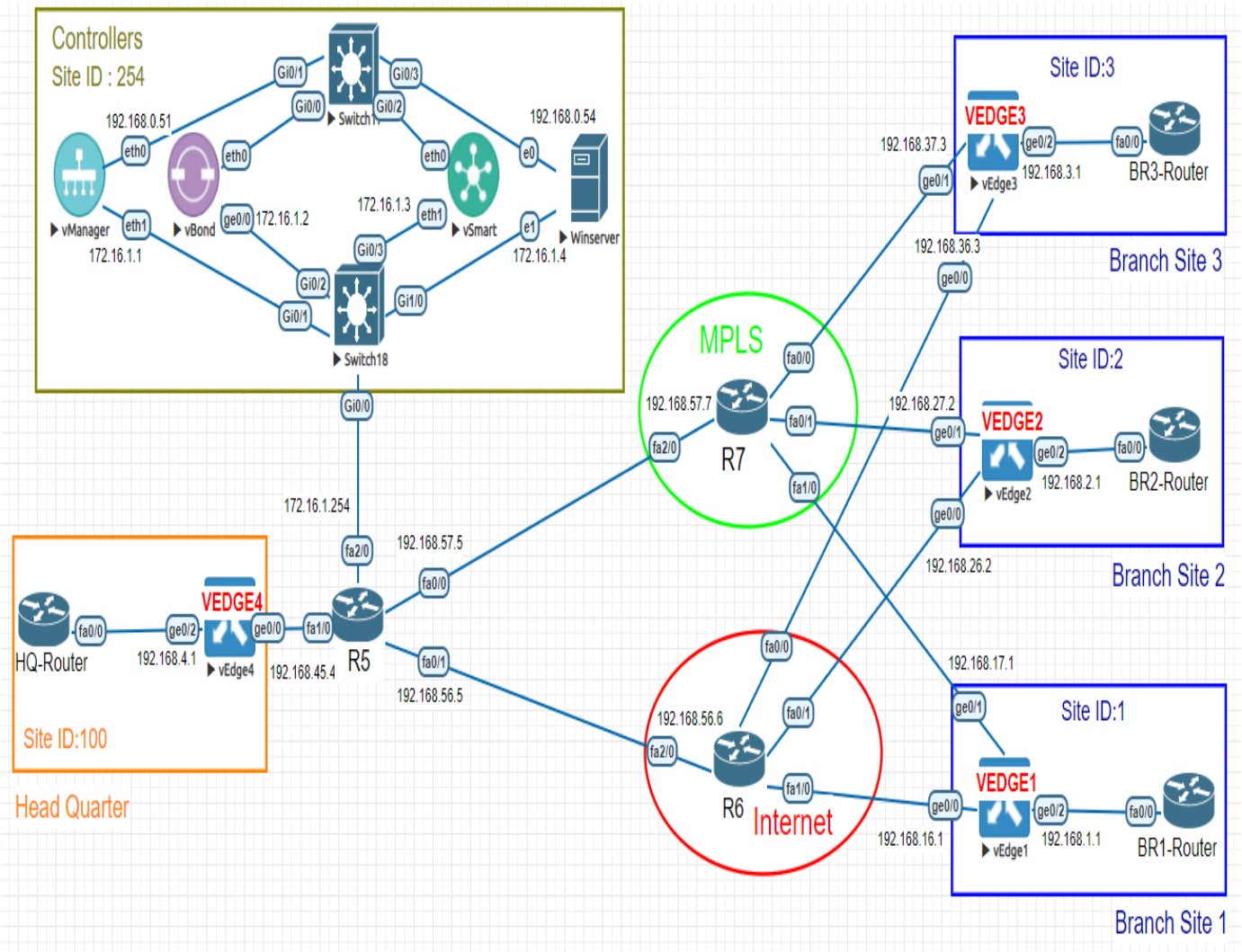
Lab Topology # 1



Configuring underlay Network

Interface Configuration

R5 Router

Interface	IP Address	Subnet Mask
fa1/0	192.168.45.5	255.255.255.0
fa2/0	172.16.1.254	255.255.255.0
fa0/0	192.168.57.5	255.255.255.0
fa0/1	192.168.56.5	255.255.255.0

R6 Router – Internet Cloud Router

Interface	IP Address	Subnet Mask
fa1/0	192.168.16.6	255.255.255.0
fa2/0	192.168.56.6	255.255.255.0
fa0/0	192.168.36.6	255.255.255.0
fa0/1	192.168.26.6	255.255.255.0

R7 Router – MPLS Cloud Router

Interface	IP Address	Subnet Mask
fa1/0	192.168.17.7	255.255.255.0
fa2/0	192.168.57.7	255.255.255.0
fa0/0	192.168.37.7	255.255.255.0
fa0/1	192.168.27.7	255.255.255.0

Task 1 – R5 Router Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure OSPF as the IGP to communicate with the MPLS Cloud. Enable all the interfaces.
- Make sure OSPF only sends and receives OSPF packets on the link towards the MPLS Cloud using the Passive-interface command.
- Configure a default route on the router towards the Internet

```
enable
conf t
!
Hostname R5
!
Interface fa1/0
ip address 192.168.45.5 255.255.255.0
no shut
!
Interface fa2/0
ip address 172.16.1.254 255.255.255.0
no shut
!
Interface fa0/0
ip address 192.168.57.5 255.255.255.0
no shut
!
Interface fa0/1
ip address 192.168.56.5 255.255.255.0
no shut
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
passive-interface default
no passive-interface fa0/0
!
ip route 0.0.0.0 0.0.0.0 192.168.56.6
do wr
```

Task 2 – R6 Router (Internet Cloud) Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure a Default Static Route. The Next Hop should point towards the IP of the R5Router [192.168.56.5].

We're Sorry; Full Content Access is for Members only.

Initializing the Controllers

1. Initializing vManage – CLI

Task 1 – Configuring the System Component

Configure the System parameters based on the following:

Host-name: vMANAGE1
Organization: XXXXXXX [Organization Name]
System-IP: 10.1.254.1
Site ID: 254
vbond Address: 172.16.1.2
Timezone: Based on the appropriate Timezone

Note: Default username/Password: **admin/admin**

```
config
!
system
host-name vMANAGE1
system-ip 10.1.254.1
site-id 254
organization-name XXXXXX
clock timezone Asia/Kolkata
vbond 172.16.1.2
!
commit
```

Task 2 – Configure the VPN parameters

Configure the VPN parameters based on the following:
vpn 0 - Interface eth1
- IP Address: 172.16.1.1/24
- Tunnel Interface
- Tunnel Services (All, NetConf, SSHD)
- Default Route: 172.16.1.254

vpn 512 - Interface eth0
- IP Address: 192.168.0.51/24

```
config
!
vpn 0
no interface eth0
interface eth1
ip address 172.16.1.1/24
tunnel-interface
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 172.16.1.254
!

vpn 512
interface eth0
ip address 192.168.0.51/24
no shut
!

commit
```

We’re Sorry; Full Content Access is for Members only

2. Initializing vBond – CLI

Task 1 – Configuring the System Component

Configure the System parameters based on the following:

Host-name: vBOND
Organization: XXXXXXX [Organization Name]
System-IP: 10.1.254.2
Site ID: 254
Vbond Address: 172.16.1.2
Timezone: Based on the appropriate Timezone

Note: Default username/Password: **admin/admin**

config
!

We're Sorry; Full Content Access is for Members only

- Tunnel Interface
- Tunnel Services (All, NetConf, SSHD)
- Default Route: 172.16.1.254

vpn 512 - Interface eth0
- IP Address: 192.168.0.52/24

```
config
!


vpn 0
no interface eth0
interface ge0/0
ip address 172.16.1.2/24
tunnel-interface
encapsulation ipsec
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 172.16.1.254
!


vpn 512
interface eth0
ip address 192.168.0.52/24
no shut
!

commit
```

3. Initializing vsmart – CLI

Task 1 – Configuring the System Component

Configure the System parameters based on the following:

Host-name: vSMART1
Organization: XXXXXXX [Organization Name]
System-IP: 10.1.254.3
Site ID: 254
vb
Tim

No

co
!
sy
ho
sy
sit
or
cl
vb
!
co

Ta

Co

vp
- IP
- T
- T
- D

vp
- IP

We're Sorry; Full Content Access is for Members only

```
config
!

vpn 0
no interface eth0
interface eth1
ip address 172.16.1.3/24
tunnel-interface
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 172.16.1.254
!

vpn 512
interface eth0
ip address 192.168.0.53/24
no shut
!
commit
```

Installing Enterprise Certificate Server (Windows 2008 server)

Task 1 – Configure the Interfaces

First Ethernet Interface:
IP Address: 192.168.0.54
Subnet Mask: 255.255.255.0

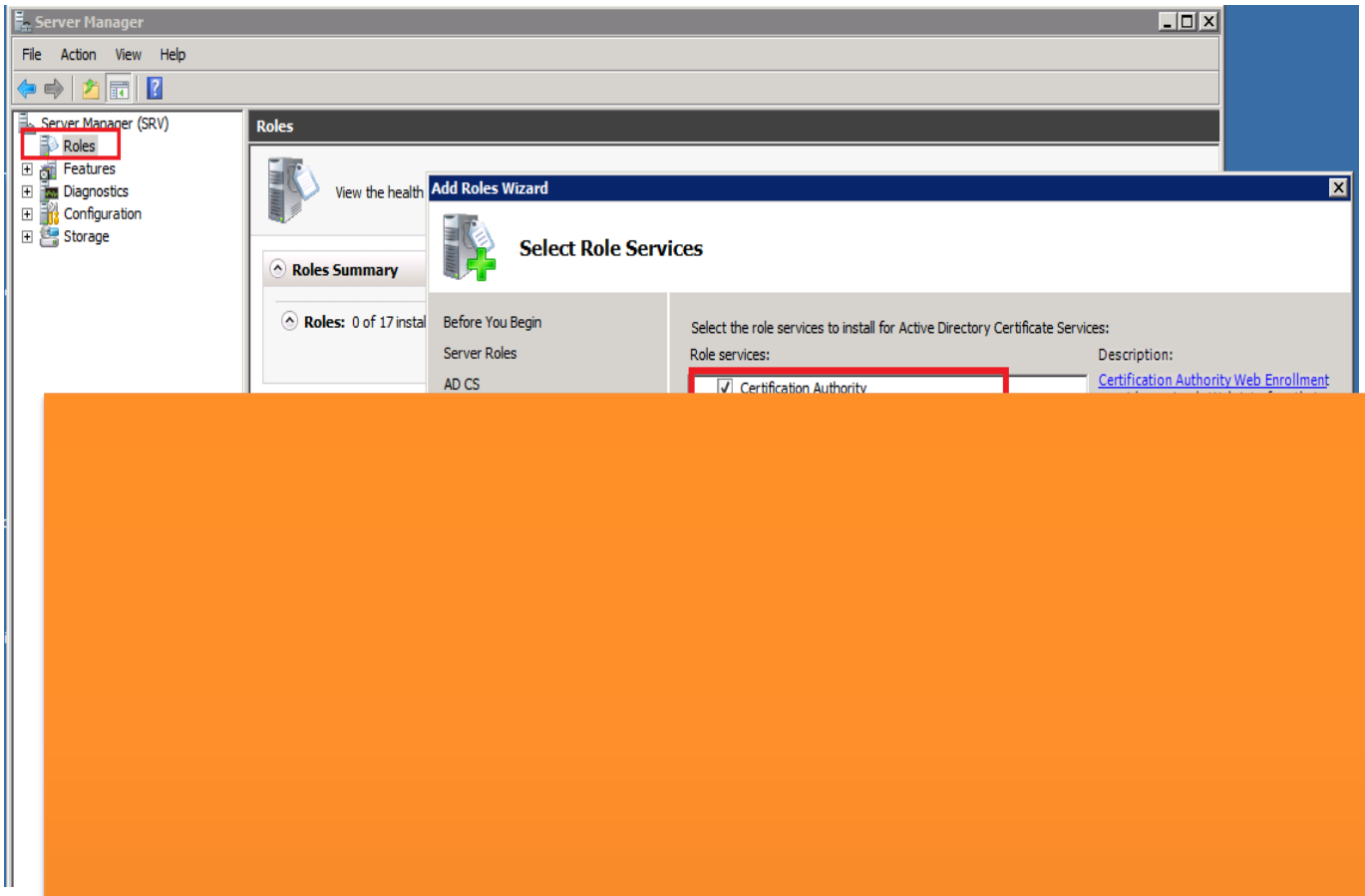
Third Ethernet Interface:
IP Address: 172.16.1.4
Subnet Mask: 255.255.255.0
Default Gateway: 172.16.1.254

Task 2 – Configure the Timezone and Time

Configure the appropriate Timezone and Date/Time on the Windows Server.
(Date/Time should be exactly same as on controllers – very important)

Task 3 – Installing the Enterprise Root Certificate Server

Step1: Open server Manager -> Roles -> Add Roles -> Select the "**Active Directory Certificate Services**" and click **Next**
Step2: Select "**Certification Authority Web Enrolment**" and click Next
Step3: Leave it as Standalone and click Next
Step4: Leave it as Root CA and click Next
Step5: Leave "Create a new private key" and click Next
Step6: Leave the default for the Cryptography for CA and click **Next**
Step7: Set the Common name as **NETTECH-CA** and click **Next**
Step8: Leave the default for the Validity Period and click Next
Step9: Click Install



Ta

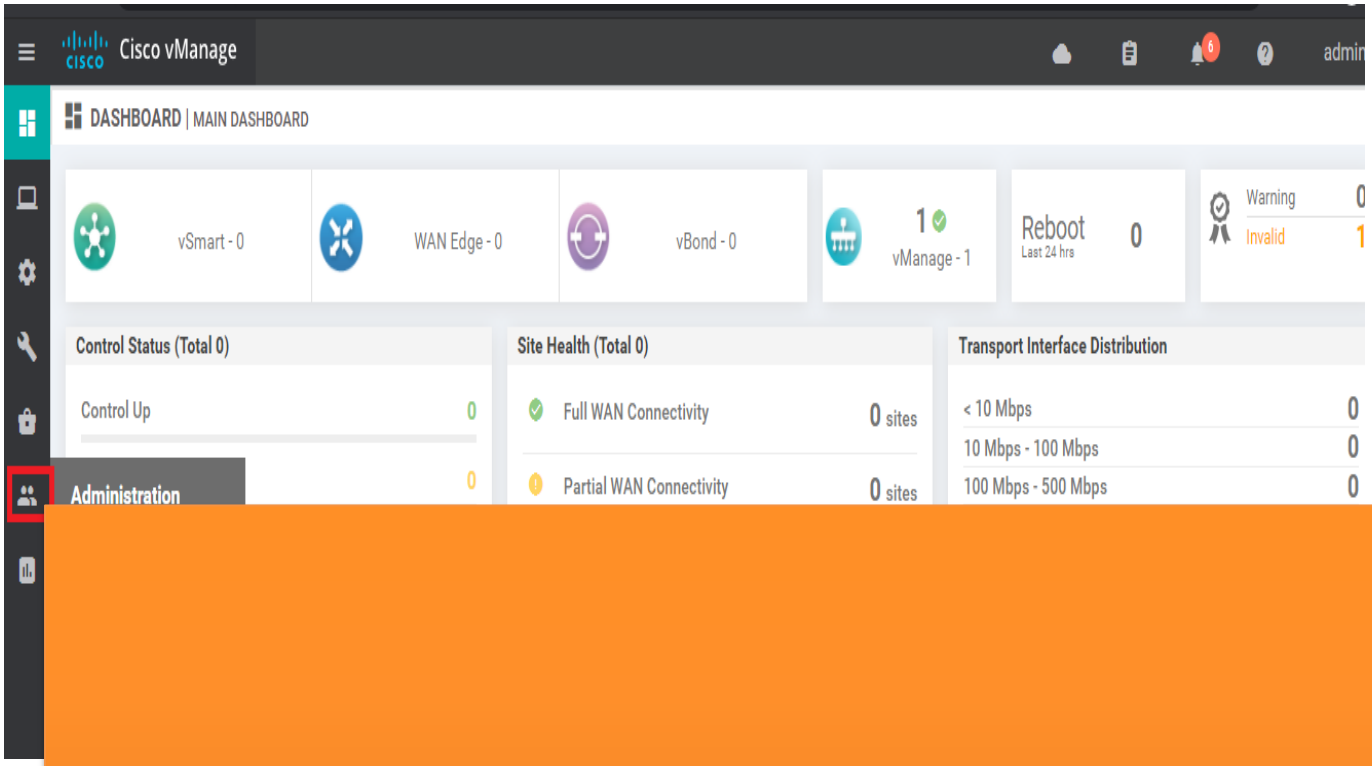
-D
wi
-W
tra

We’re Sorry; Full Content Access is for Members only

Initializing vMANAGE – GUI

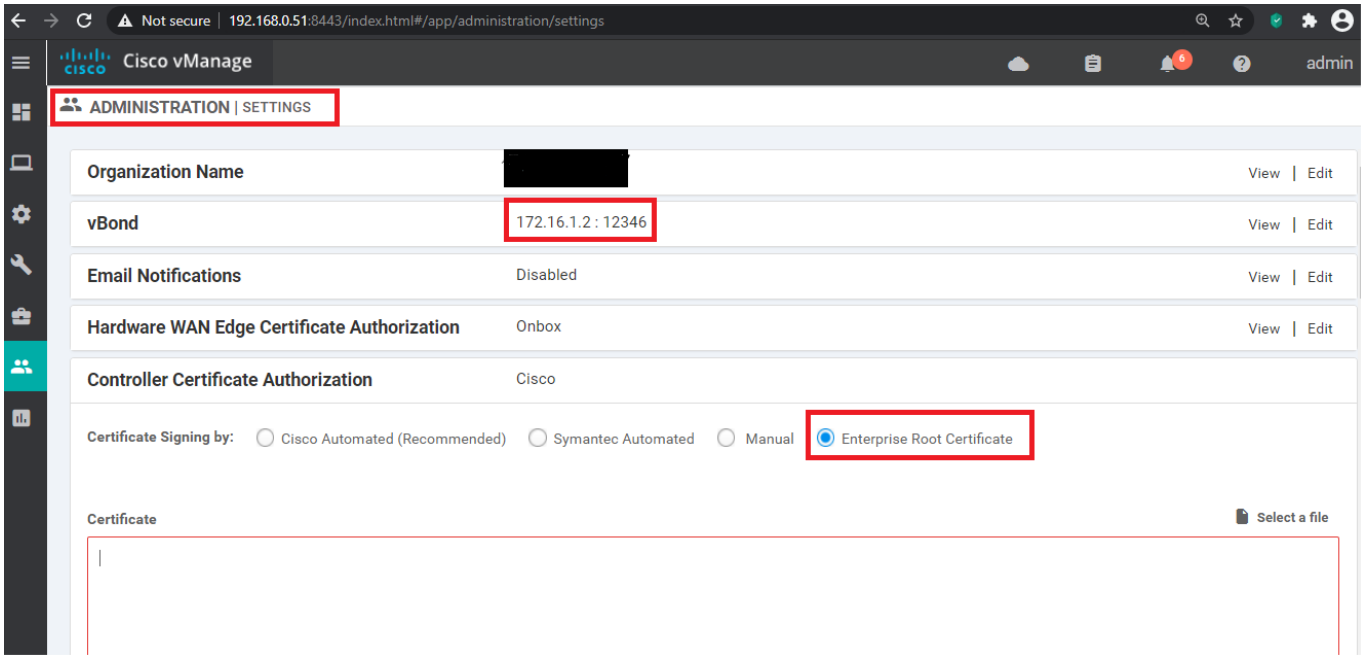
Task 1 – Organization name & vBond Address

- Log into the vManage from the Server by browsing to **https://192.168.0.51:8443** using a username of **admin** and a password of **admin.**
- Navigate to Administration -> Settings
- Click **Edit** on the Organization name and set it to Your **Organization Name**. Confirm the Organization name. Click **OK.**
- Click **Edit** on the **vBond** address and change it to **172.16.1.2** Confirm and click **OK**



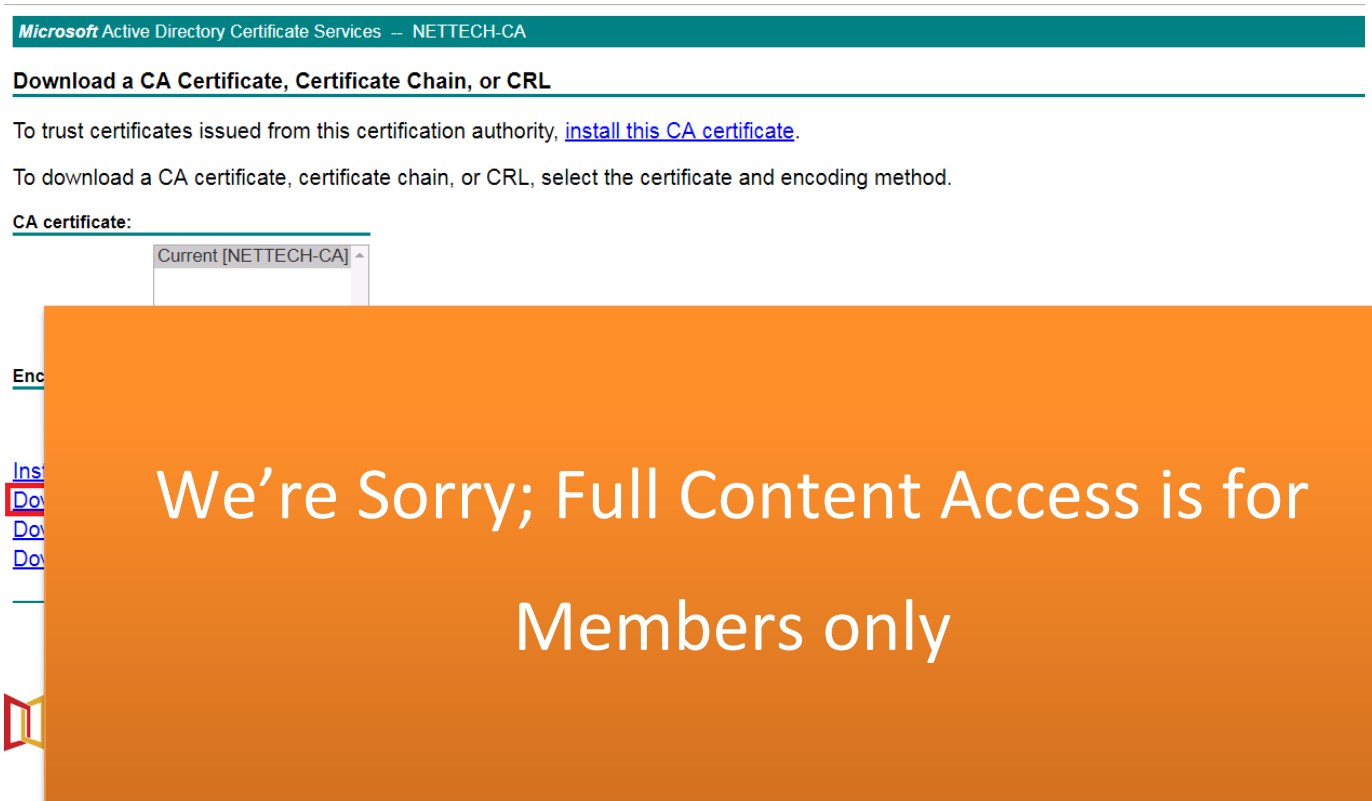
We're Sorry; Full Content Access is for Members only

Task 2 – Configure Controller Certificate Authorization as Enterprise Root



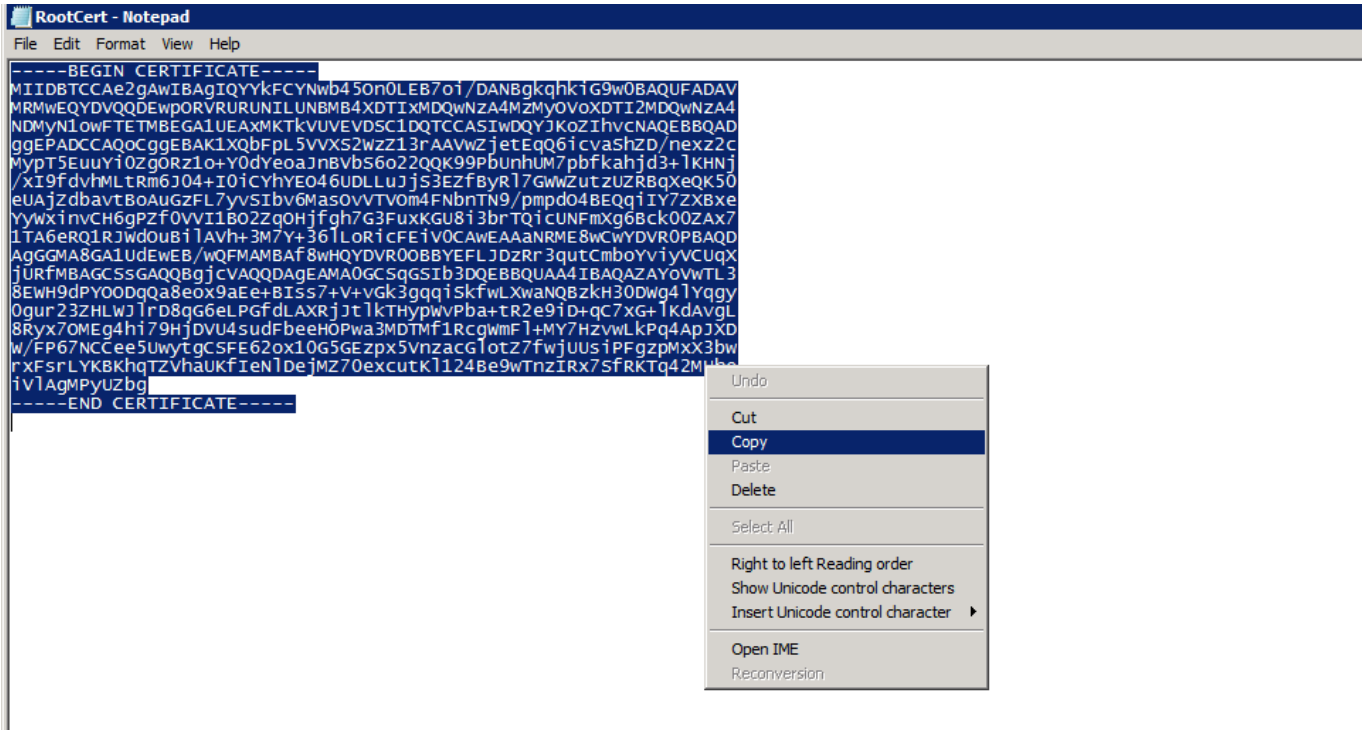
Task 3 – Download and Install Enterprise Root Certificate

- Log in to windows 2008 server machine
- Open Google Chrome and browse to http://192.168.0.54/certsrv
- Click “Download Root Certificate”.
- Select “Base 64”.
- Click “Download CA Certificate”.

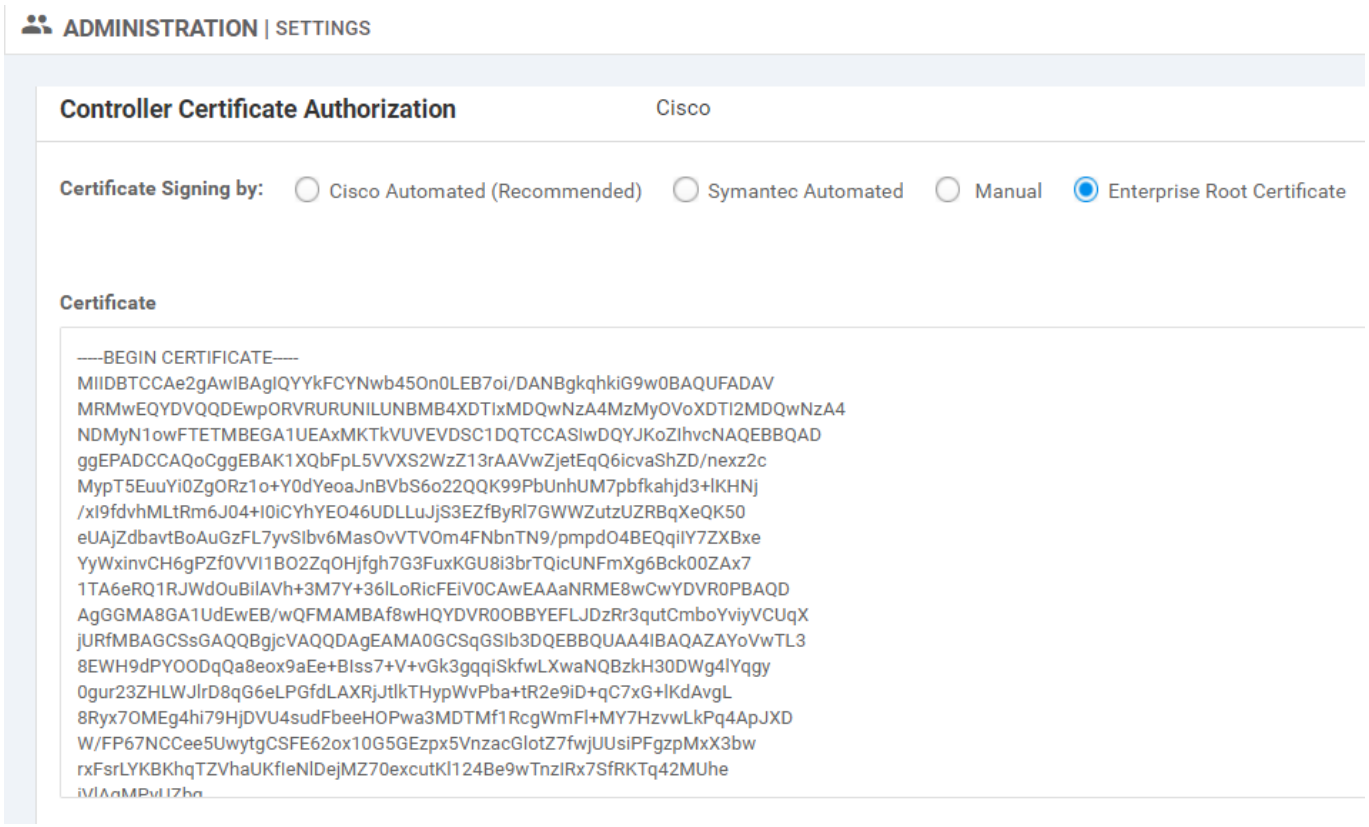


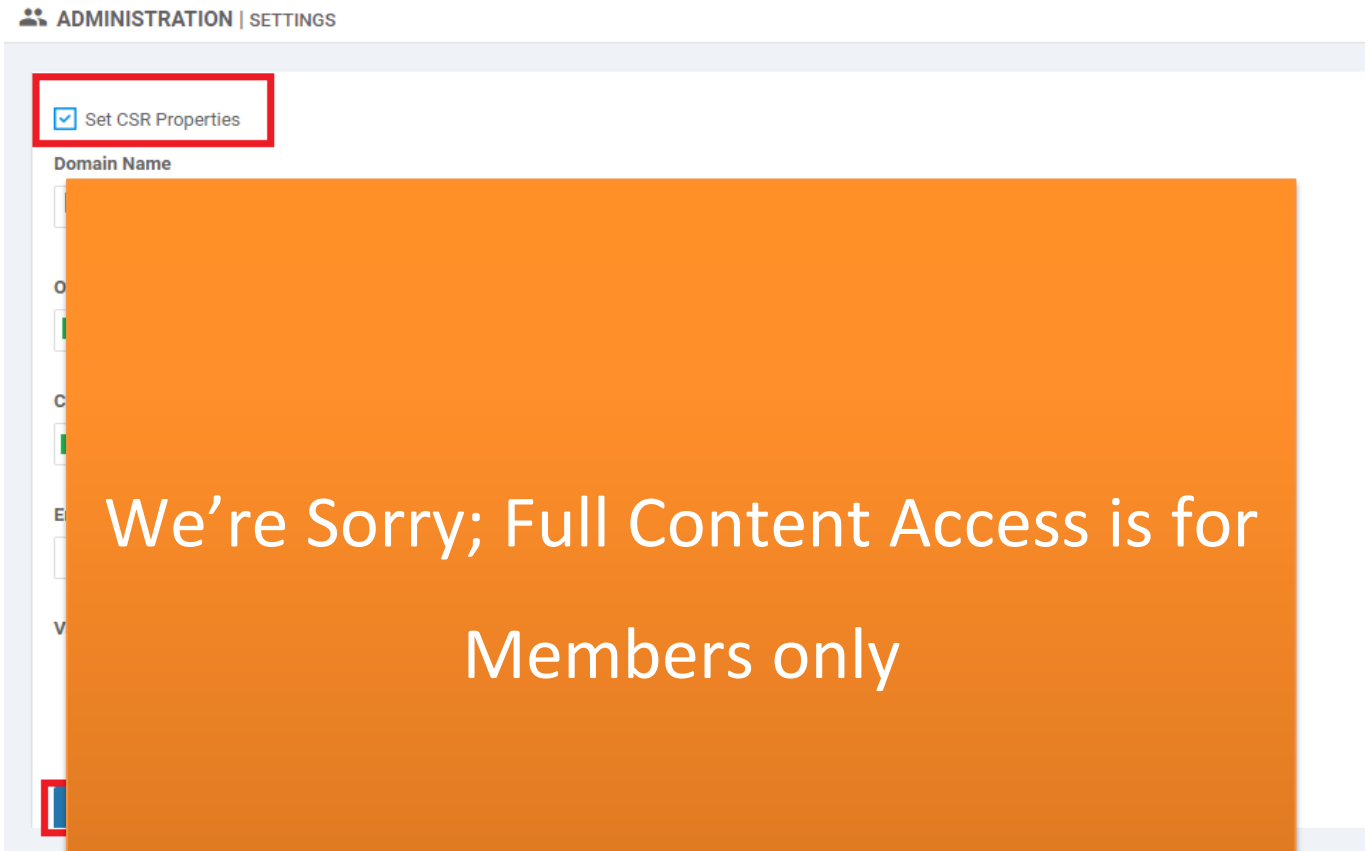
We’re Sorry; Full Content Access is for Members only

- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file "**Certnew**" to "**RootCert**".
- Open the "**RootCert.cer**" file using Notepad.
- Copy using CTRL-A and CTRL-C.



We're Sorry; Full Content Access is for Members only

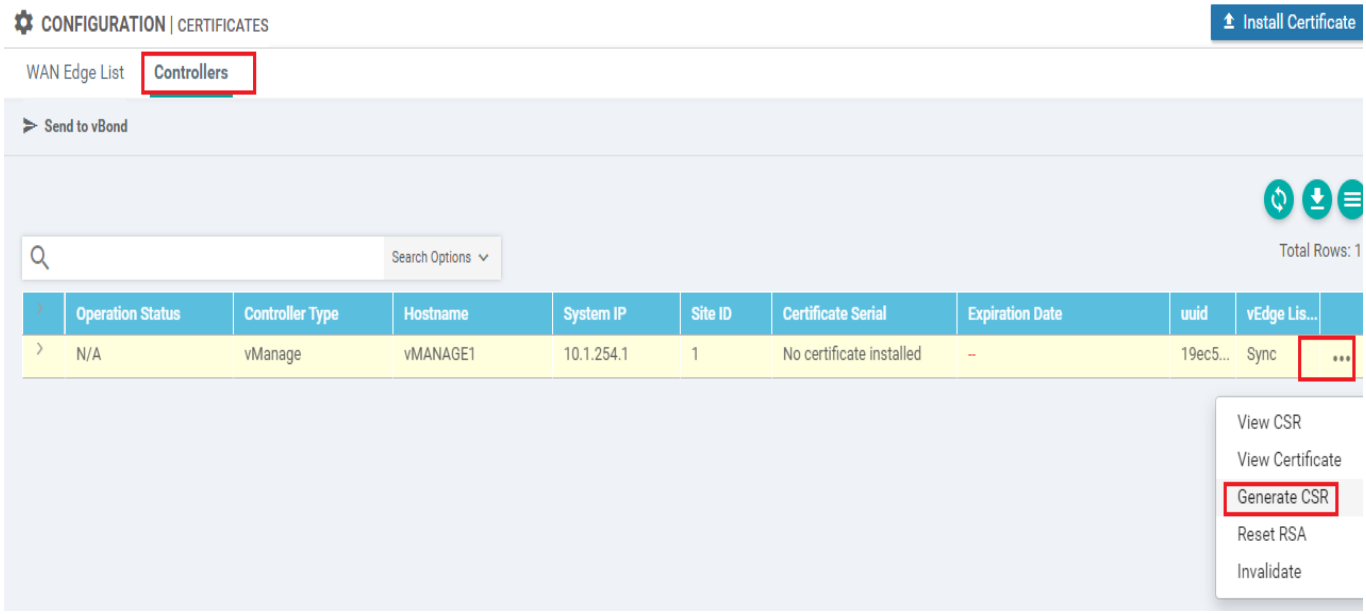




We’re Sorry; Full Content Access is for Members only

Task 4 – Generate a CSR for vManage

- Navigate to **Configuration -> Certificates -> Controllers -> vManage -> Generate CSR**
- It will open a window with the CSR. Copy by using **CTRL-A** and **CTRL-C.**



We're Sorry; Full Content Access is for Members only