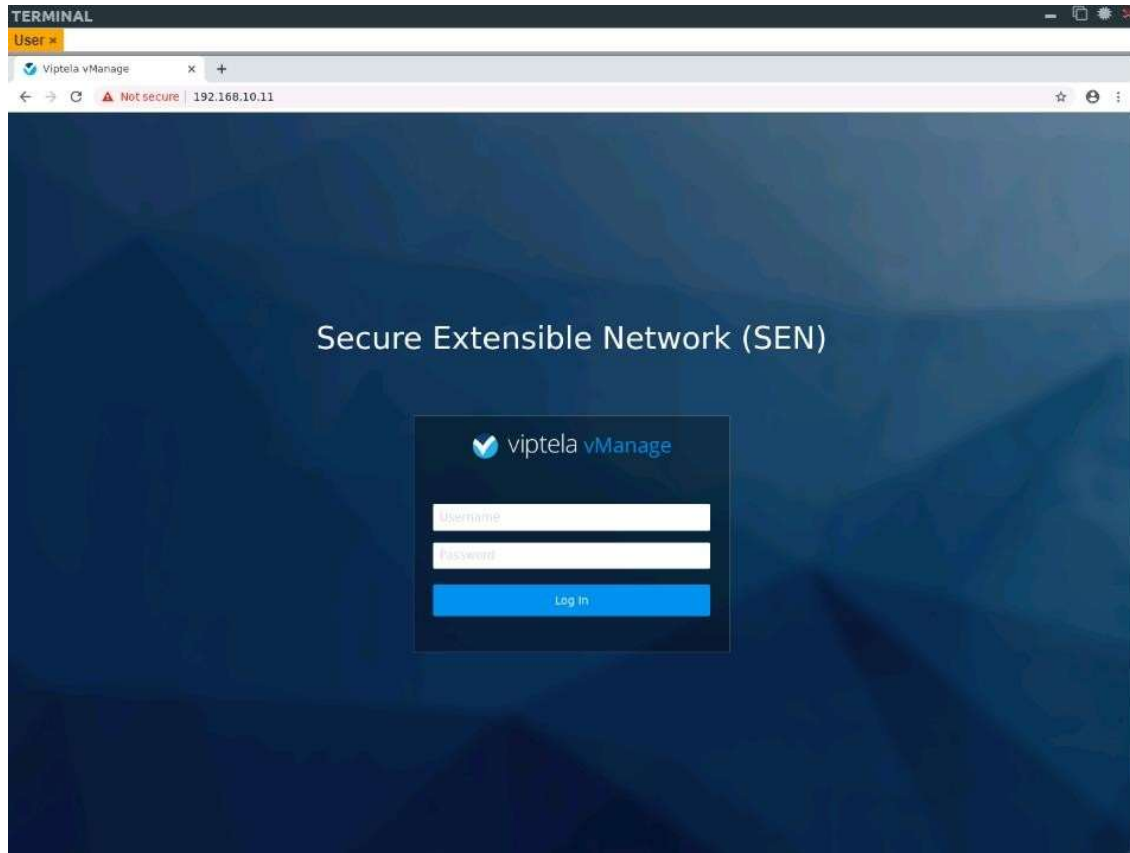
If cant login, login LAN device and verify interface state:

```
LAN>show ip int bri
Interface                IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0      192.168.1.1     YES NVRAM  administratively
down down
GigabitEthernet0/1      192.168.10.1    YES NVRAM  administratively
down down

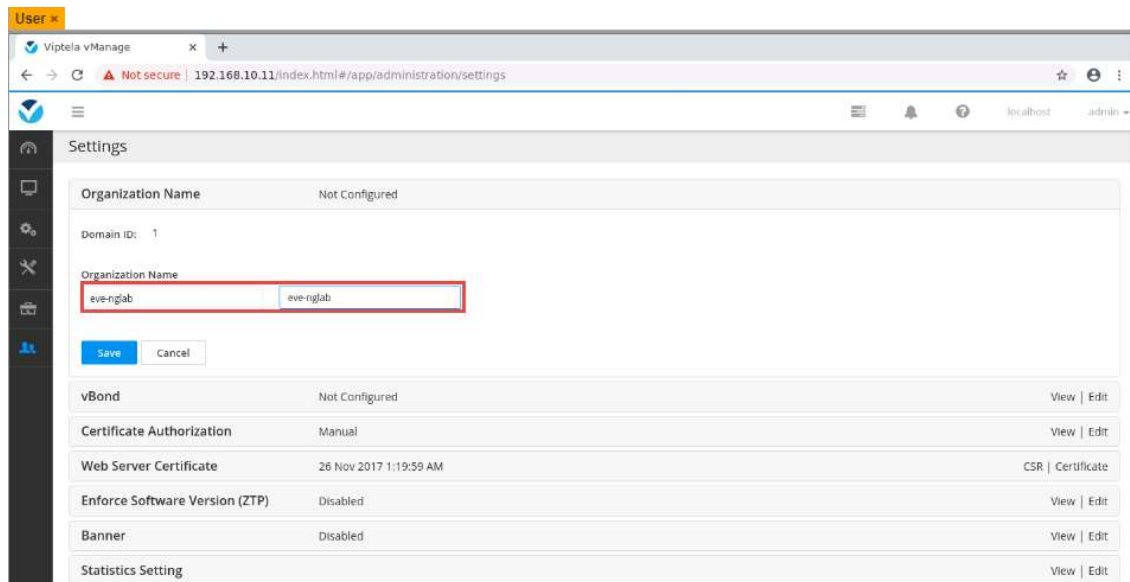
LAN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

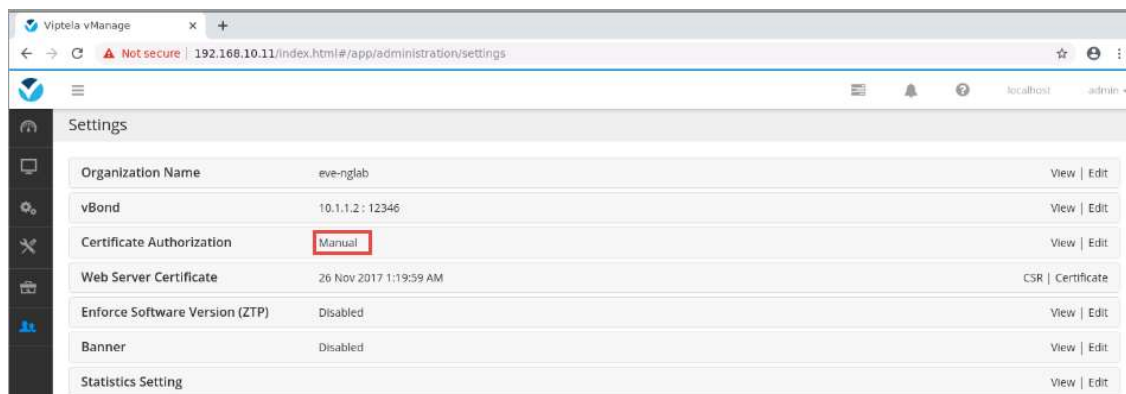
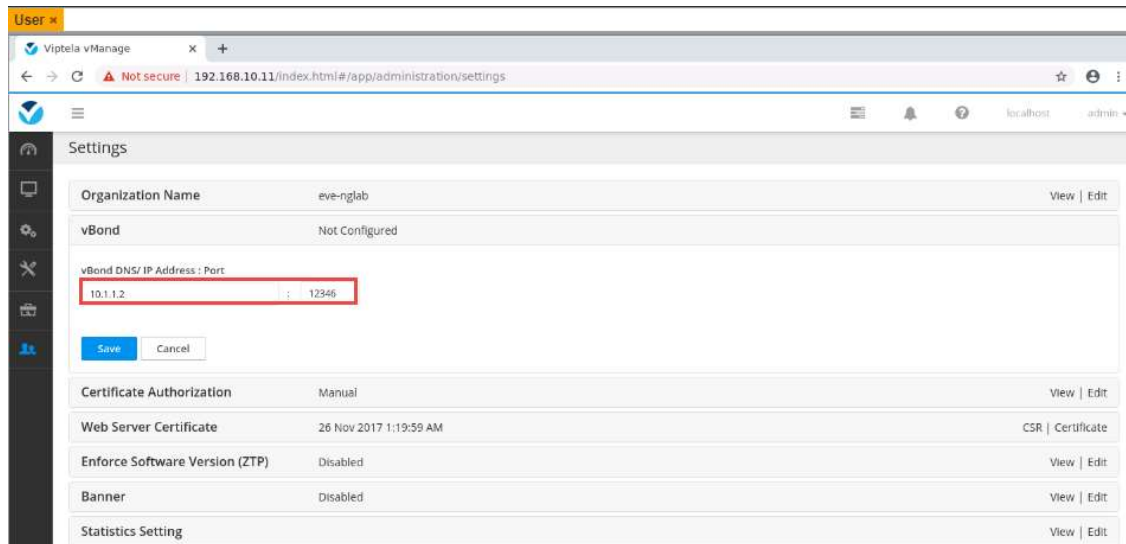
```
LAN(config)#int rang g0/0 - 1  
LAN(config-if-range)#no sh
```

→ Do the same with WAN router.



Go to Administration -> Setting





## **Task2: Lab configuration**

### **- vManage**

```
vmanage# conf t
Entering configuration mode terminal
vmanage(config)# system
vmanage(config-system)# system-ip 1.1.1.1
vmanage(config-system)# site-id 1000
vmanage(config-system)# organization-name "eve-nglab"
vmanage(config-system)# vbond 10.1.1.2
vmanage(config-system)# !
vmanage(config-system)# vpn 0 int eth1
vmanage(config-interface-eth1)# ip add 10.1.1.1/24
vmanage(config-interface-eth1)# no shut
vmanage(config-interface-eth1)# exit
vmanage(config-vpn-0)# ip route 0.0.0.0/0 10.1.1.254
vmanage(config-vpn-0)# !
vmanage(config-vpn-0)# commit and-quit
```

### **- vBond**

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vBond
vedge(config-system)# system-ip 1.1.1.2
vedge(config-system)# site-id 1000
vedge(config-system)# organization-name "eve-nglab"
vedge(config-system)# vbond 10.1.1.2 local vbond-only
vedge(config-system)# !
vedge(config-system)# vpn 512 int eth0
vedge(config-interface-eth0)# ip add 192.168.10.12/24
vedge(config-interface-eth0)# no shut
vedge(config-interface-eth0)# exit
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.10.1
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# vpn 0 int ge0/0
vedge(config-interface-ge0/0)# ip add 10.1.1.2/24
vedge(config-interface-ge0/0)# no shut
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# ip route 0.0.0.0/0 10.1.1.254
vedge(config-vpn-0)# commit and-quit
```

#### - vSmart

```
vsmart(config-vpn-0)# system
vsmart(config-system)# system-ip 1.1.1.3
vsmart(config-system)# site-id 1000
vsmart(config-system)# organization-name "eve-nglab"
vsmart(config-system)# vbond 10.1.1.2
vsmart(config-system)# !
vsmart(config-system)# vpn 512 int eth0
vsmart(config-interface-eth0)# ip add 192.168.10.13/24
vsmart(config-interface-eth0)# no shut
vsmart(config-interface-eth0)# exit
vsmart(config-vpn-512)# ip route 0.0.0.0/0 192.168.10.1
vsmart(config-vpn-512)# !
vsmart(config-vpn-512)# vpn 0 int eth1
vsmart(config-interface-eth1)# no int eth0
vsmart(config-interface-eth1)# ip add 10.1.1.3/24
vsmart(config-interface-eth1)# no shut
vsmart(config-interface-eth1)# exit
vsmart(config-vpn-0)# ip route 0.0.0.0/0 10.1.1.254
vsmart(config-vpn-0)# !
vsmart(config-vpn-0)# commit and-quit
Commit complete.
vsmart#
```

#### - vEdge site 1

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# system-ip 2.1.1.1
vedge(config-system)# site-id 1
```

```
vedge(config-system)# organization-name eve-nglab
vedge(config-system)# vbond 10.1.1.2
vedge(config-system)# vpn 0 int ge0/0
vedge(config-interface-ge0/0)# ip add 172.16.0.2/24
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# ip route 0.0.0.0/0 172.16.0.254
vedge(config-vpn-0)# commit and-quit
```

#### - vEdge site 2

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# system-ip 3.1.1.1
vedge(config-system)# site-id 2
vedge(config-system)# organization-name eve-nglab
vedge(config-system)# vbond 10.1.1.2
vedge(config-system)# vpn 0 int ge0/0
vedge(config-interface-ge0/0)# ip add 172.17.0.2/24
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# ip route 0.0.0.0/0 172.17.0.254
vedge(config-vpn-0)# commit and-quit
Commit complete.
```

### **Task3: Certificate installation**

#### - vManage

```
vmanage# vshell
vmanage:~$ openssl genrsa -out ROOTCA.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
vmanage:~$
```

Created ROOTCA.pem with ROOTCA.key

```
openssl req -x509 -new -nodes -key ROOTCA.key -sha256 -days 1024 \
> -subj "/C=AU/ST=NSW/L=NSW/O=eve-nglab /CN=vmanage.lab" \
> -out ROOTCA.pem
```

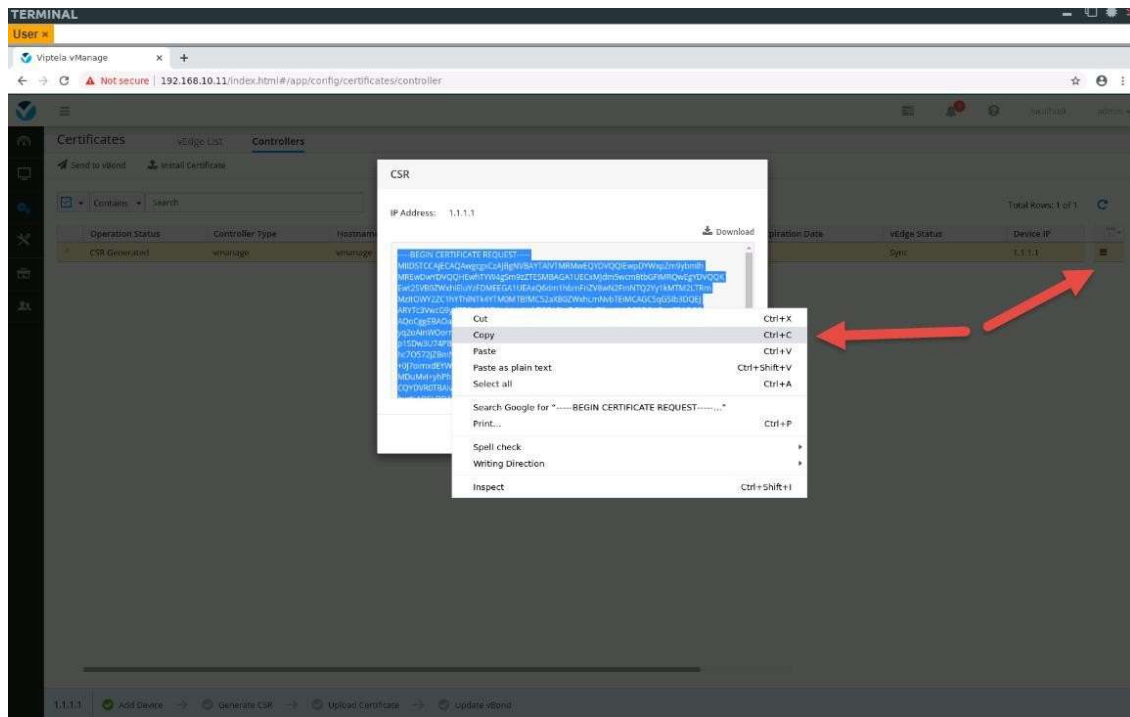
Install ROOTCA.pem

```
exit
vmanage# request root-cert-chain install /home/admin/ROOTCA.pem

Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Successfully installed the root certificate chain
```

Login vManage to create certificate request

Configuration → Certificates → Controllers → vManage → Generate CSR then copy



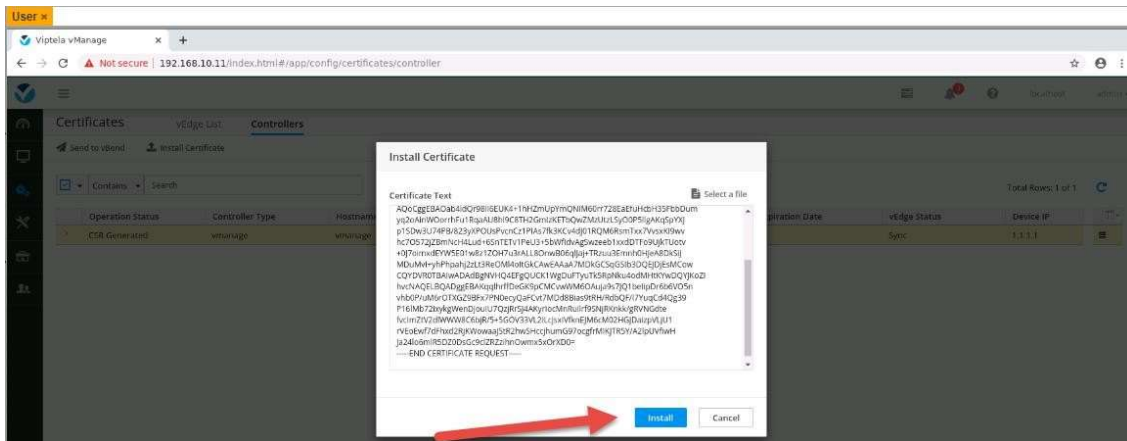
Create **vmanage.crt** with CSR code copy above.  
And create **vmanage.csr** with ROOTCA.key

```
openssl x509 -req -in vmanage.csr \  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \  
-out vmanage.crt -days 500 -sha256
```

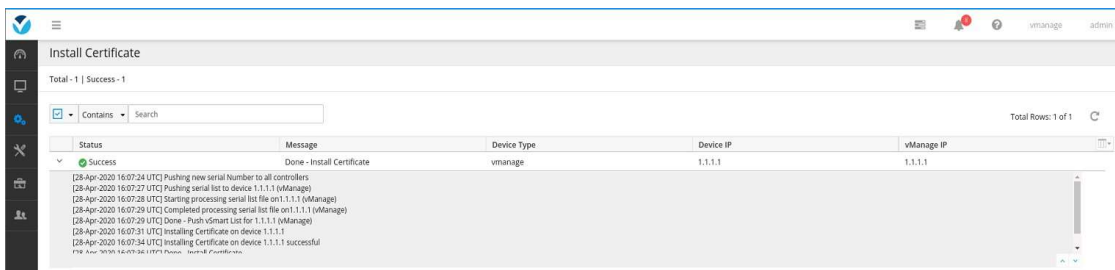
**Result:**

```
Signature ok  
subject=/C=US/ST=California/L=San Jose/OU=eve-nglab/O=vIptela  
Inc/CN=vmanage_07af546c-d136-4f32-9f6d-  
aa8e598a3410_0.viptela.com/emailAddress=support@viptela.com  
Getting CA Private Key
```

Copy content vmanage.crt file by using “cat vmanage.crt” then install certificate on vManage



Configuration → Certificates → Controllers → Install Certificate



- **vBond:**

```

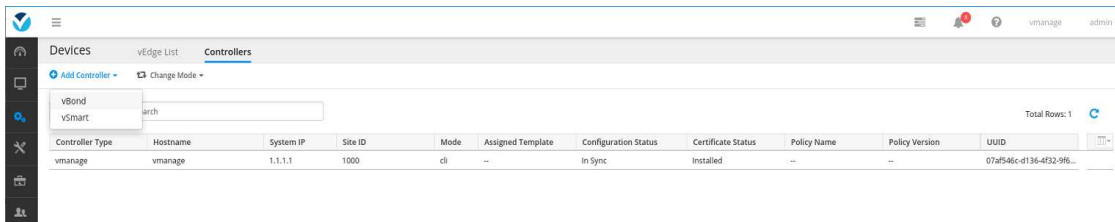
vBond# request root-cert-chain install
scp://admin@192.168.10.11:/home/admin/ROOTCA.pem vpn 512

Result:
Uploading root-ca-cert-chain via VPN 512
Copying ... admin@192.168.10.11:/home/admin/ROOTCA.pem via VPN 512
Warning: Permanently added '192.168.10.11' (ECDSA) to the list of
known hosts.
viptela 16.2.11

admin@192.168.10.11's password:
ROOTCA.pem 100% 1265
1.2KB/s 00:00
Successfully installed the root certificate chain

```

Add vBond to vmanage:



Configuration → Certificates → Controllers → Add Controller:



### Add vBond

vBond Management IP Address

Username

Password

Generate CSR

If vbond adding unsuccessful, lets no tunnel-interface as bellow:

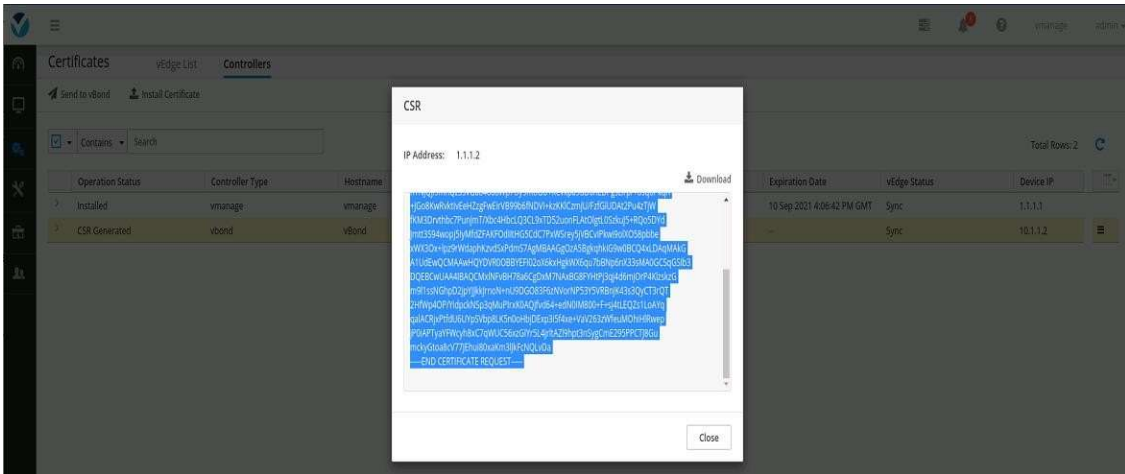
```
vBond# conf t
Entering configuration mode terminal
vBond(config)# vpn 0
vBond(config-vpn-0)# interface ge0/0
vBond(config-interface-ge0/0)# no tunnel-interface
vBond(config-interface-ge0/0)# commit
Commit complete.
vBond(config-interface-ge0/0)#
```

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Configuration Status	Certificate Status	Policy Name	Policy Version	UUID
vmanage	vmanage	1.1.1.1	1000	cli	--	In Sync	Installed	--	--	07af546c-d136-4f32-9f6...
vbond	vbond	1.1.1.2	1000	cli	--	--	Not-installed	--	--	cb05c222-0188-4384-a5...

View vBond CSR:

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	vEdge Status	Device IP
> Installed	vmanage	vmanage	1.1.1.1	1000	BB36DBCE6DF3384F	10 Sep 2021 4:06:42 PM GMT	Sync	1.1.1.1
> CSR Generated	vbond	vbond	1.1.1.2	1000	N/A	--	Sync	10.1.1.2

Configuration → Certificates → Controllers → vBond → View CSR



On vManage, create vbond.csr with content above

**- vManage**

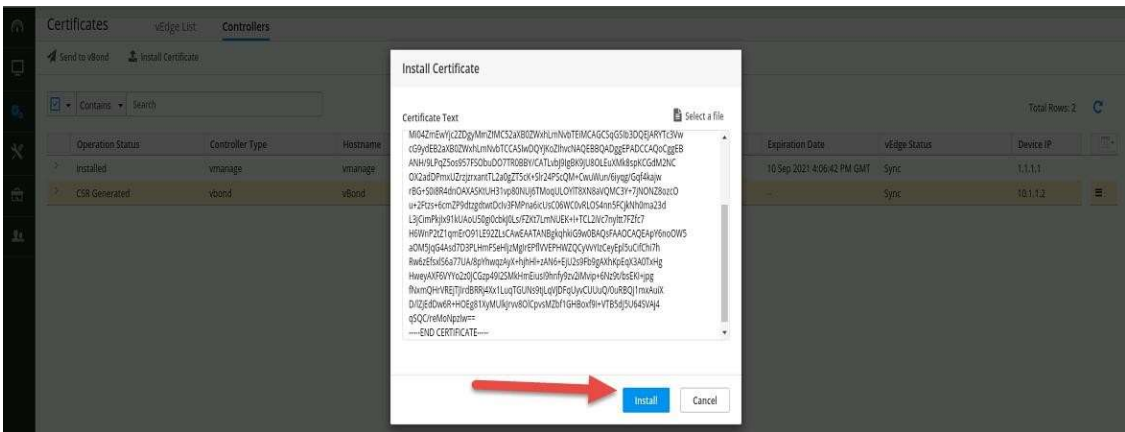
```

openssl x509 -req -in vbond.csr \
> -CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \
> -out vbond.crt -days 500 -sha256

Result:
Signature ok
subject=/C=US/ST=California/L=San Jose/OU=eve-nglab/O=vIptela
Inc/CN=vbond_cdb5c222-0188-4384-a5c2-
8fa0b76d822f_0.viptela.com/emailAddress=support@viptela.com
Getting CA Private Key
vmanage:~$

```

Using “cat vbond.crt” to see file contents then copy and install certificate on vManage web



Configuration → Certificates → Controllers → Install Certificate

Install Certificate

Total - 1 | Success - 1

Contains Search

Total Rows: 1 of 1

Status	Message	Device Type	Device IP	vManage IP
Success	Done - Push vSmart List for 10.1.1.2 (vBond)	vbond	10.1.1.2	1.1.1.1

[28-Apr-2020 16:24:37 UTC] Pushing new serial Number to all controllers  
 [28-Apr-2020 16:24:39 UTC] Installing Certificate on device 10.1.1.2  
 [28-Apr-2020 16:24:41 UTC] Installing Certificate on device 10.1.1.2 successful  
 [28-Apr-2020 16:24:42 UTC] Pushing serial list to device 10.1.1.2 (vBond)  
 [28-Apr-2020 16:24:43 UTC] Starting processing serial list file on 10.1.1.2 (vBond)  
 [28-Apr-2020 16:24:44 UTC] Completed processing serial list file on 10.1.1.2 (vBond)  
 [28-Apr-2020 16:24:44 UTC] Done - Push vSmart List for 10.1.1.2 (vBond)

Send certificate to vBond  
 Configuration → Certificates → Controllers → Send to vBond

Push vSmart List

Total - 2 | Success - 2

Contains Search

Total Rows: 2 of 2

Status	Message	Device Type	Hostname	System IP	Site ID	vManage IP
Success	Done - Push vSmart List for 1.1.1.1 (v...	vmanage	vmanage	1.1.1.1	1000	1.1.1.1
Success	Done - Push vSmart List for 10.1.1.2 (v...	--	--	--	--	1.1.1.1

[28-Apr-2020 16:26:38 UTC] Initiating push serial list  
 [28-Apr-2020 16:26:39 UTC] Pushing serial list to device 1.1.1.1 (vManage)  
 [28-Apr-2020 16:26:40 UTC] Starting processing serial list file on 1.1.1.1 (vManage)  
 [28-Apr-2020 16:26:41 UTC] Completed processing serial list file on 1.1.1.1 (vManage)  
 [28-Apr-2020 16:26:41 UTC] Done - Push vSmart List for 1.1.1.1 (vManage)

[28-Apr-2020 16:26:38 UTC] Initiating push serial list  
 [28-Apr-2020 16:26:39 UTC] Pushing serial list to device 10.1.1.2 (vBond)  
 [28-Apr-2020 16:26:40 UTC] Starting processing serial list file on 10.1.1.2 (vBond)  
 [28-Apr-2020 16:26:41 UTC] Completed processing serial list file on 10.1.1.2 (vBond)  
 [28-Apr-2020 16:26:42 UTC] Done - Push vSmart List for 10.1.1.2 (vBond)

- **vSmart:**

```

vsmart# request root-cert-chain install
scp://admin@192.168.10.11:/home/admin/ROOTCA.pem vpn 512

Result:

Uploading root-ca-cert-chain via VPN 512
Copying ... admin@192.168.10.11:/home/admin/ROOTCA.pem via VPN 512
Warning: Permanently added '192.168.10.11' (ECDSA) to the list of
known hosts.
viptela 16.2.11

admin@192.168.10.11's password:
ROOTCA.pem                               100% 1265
1.2KB/s   00:00
Successfully installed the root certificate chain
  
```

- **Add vSmart to vManage web**

Configuration → Devices → Controllers → Add Controller → vSmart

### Add vSmart

**vSmart Management IP Address**

**Username**

**Password**

**Protocol**      **Port**

DTLS     

Generate CSR

**Add**      **Cancel**

View and copy vSmart CSR  
Configuration → Certificates → Controllers → vSmart → View CSR:

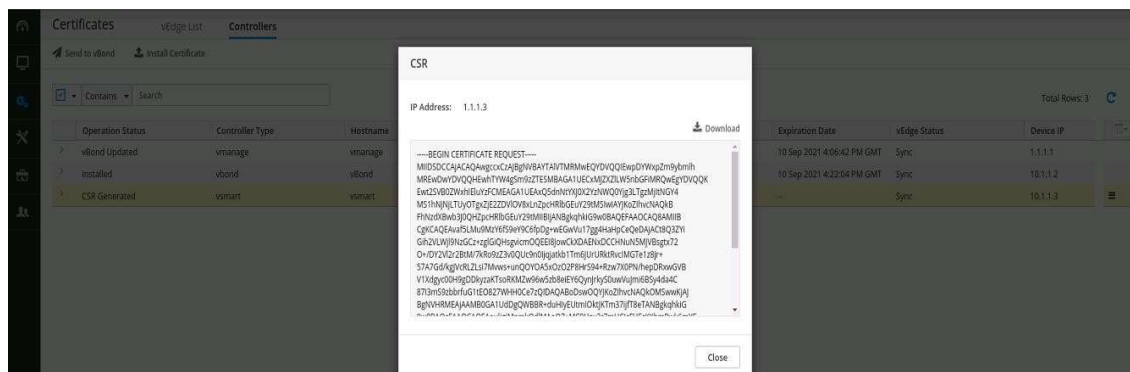
Send to vBond   Install Certificate

Contains   Search

Total Rows: 3

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	vEdge Status	Device IP
> vBond Updated	vmanage	vmanage	1.1.1.1	1000	BB34DBCE6DF3384F	10 Sep 2021 4:06:42 PM GMT	Sync	1.1.1.1
> Installed	vbond	vbond	1.1.1.2	1000	BB34DBCE6DF33850	10 Sep 2021 4:22:04 PM GMT	Sync	10.1.1.2
> CSR Generated	vsmart	vsmart	1.1.1.3	1000	N/A	--	Sync	10.1.1.3

View CSR  
View Certificate  
Generate CSR  
Reset RSA  
Invalidate



Create vsmart.csr file on vManage with contents viewed above.  
Author vsmart.csr with ROOTCA.key

- vManage:

```
openssl x509 -req -in vsmart.csr \
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \
-out vsmart.crt -days 500 -sha256
```

Result:

```
Signature ok
subject=/C=US/ST=California/L=San Jose/OU=eve-nglab/O=vIptela
Inc/CN=vsmart_f35d4b87-8322-4f81-a63c-
52981f16d5e9_1.viptela.com/emailAddress=support@viptela.com
Getting CA Private Key
```

Using “cat vmsart.crt” to see contents and copy then install certificate:

Configuration → Certificates → Controllers → Install Certificate

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	vEdge Status	Device IP
vBond Updated	vmanage	vmanage	1.1.1.1	1000	BB36DBCE6DF3384F	10 Sep 2021 4:06:42 PM GMT	Sync	1.1.1.1
Installed	vBond	vBond	1.1.1.2	1000	BB36DBCE6DF33850	10 Sep 2021 4:22:04 PM GMT	Sync	10.1.1.2
vBond Updated	vsmart	vsmart	1.1.1.3	1000	BB36DBCE6DF33851	10 Sep 2021 4:34:28 PM GMT	Sync	10.1.1.3

- **vEdge:**

on vManage, using “cat ROOTCA.pem” to see contents then create ROOTCA.pem file on vEdge with same contents. Install ROOTCA.pem on vEdge with command:

```
vedge# request root-cert-chain install /home/admin/ROOTCA.pem
```

Result:

```
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Create vedge01.csr file

```
request csr upload /home/admin/vedge01.csr
```

```
Uploading CSR via VPN 0
Enter organization-unit name : eve-nglab
Re-enter organization-unit name : eve-nglab
```

```
Generating private/public pair and CSR for this vedge device
Generating CSR for this vedge device..... [DONE]
Copying ... /home/admin/vedge01.csr via VPN 0
CSR upload successful
```

Using "cat vedge01.csr" to copy contents and create vedge01.csr file on vManage.  
Create vedge01.crt with command below:  
vMange:

```
openssl x509 -req -in vedge01.csr \  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \  
-out vedge01.crt -days 500 -sha256
```

Result:  
Signature ok  
subject=/C=US/ST=California/L=San Jose/OU=eve-nglab/O=vIPTela  
Inc/CN=vedge-368755e1-cfc9-4dbe-984e-9a8d7e3f41f9-  
0.viptela.com/emailAddress=support@viptela.com  
Getting CA Private Key

On vedge01, create vedge01.crt same contents with file on vManage then install with  
command below:

```
vedge# request certificate install /home/admin/vedge01.crt
```

**Result:**  
Installing certificate via VPN 0  
Copying ... /home/admin/vedge01.crt via VPN 0  
Successfully installed the certificate

Check serial number:

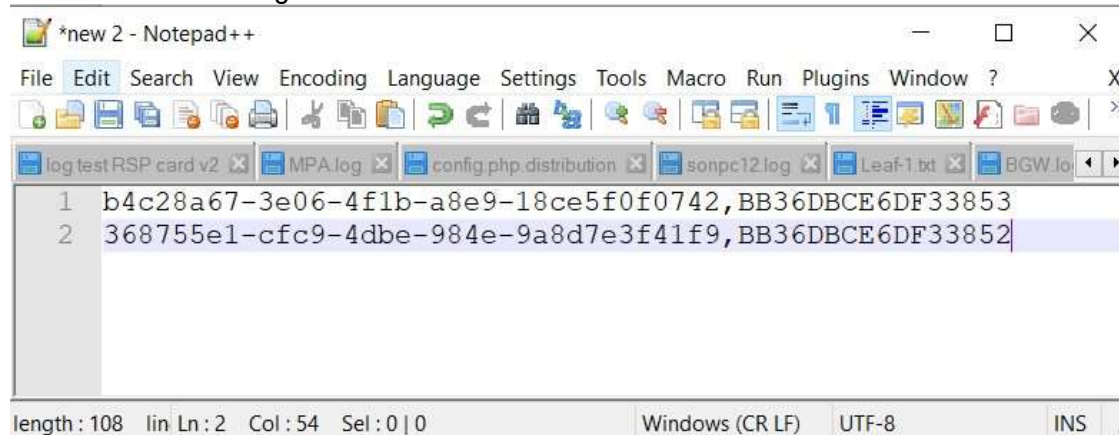
```
vedge# show certificate serial
```

Chassis number: 368755e1-cfc9-4dbe-984e-9a8d7e3f41f9 serial  
number: BB36DBCE6DF33852

Create text file with code:

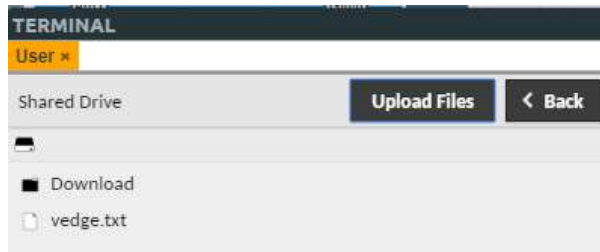
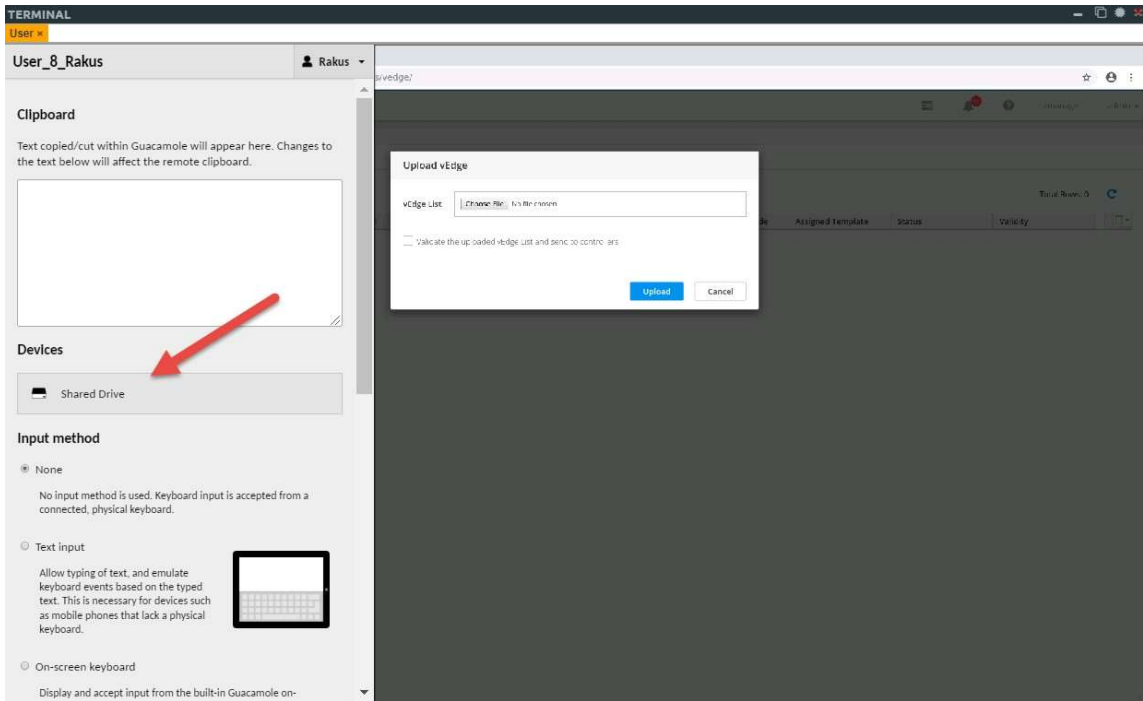
```
368755e1-cfc9-4dbe-984e-9a8d7e3f41f9, BB36DBCE6DF33852
```

Do the same with vedge02. Check serial and add to text file.

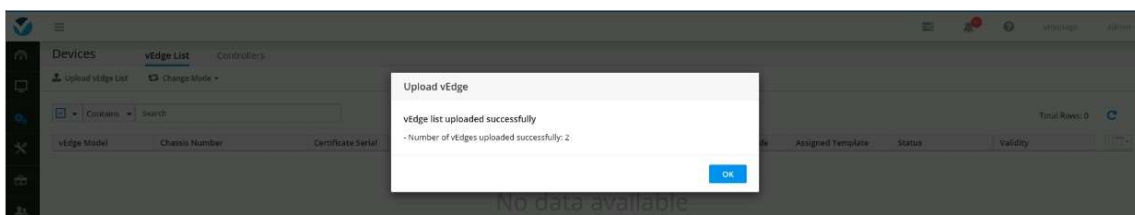
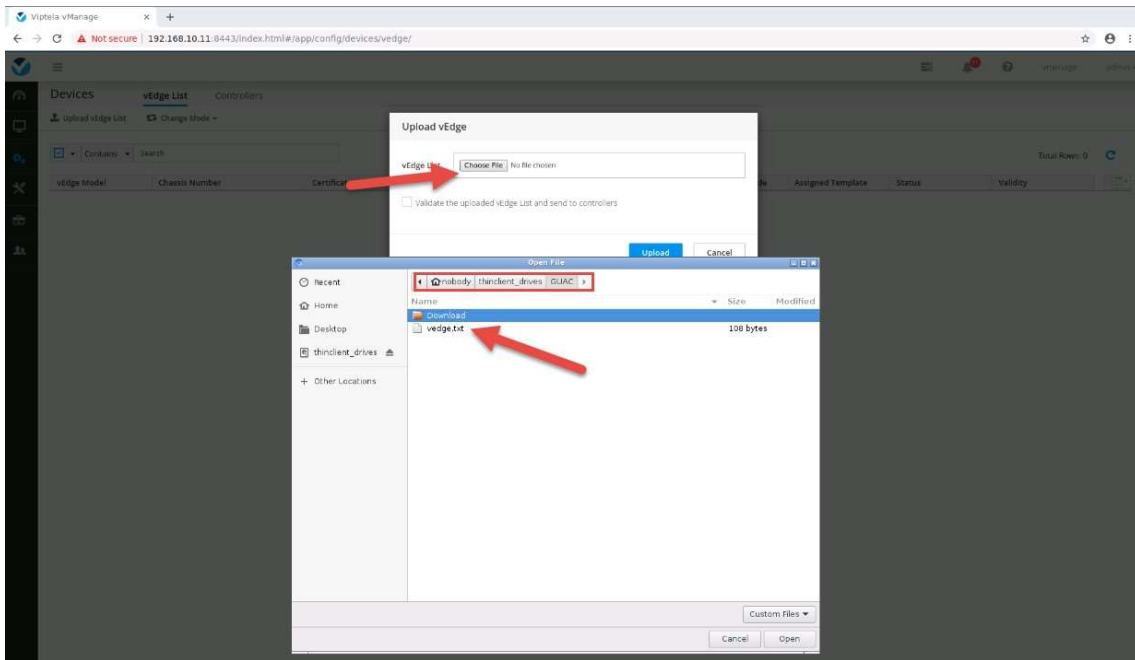


### Task 4: Upload vEdge list

On User PC, press **Ctrl + Shift + ALT** and choose **Shared Driver** -> **Upload file**



Upload vedge file to vManage



Send vedge list to controller  
 Configuration → Certificates → vEdge List → Send to Controllers

**Certificates** vEdge List Controllers

Send to Controllers Click Send to Controllers to sync the vEdge list on all controllers

Chassis Number	Certificate Serial	Hostname	IP Address	Validate
b4c2ba57-3e06-4f1b-89e9-18ce5f0f0742	BB36DC6CFD33853	--	--	invalid   staging   valid
368755e1-efc9-40be-984e-9a8d7e3fa1f9	BB36DC6CFD33852	--	--	invalid   staging   valid

**Push vEdge List**

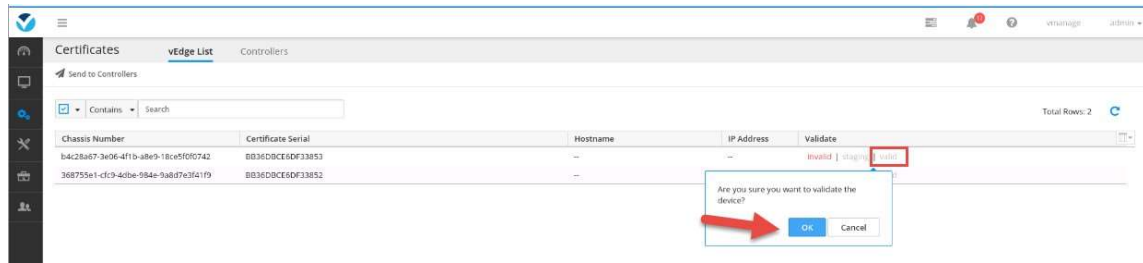
Total: 3 | Success: 3

status	Message	Device type	Hostname	System IP	Site ID	vManage IP
Success	Done - Push vEdge List for 1.1.1.1 (v...	vmanage	vmanage	1.1.1.1	1000	1.1.1.1
Success	Done - Push vEdge List for 10.1.1.2 (L...	--	--	--	--	1.1.1.1
Success	Done - Push vEdge List for 10.1.1.3 (L...	--	--	--	--	1.1.1.1

Validate vEdges

Configuration → Certificates → vEdge List → (vEdge) → Valid





Then send to controller after valid all vedge



### - Configure tunnel

#### vManage/Smart

```
vpn 0
interface eth1
tunnel-interface
```

#### vBond

```
vpn 0
interface ge0/0
tunnel-interface encapsulation ipsec
```

### Task 5: Verification:

