SD-WAN CONTROL and DATA PLANE

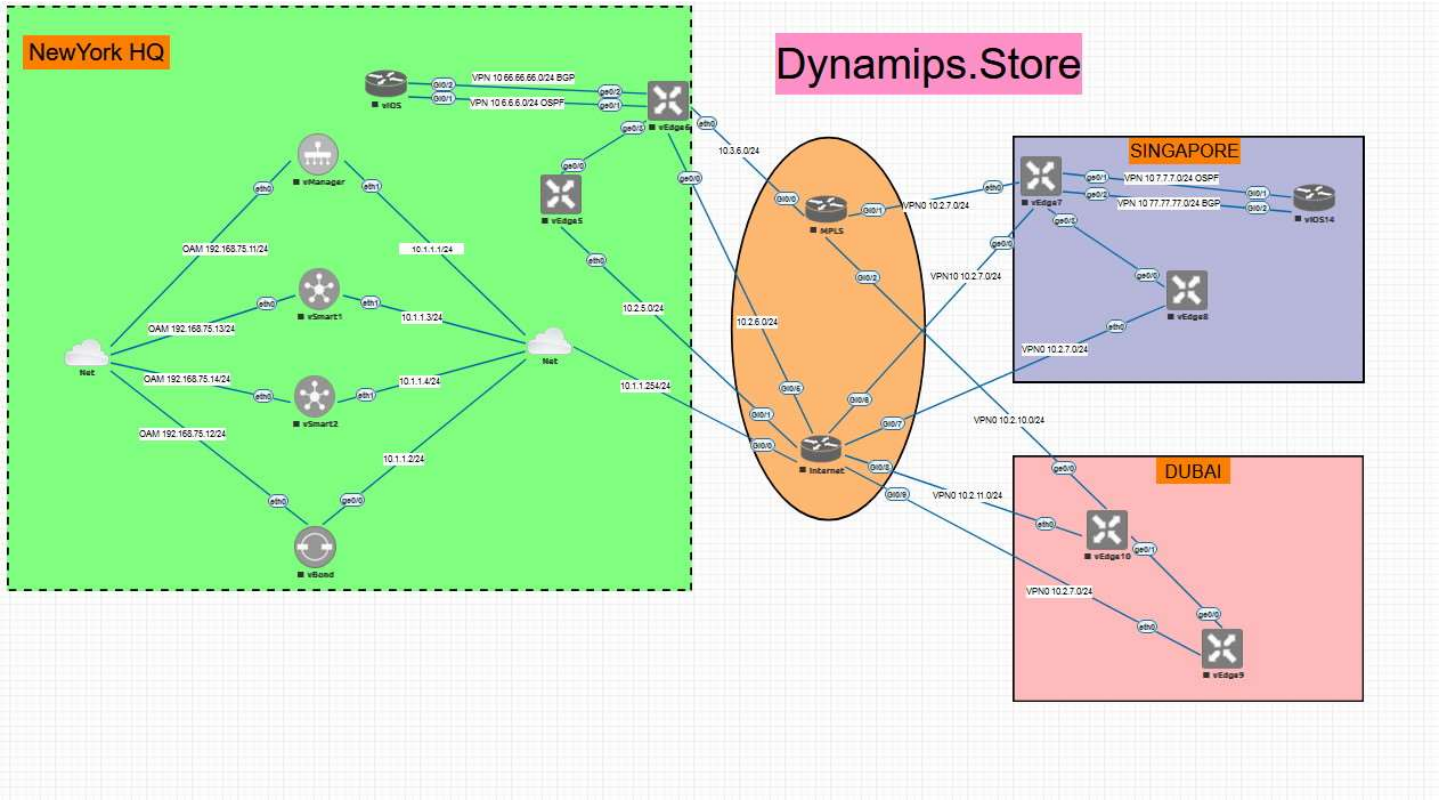
Document Information:

Lab Objective:

This lab is about setting up Control Plane and Data Plane for Sdwan. After the labs,we can see connection control from Vsmart, Vmanage, Vbond and Vedges. For Data Plane, In Vedge, we have IPsec tunnel, BFD session then check the Tlocs info …

Requirement:

- Software:
  - eve-nglab version 1.0.2 if eve-nglab still version 1.0.1, let login vm console with account root/eve then run command: wget -O - https://user.eve-nglab.com/upgrade/1.0.2 | bash
- Hardware requirement:
  - RAM 24Gb **Lab topology:**



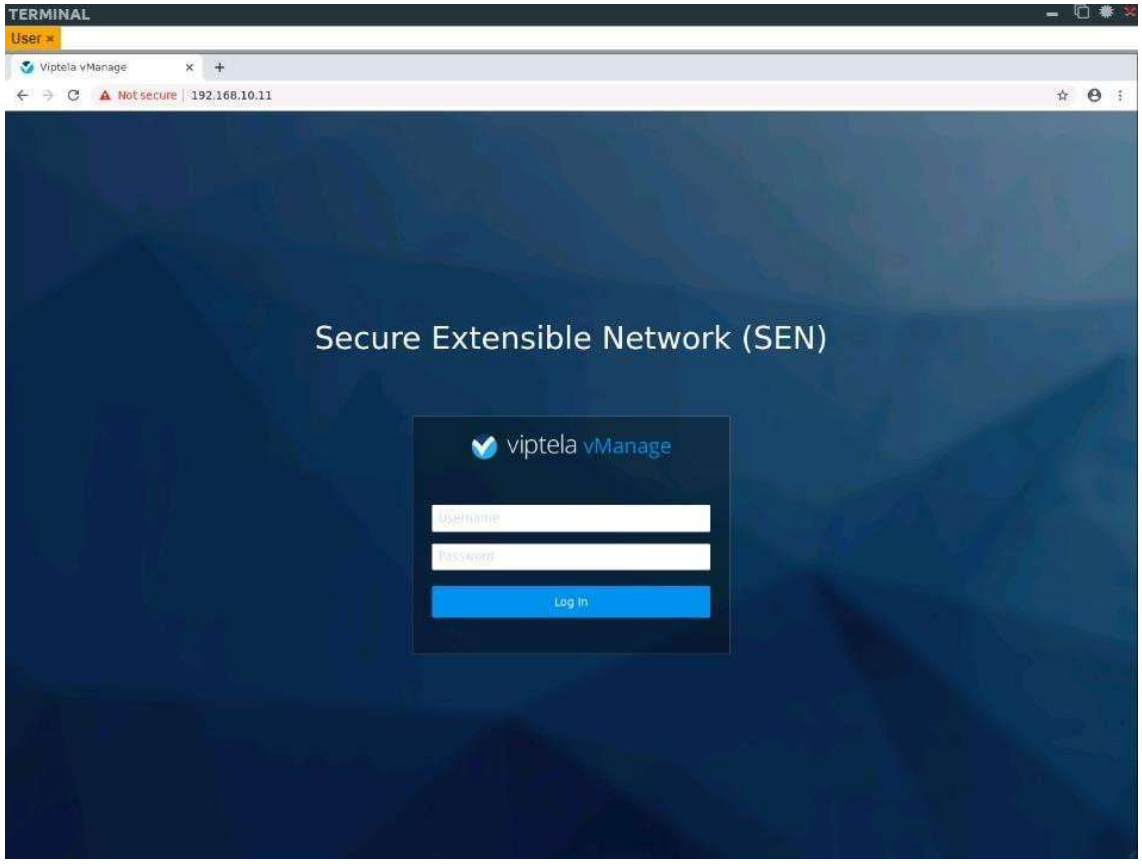
Taks1: Setup vManage web management

- Setup IP web management for

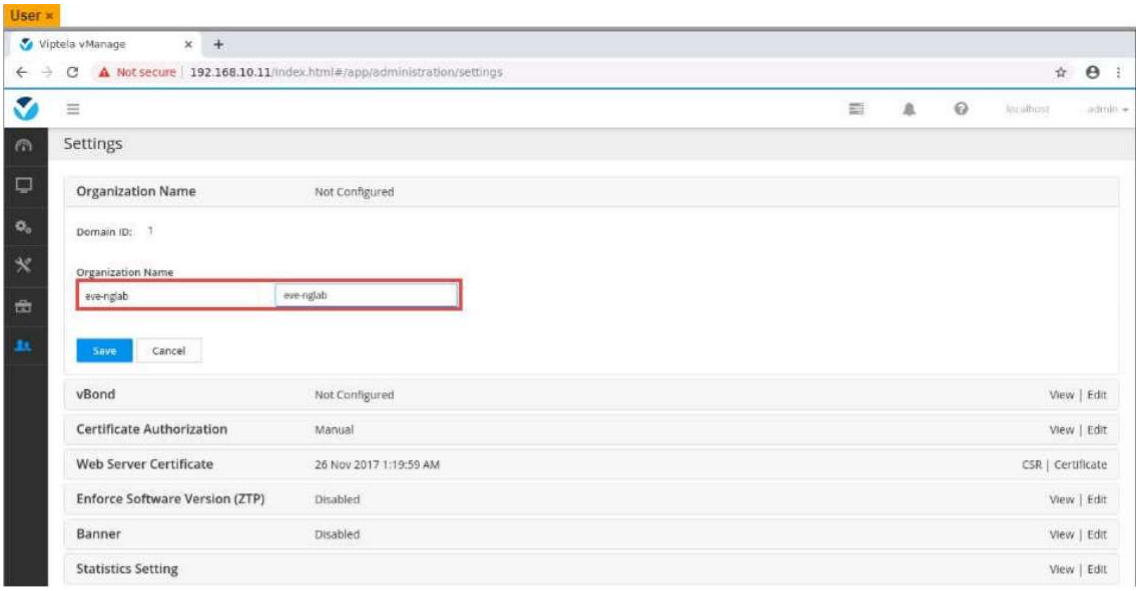
vManage: Console to vManager

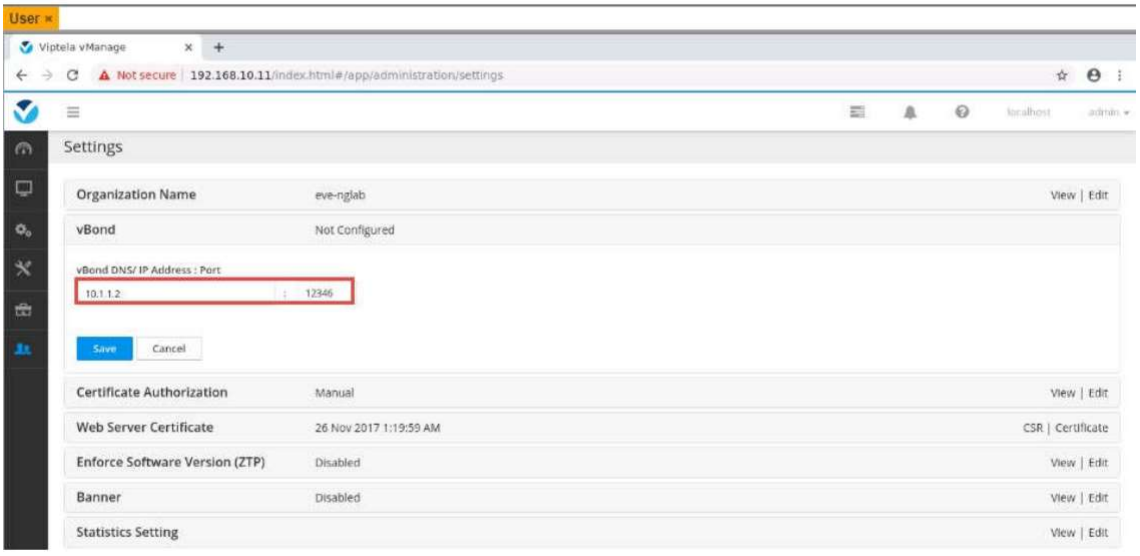
```
config t
vpn 512
interface eth0
ip address 192.168.75.11/24
no shutdown !
ip route 0.0.0.0/0 192.168.75.1
```

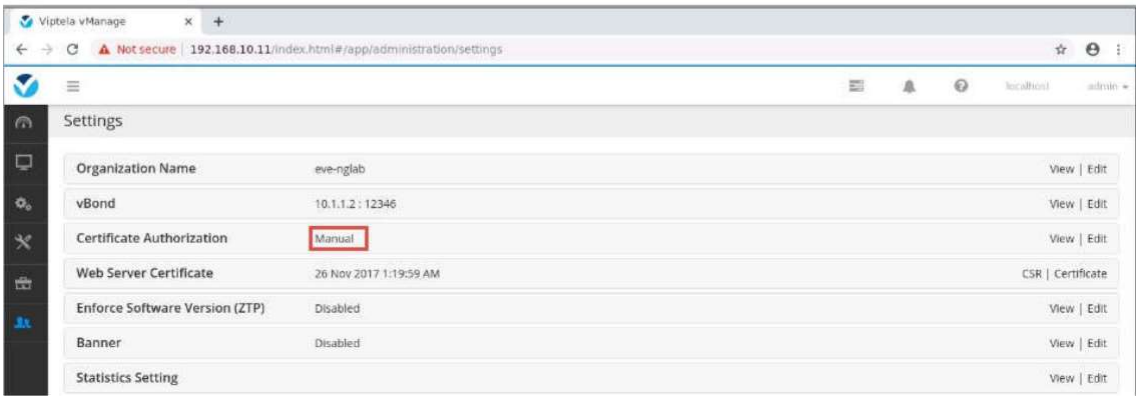
Click to User icon -> login vManage web with ip address: 192.168.10.11. Login with account:
admin/admin



Go to Administration -> Setting


User
Viptela vManage
Not secure | 192.168.10.11/index.html#/app/administration/settings
Settings
Organization Name
Not Configured
Domain ID: 1
Organization Name
eve-nglab
eve-nglab
Save
Cancel
vBond
Not Configured
View | Edit
Certificate Authorization
Manual
View | Edit
Web Server Certificate
26 Nov 2017 1:19:59 AM
CSR | Certificate
Enforce Software Version (ZTP)
Disabled
View | Edit
Banner
Disabled
View | Edit
Statistics Setting
View | Edit


User
Viptela vManage
Not secure | 192.168.10.11/index.html#/app/administration/settings
Settings
Organization Name
eve-nglab
View | Edit
vBond
Not Configured
vBond DNS/ IP Address : Port
10.1.1.2
12346
Save
Cancel
Certificate Authorization
Manual
View | Edit
Web Server Certificate
26 Nov 2017 1:19:59 AM
CSR | Certificate
Enforce Software Version (ZTP)
Disabled
View | Edit
Banner
Disabled
View | Edit
Statistics Setting
View | Edit


Viptela vManage
Not secure | 192.168.10.11/index.html#/app/administration/settings
Settings
Organization Name
eve-nglab
View | Edit
vBond
10.1.1.2 : 12346
View | Edit
Certificate Authorization
Manual
View | Edit
Web Server Certificate
26 Nov 2017 1:19:59 AM
CSR | Certificate
Enforce Software Version (ZTP)
Disabled
View | Edit
Banner
Disabled
View | Edit
Statistics Setting
View | Edit

Task2: Lab configuration

- **vManage**

```
vmanage# conf t
Entering configuration mode terminal
vmanage(config)# system
vmanage(config-system)# system-ip
10.1.1.1
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 10.1.1.2
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 192.168.75.12/24
vedge(config-interface-eth0)# no shut
vedge(config-interface-eth0)# exit
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.75.1
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 1**

```
vsmart(config-vpn-0)# system
vsmart(config-system)# system-ip
10.1.1.3
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
192.168.75.13/24 vsmart(config-interface-
eth0)# no shut
vsmart(config-interface-eth0)# exit
vsmart(config-vpn-512)# ip route 0.0.0.0/0
192.168.75.1
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#
```

- **vSmart 2**

```
vsmart(config-vpn-0)# system
vsmart(config-system)# system-ip
10.1.1.4
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
192.168.75.14/24
vsmart(config-interface-eth0)#
no shut vsmart(config-interface-
eth0)# exit
vsmart(config-vpn-512)# ip route 0.0.0.0/0
192.168.75.1 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
10.1.1.4/24 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 6 Newyork HQ**

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# system-ip
10.2.6.1
vedge(config-system)# site-id 100
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
10.2.6.1/24
vedge(config-interface-ge0/0)# no
shutdown vedge(config-interface-
ge0/0)# exit
vedge(config-vpn-0)# ip route 0.0.0.0/0
10.2.6.254 vedge(config-vpn-0)# commit
and-quit
```

- **vEdge7 Singapore**

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# system-ip
10.2.7.1
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
10.2.7.1/24 vedge(config-interface-ge0/0)#
no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# ip route 0.0.0.0/0
10.2.7.254 vedge(config-vpn-0)# commit and-
quit Commit complete.
```

Task3: Certificate installation

- vManage

Step 1 : Create ROOTCA.key

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

Step 2: Created ROOTCA.pem with ROOTCA.key

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

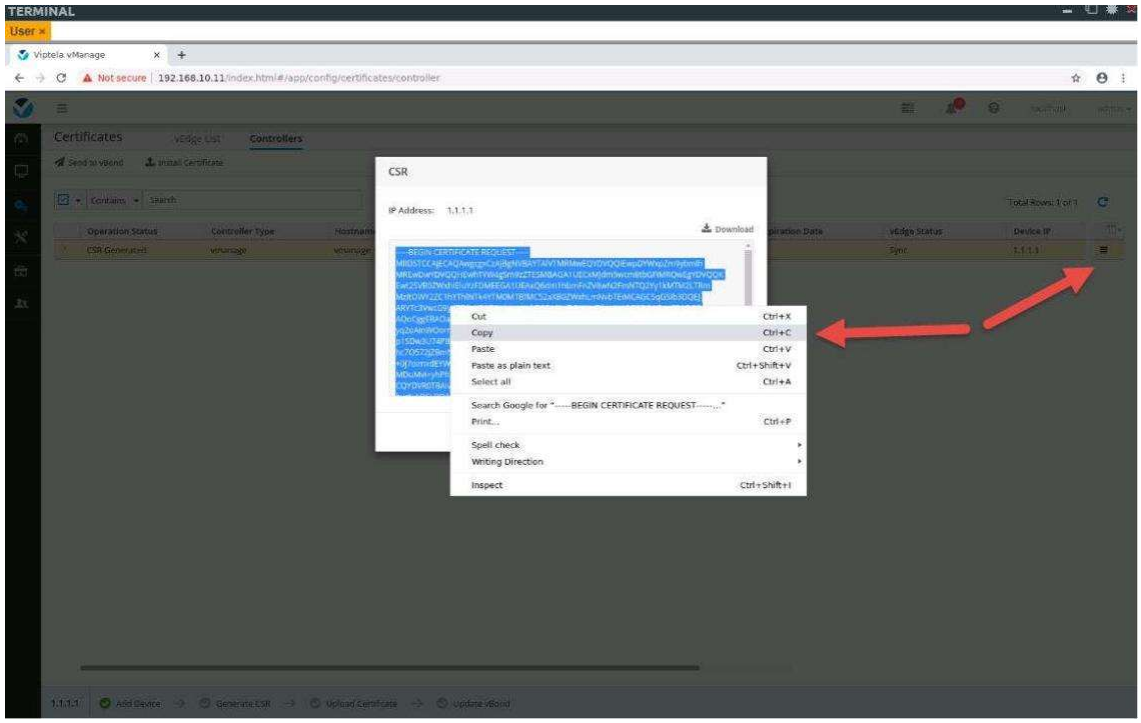
Step 3: Install ROOTCA.pem

```
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
```

Step 4 : Login vManage to create certificate request

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



Step 5: In the vshell use vim to create a file named vmanage.csr with the text from the popup.

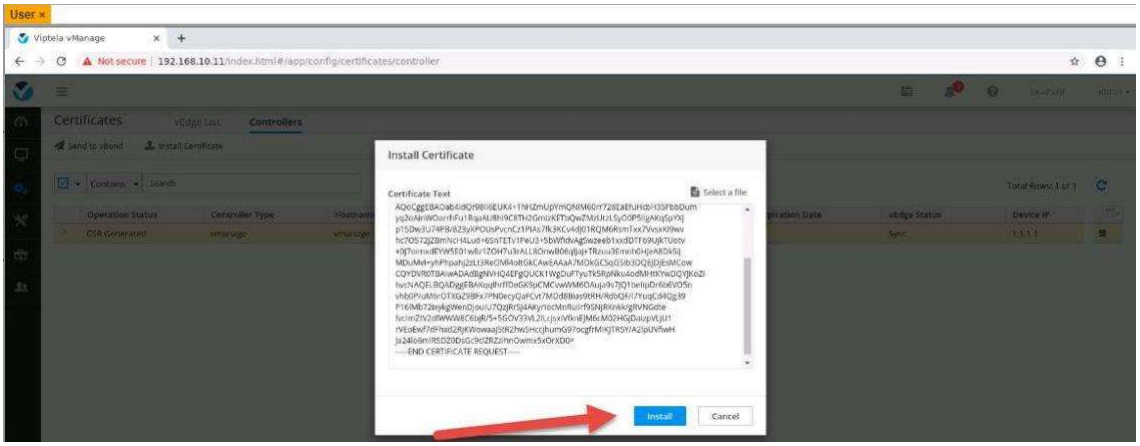
Create vmanage.csr with CSR code copy above.
Use vim editor to create this file in Vshell mode of Vmanage.
Vi vmanage.csr
:qw! To exit the vim file.

Step 6: And create vmanage.crt with ROOTCA.key

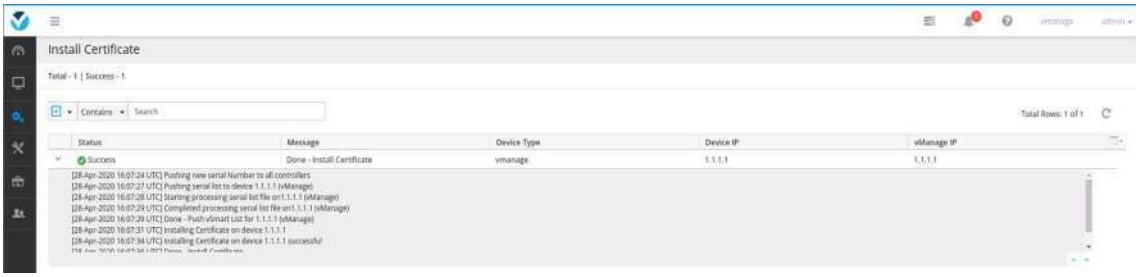
```
openssl x509 -req -in vmanage.csr \
-CA ROOTCA.pem -CAkey ROOTCA.key -
CAcreateserial \ -out vmanage.crt -days 500
-sha256
Result:
Signature ok
```

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

Step 7 : Copy content vmanage.crt file by using “cat vmanage.crt” then install certificate on vManage



Configuration → Certificates → Controllers → Install Certificate



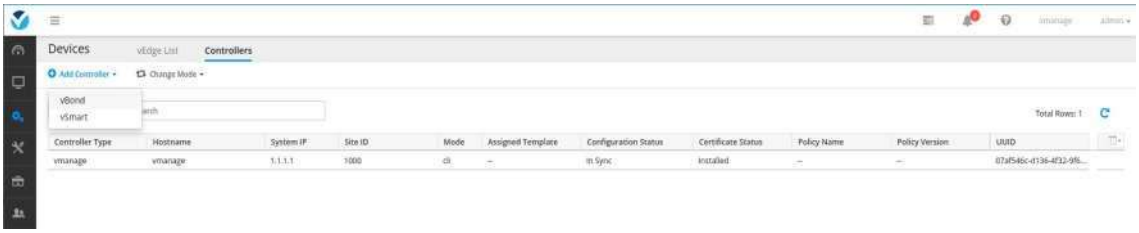
- **vBon**

d: Step 1:

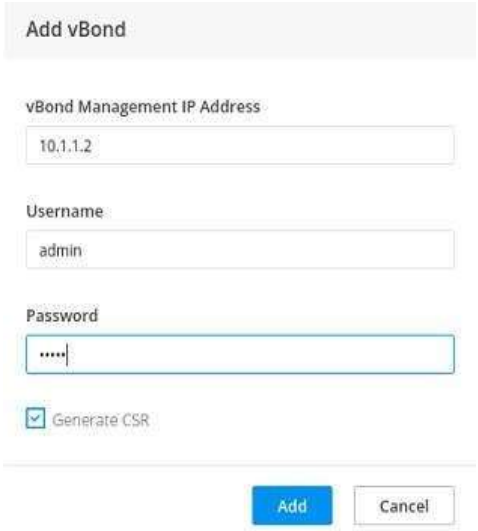
```
vBond# request root-cert-chain install
scp://admin@192.168.75.11:/home/admin/ROOTCA.pem
vpn 512 Result:
Uploading root-ca-cert-chain via VPN 512
Copying ... admin@192.168.10.11:/home/admin/ROOTCA.pem via
VPN 512
Warning: Permanently added '192.168.10.11' (ECDSA) to the
list of
known hosts.
viptela 16.2.11
 admin@192.168.10.11's
password
:                                          100% 1265
```

```
ROOTCA.p
em
1.2KB/s  00:00
Successfully installed the root certificate chain
```

Step 2: Add vBond to vmanage:
And Vbond IP here is IP in VPN0, not VPN 512

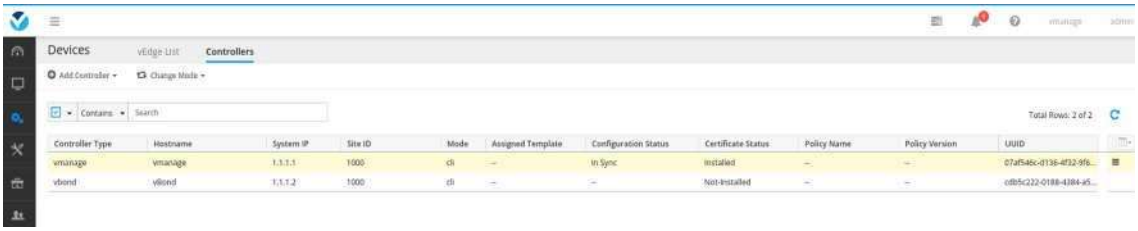


Configuration → Certificates → Controllers → Add Controller:

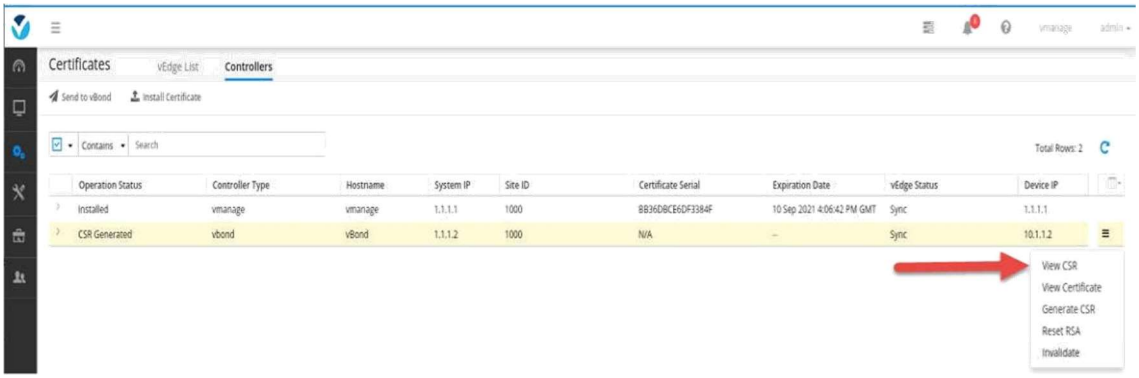


Step 3 : If vbond adding unsuccessful, lets no tunnel-interface as bellow:

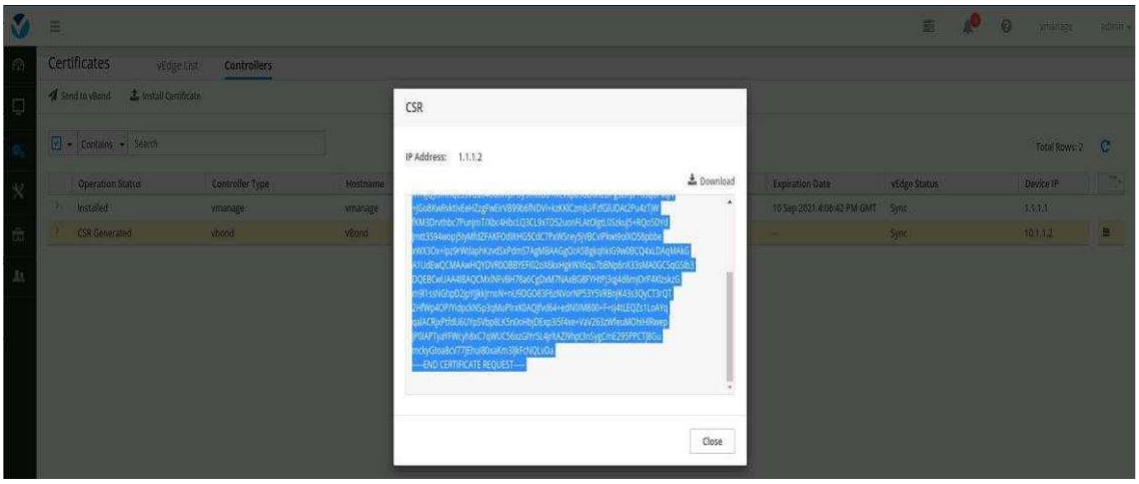
```
vBond# conf t
Entering configuration mode terminal
vBond(config)# vpn 0
vBond(config-vpn-0)#  interface ge0/0
vBond(config-interface-ge0/0)# no tunnel-
interface vBond(config-interface-ge0/0)#
commit
Commit complete.
vBond(config-interface-ge0/0)#
```



Step 4: View vBond CSR:



Configuration → Certificates → Controllers → vBond → View CSR



vManage

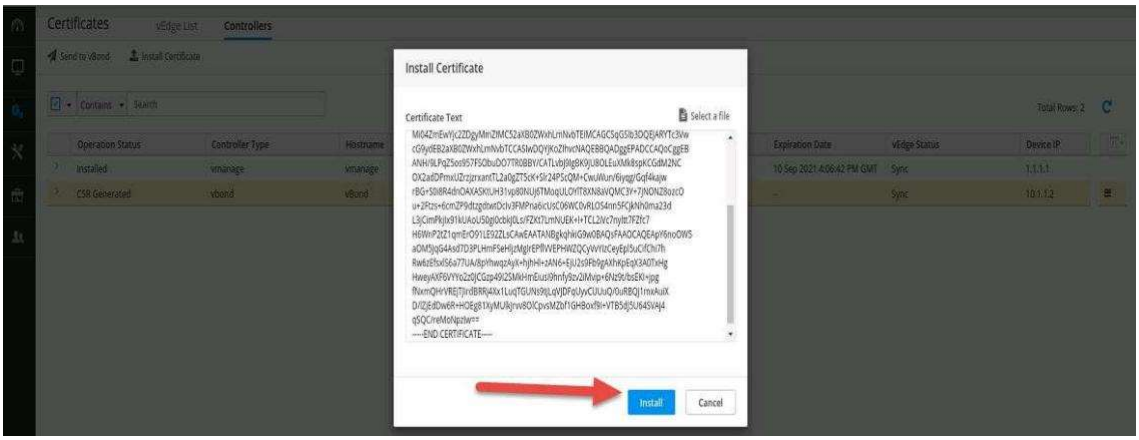
Step 5: On vManage, create vbond.csr with content above using VIM editor in Vshell of Vmanage.

Step 6: Create vbond.crt from Vmange Vsell. // Sign the vbond.csr file with the ROOTCA.key
//vi vbond.csr , press i to insert data, then press ESC to escape the insert things, then press :wq! To save file vbond.csr in Vshell of Vmanage.

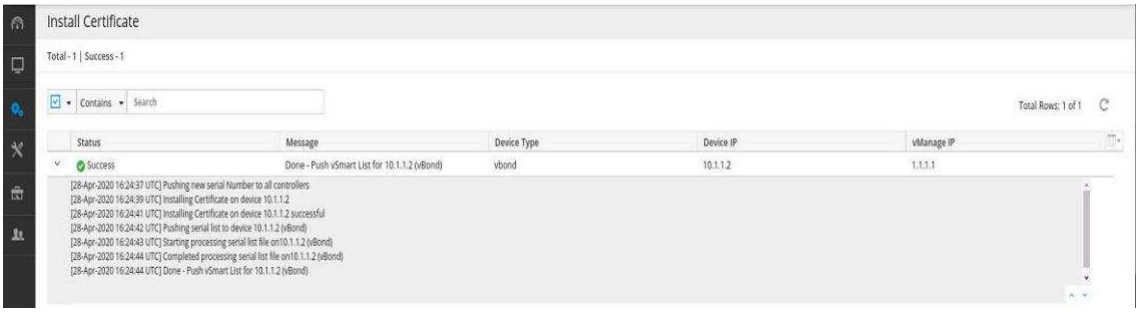
```
openssl x509 -req -in vbond.csr \
 -CA ROOTCA.pem -CAkey ROOTCA.key -
 CAcreateserial \ -out vbond.crt -days 500 -
 sha256

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:~$
```

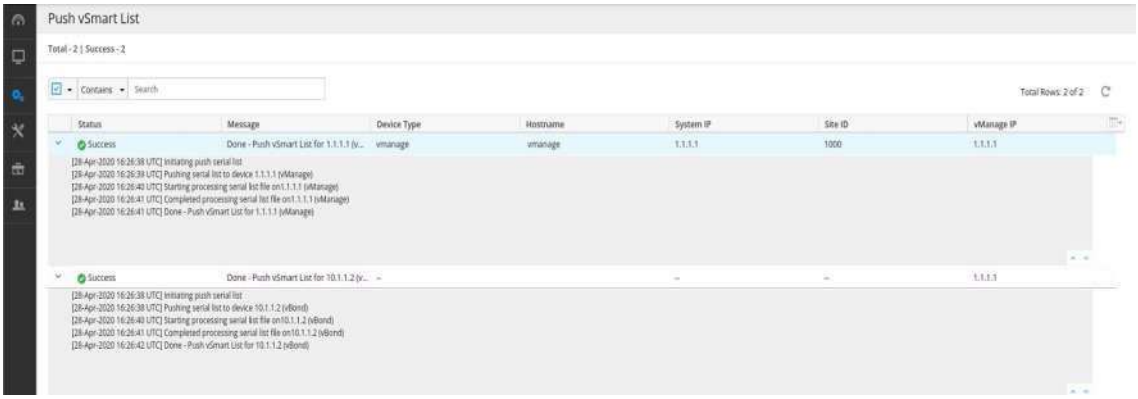
Step 7 : Using “cat vbond.crt” to see file contents then copy and install certificate on vManage web



Configuration → Certificates → Controllers → Install Certificate



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



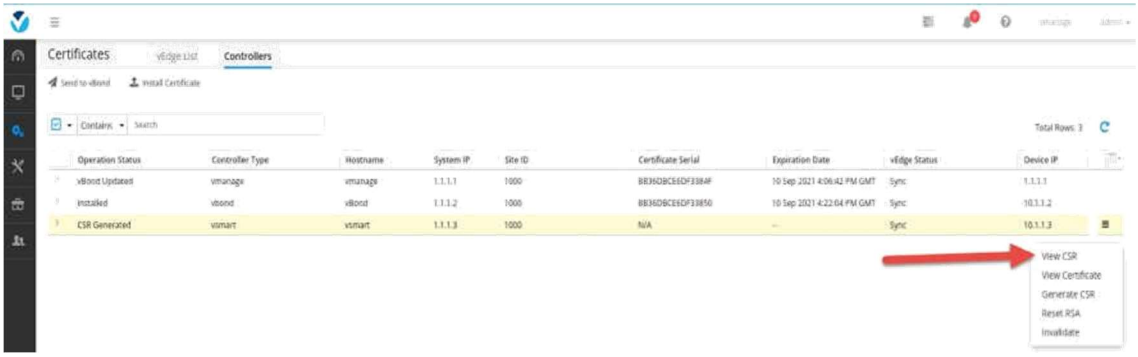
- **vSmart:**

```
vsmart# request root-cert-chain install
scp://admin@192.168.75.11:/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.p
em                                            100% 1265
1.2KB/s   00:00
Successfully installed the root certificate chain
```

Step 2 : Add vSmart to vManage web

Configuration → Devices → Controllers → Add Controller → vSmart

Step 3: View and copy vSmart CSR
Configuration → Certificates → Controllers → vSmart → View CSR:



Step 4: in Vmange :

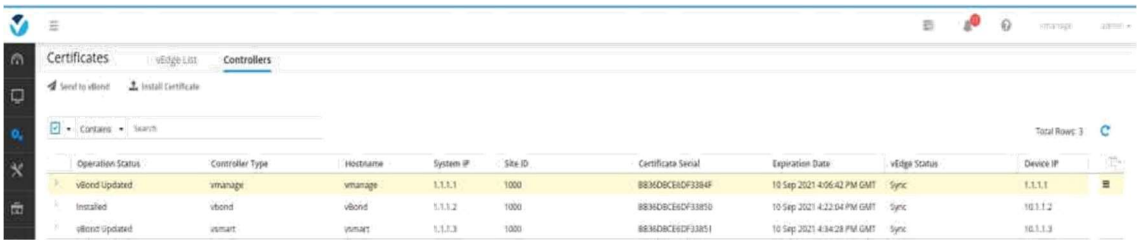
Create vsmart1.csr file on vManage with contents viewed above using VIM editor. (I have 2 vsmarts to make backup)
Sign vsmart1.csr with ROOTCA.key (I have 2 Vsmarts)

- **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 vmsart6.crt” to see contents and copy then install certificate:

Configuration → Certificates → Controllers → Install Certificate



I will make for Vsmart 7 with the same procedure

vEdge:

Step 1 : **on vManage,** using “cat ROOTCA.pem” to see contents then create ROOTCA.pem file on vEdge with same contents.

Step 1 : Install ROOTCA.pem on vEdge with command: **`request root-cert-chain install /home/admin/ROOTCA.pem`**

`The purpose is to SCP the ROOTCA.pem from Vmanage to Vedge`

The interesting here is using VPN 0.

//if we have OAM to this Vedge

Or can use this command : ***request root-cert-chain install scp://admin@192.168.75.11:/home/admin/ROOTCA.pem vpn 512***

```
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
```

Step 2 : Create vedge01.csr file : Do it on Vedge using below command

```
request csr upload /home/admin/vedge06.csr

Uploading CSR via VPN 0
Enter organization-unit name       : sdwan
Re-enter organization-unit name     : sdwan
Generatin private/public pair and CSR for this vedge
g         device
Generatin CSR for this vedge
g         device                    ........[DONE]
Copying ... /home/admin/vedge01.csr via VPN 0
CSR
upload    successful
```

Step 3: *Using "cat vedge06.csr" to copy contents* and create vedge06.csr file on vManage. Create vedge06.crt with command bellow: vMange:

```
openssl x509 -req -in vedge06.csr\
-CA ROOTCA.pem -CAkey ROOTCA.key -
CAcreateserial\ -out vedge06.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-
9a8d7e3f41f90.viptela.com/emailAddress=support@vipte
la .com Getting CA Private Key
```

Step 4 : On vedge06, create vedge06.crt same contents with file on vManage then install with
command bellow: Note in Normal mode, not Vshell mode

request certificate install scp://admin@10.1.1.1:/home/admin/vedge06.crt
!you can use the command on the box too. But I love to use the command with SCP

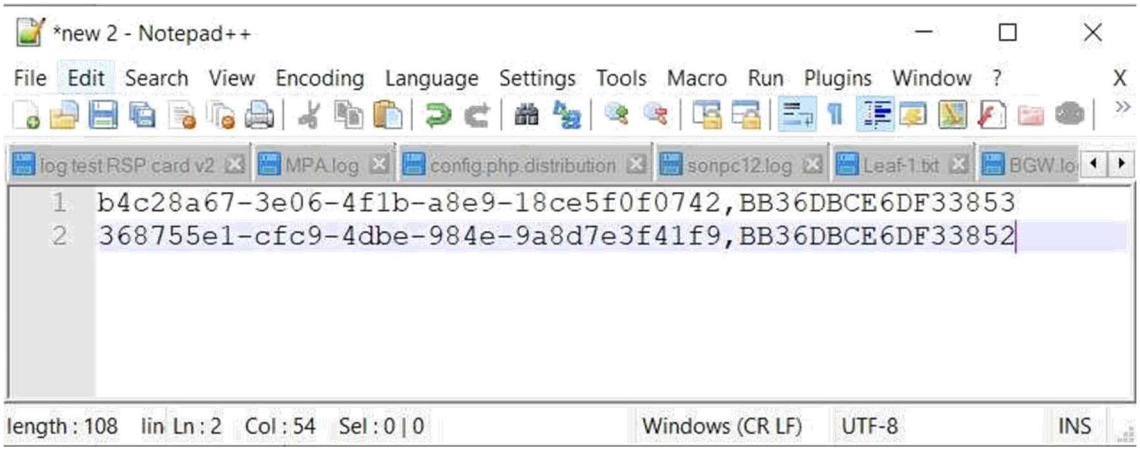
```
vedge# request certificate install /home/admin/vedge06.crt
Result:
Installing certificate via VPN 0
Copying ... /home/admin/vedge01.crt via VPN 0
Successfully installed the certificate
```

Check serial number:

```
vedge# show certificate serial
Chassis number: 368755e1-cfc9-4dbe-984e-9a8d7e3f41f9 serial
```

number: BB36DBCE6DF33852

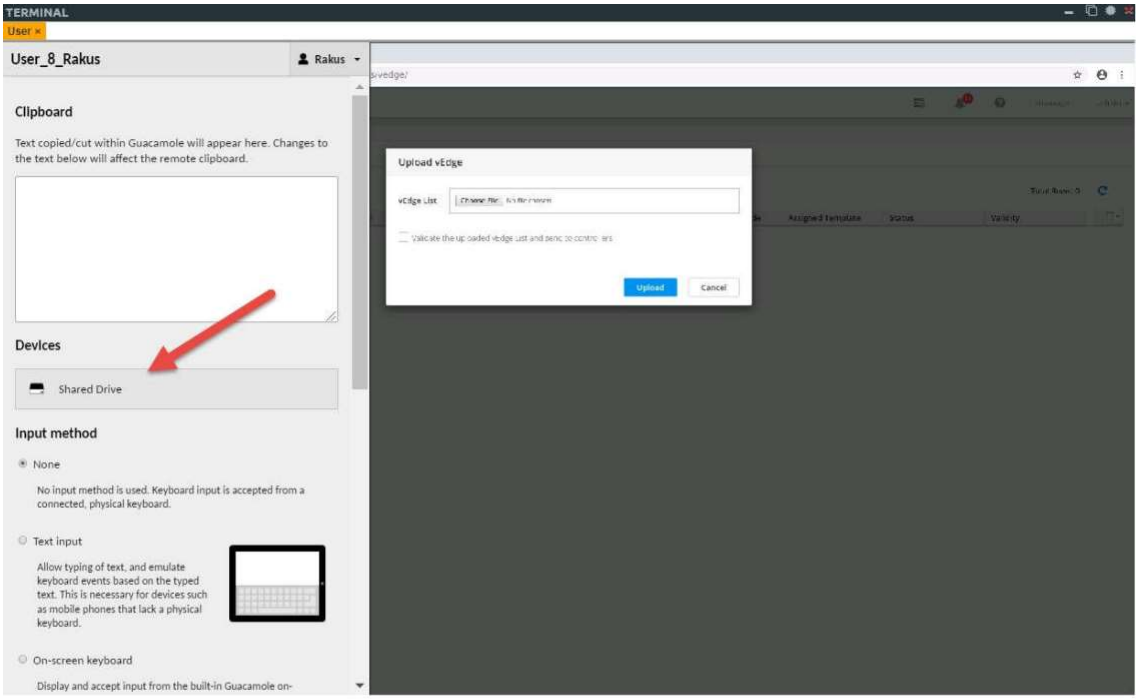
Create text file with code: 368755e1-cfc9-4dbe-984e-9a8d7e3f41f9,BB36DBCE6DF33852 Do the same with vedge06. Check serial and add to text file.

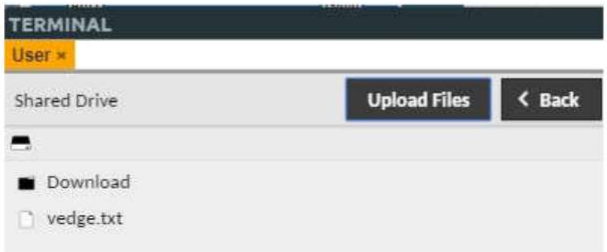


Task 4: Upload vEdge list

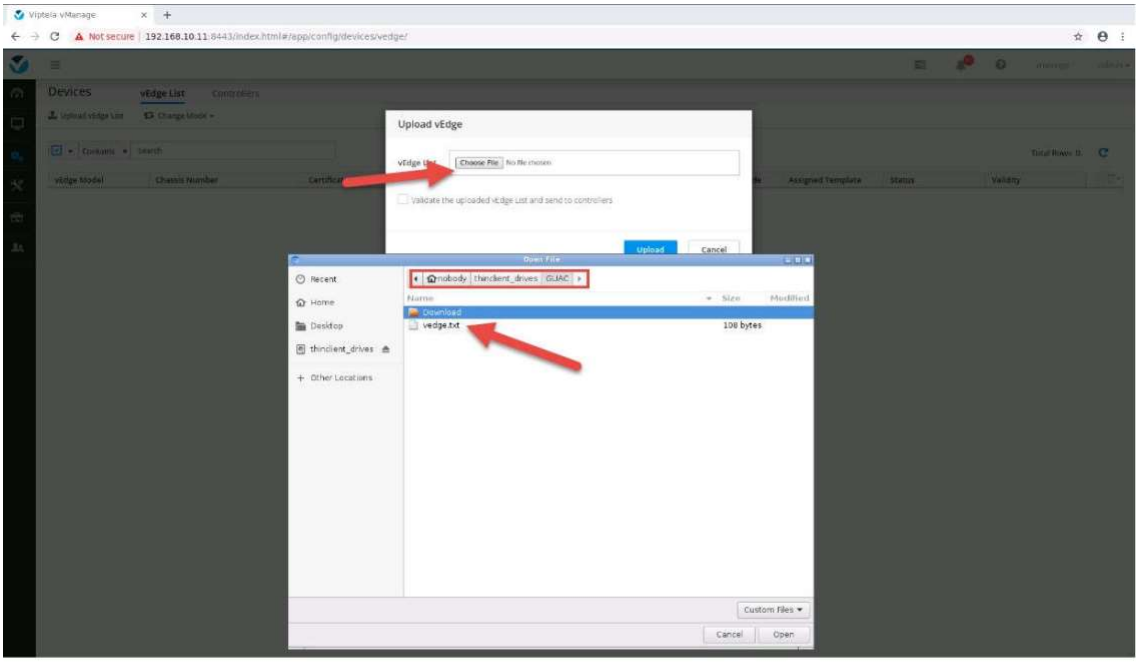
Method 1: For this lab , you just upload Vedgelist from your computer to Vmanage

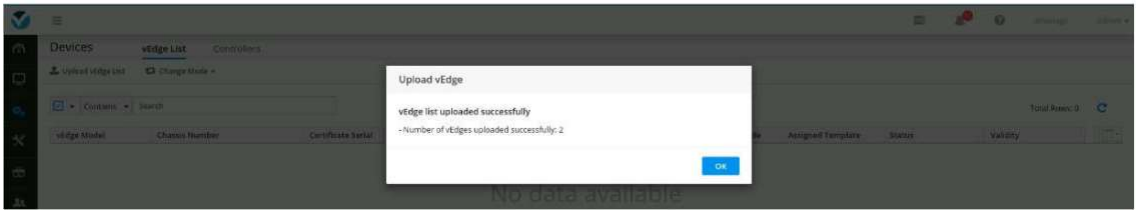
Method 2: it is working for SDWAN lab 1 by Rakus. He made PC on EVE.



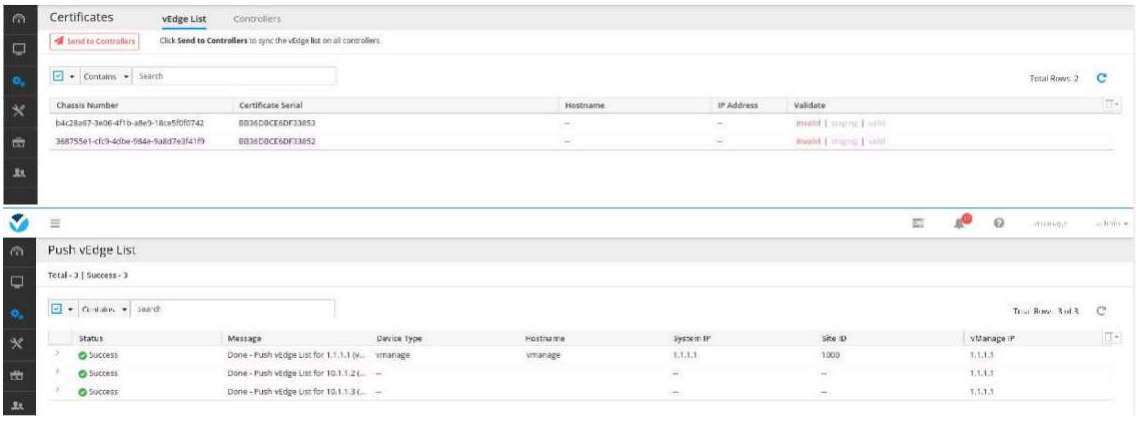


Upload vedge file to vManage





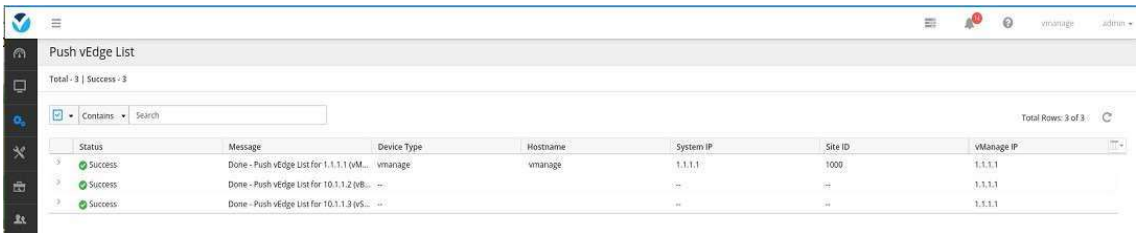
Send vedge list to controller
Configuration → Certificates → vEdge List → Send to Controllers



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:

```
vmanage# show control
connections
PEER                 PEER            DOMAI                PRIVA
PEER   PEER   PEER         SITE      N         PEER       TE
             PUBLI                                       INSTAN
PEER         C                                           CE
       PROTOCOL                              PRIVATE
TYPE   SYSTEM      IP      ID        ID       IP         PORT
PUBLIC                  REMOTE
IP             PORT      COLOR    STATE       UPTIME
-------------------------------------------------------------------
----------------------
-----------------------------------------------------------------
----------------------
vedge  dtls 3.1.1.1        2         1      172.17.0.2
```

```
1234                        defaul
6      172.17.0.2  12346    t            up        0:00:00:34
       vsmar                           100
0      t      dtls 1.1.1.3        0         1       10.1.1.3
1234   10.1.1              defau
6      .3           12346  lt           up        0:00:00:28
0      vbond  dtls 1.1.1.2        0         0       10.1.1.2
1234   10.1.1              defau
6      .2           12346  lt           up        0:00:00:47
1      vbond  dtls 1.1.1.2        0         0       10.1.1.2
1234   10.1.1              defau
6      .2           12346  lt           up        0:00:00:46
2      vedge  dtls 2.1.1.1 defaul 1         1     172.16.0.2
1234
6      172.16.0.2  12346    t            up        0:00:00:29
2      vbond  dtls 1.1.1.2        0         0       10.1.1.2
```

```
      10.1.        1234  defau                    0:00:00:4
12346 1.2          6     lt          up           7
                   1.1.1
3     vbond dtls   .2          0        0        10.1.1.2
      10.1.1       1234  defaul
12346 .2           6     t           up           0:00:00:47
vsmart# show control
connections
                                                          PEE
                   PEE          SIT    PEER               R
      PEER  PEER   R            E      DOMAIN  PEER
PRIVAT             PUBLI
E     PEER         C
INSTA       PROTOCOL SYSTEM
NCE   TYPE  IP                 ID       ID       PRIVATE IP
                         REMOTE
PORT  PUBLIC IP   PORT   COLOR        STATE      UPTIME
-------------------------------------------------------------
----------------------
-------------------------------------------------------------
---------------------
0     vedge  dtl    2.1.1.1     1        1          172.16.0
                                                        .2
123                      defaul                0:00:00
46    172.16.0.2 12346   t         up          :53        0
ved                                          172.17.0   1234
ge    dtls 3.1.1.1       2        1              .2      6
                  defau                0:00:00          vbon
172.17.0.2 12346   lt      up         :58        0        d
dtl                                  10.1.1     1234
s     -            0       0        .2         6   10.1.1.2
123   defau                                      vmana
46    lt           up          0:00:01:00 0       ge    dtls
1.1.1                          10.1.      1234  10.1.1     1234
.1          1000     0         1.1        6          .1        6
defau                       0:00:00                   dtl
lt            up  10.1.1   :52          1     vbond     s    -
0       0             .2
123                      defaul                0:00:00
46    10.1.1.2   12346   t         up          :59

vedge# show control
connections
PEE
R                                  PEER
CONTROLLER
PEE    PEER          SIT
R      PEER          E       DOMAIN PEER
```

```
PRI
V   PEER                            PUB
GRO
UP
TYP   PROT                           PRIVATE
E     SYSTEM IP       ID      ID    IP
POR  PUBLIC                          PORT  LOCAL         PROXY
T    IP                              COLOR               STATE
UPTIM
E         ID
-------------------------------------------------------------------
--------------------
-------------------------------------------------------------------
--------------------
------------------
----
vsma        dtls
rt       1.1.1.3       1000     1  10.1.1.3
                                    12346               u
12346 10.1.1.3                      default         No  p
0:00:04
:40      0
vbon        dtls
d        0.0.0.0       0        0  10.1.1.2
                                    12346               u
12346 10.1.1.2                      default         -   p
0:00:09
:29      0
vmanage dtls
1.1.1.1               1000     0  10.1.1.1
                                    12546               u
12546 10.1.1.1                      default         No  p
0:00:04
:40      0
```