Deployment CISCO

SD-WAN

LAB ON EVE-NG

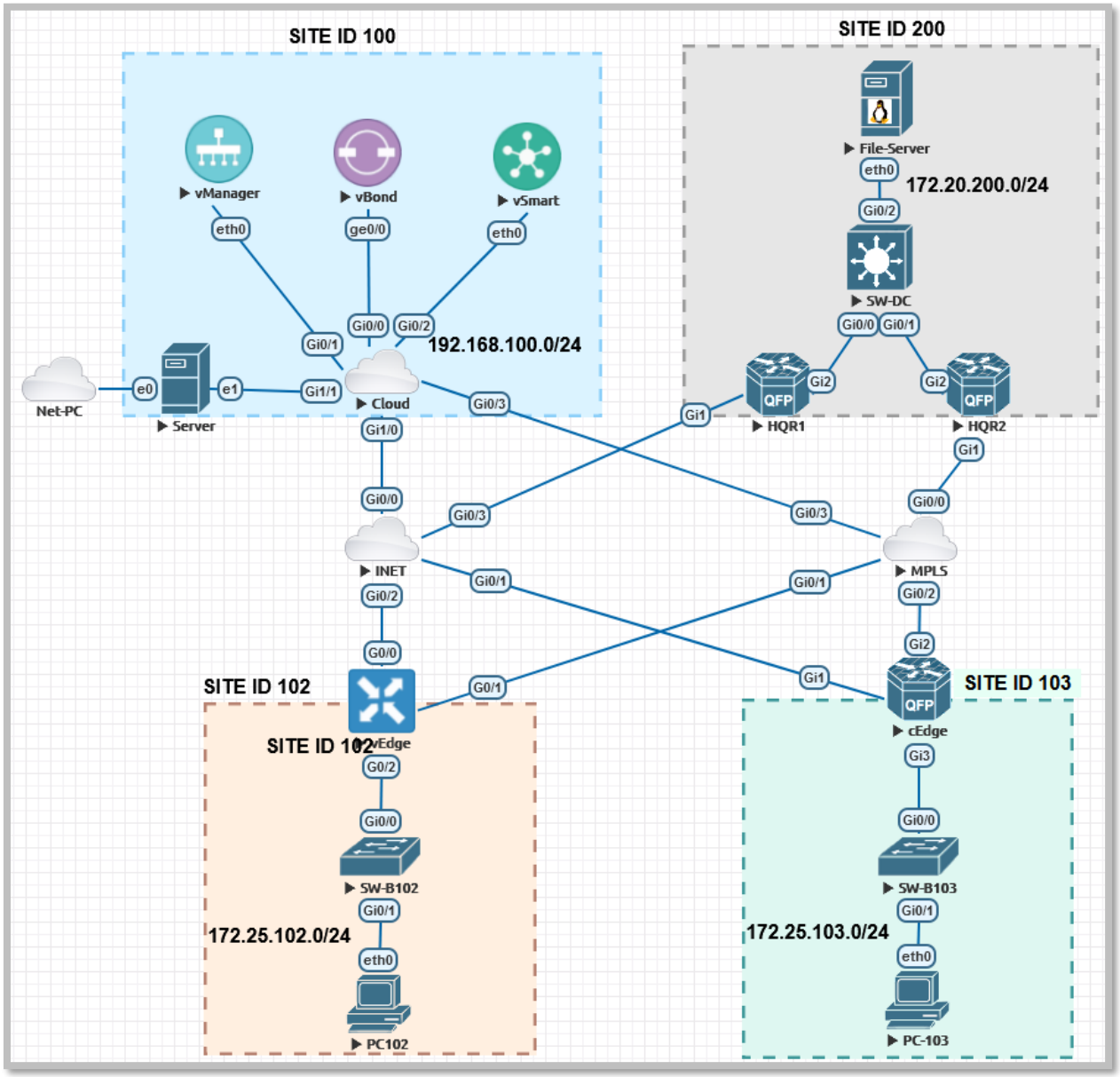
Mostafa-Rafati

SD-WAN LAB on Eve-ng

EVE-NG Requirements (Cisco SD-WAN)

1. Default Requirement (64G Ram,16 vCPU)
2. EVE-NG version: 2.0.3-105
3. QEMU version: 2.4.0
4. Add image
   - Windows Server 2012 (2 vCPU,8G RAM)
   - vIOS Advance Enterprise k9(2 vCPU,2G RAM)
   - CSR1000vng-ucmk9.16.12.1d-sdwan (2 vCPU,4G RAM)
   - Viptella Controller version 19.3
     - vManage (4 vCPU,24G RAM)
     - vBond (2 vCPU,2G RAM)
     - vSmart (2 vCPU,2G RAM)
     - vEdge (2 vCPU,2G RAM)

SD-WAN LAB Diagram on EVE-NG



Add Viptela Controller on EVE-NG

https://www.eve-ng.net/index.php/documentation/howtos/howto-add-cisco-viptela-images-set/

Deployment of Cisco Viptela vManage 19.3 image

1- SSH to EVE and login as root, from cli and create image directory on the EVE:

```
mkdir /opt/unetlab/addons/qemu/vtmgmt-19.3
```

2- Upload the downloaded `viptela-vmanage-19.3-genericx86-64.qcow2` image to the `/opt/unetlab/addons/qemu/vtmgmt-19.3` using FileZilla or WinSCP

3- Go to image location and rename uploaded image to `hda.qcow2`

```
cd /opt/unetlab/addons/qemu/vtmgmt-19.3

mv viptela-vmanage-19.3-genericx86-64.qcow2 hda.qcow2
```

4- IMPORTANT: Create additional (Second!) storage 100Gb HDD `hdb.qcow2`

```
/opt/qemu/bin/qemu-img create -f qcow2 hdb.qcow2 100G
```

Deployment of Cisco Viptela vSmart 19.3 image

5- SSH to EVE and login as root, from cli and create temporary working directory on the EVE's root:

```
mkdir /opt/unetlab/addons/qemu/vtbond-19.3
```

1- Upload the downloaded `viptela- smart-19.3-genericx86-64.qcow2` image to the `/opt/unetlab/addons/qemu/ vtsmart-19.3` using FileZilla or WinSCP

2- Go to image location and rename uploaded image to `hda.qcow2`

```
cd /opt/unetlab/addons/qemu/vtbond-19.3
mv viptela-edge-19.3-genericx86-64.qcow2 hda.qcow2
cd
```

Deployment of Cisco Viptela vBond 19.3 image

3- SSH to EVE and login as root, from cli and create image directory on the EVE:

```
mkdir /opt/unetlab/addons/qemu/vtedge-19.3
```

1- Upload the downloaded `viptela- smart-19.3-genericx86-64.qcow2` image to the `/opt/unetlab/addons/qemu/ vtsmart-19.3` using FileZilla or WinSCP

2- Go to image location and rename uploaded image to `hda.qcow2`

```
cd /opt/unetlab/addons/qemu/vtedge-19.3
mv viptela-edge-19.3-genericx86-64.qcow2 hda.qcow2
cd
```

3- Fix permissions

```
cd
/opt/unetlab/wrappers/unl_wrapper -a fixpermissions
```

Add WAN-Edge on EVE-NG

Add Viptela vEdge 19.3 image on EVE-NG

1- SSH to EVE and login as root, from cli and create working directory on the EVE's root:

```
mkdir /opt/unetlab/addons/qemu/vtedge-19.3
```

2- Upload the downloaded **`viptela-edge-19.3-genericx86-64.qcow2`** image to the **`/opt/unetlab/addons/qemu/vtedge-19.3`** using FileZilla or WinSCP.
3- Go to image location and rename uploaded image to **`hda.qcow2`**

```
cd /opt/unetlab/addons/qemu/vtedge-19.3
mv viptela-edge-19.3-genericx86-64.qcow2 hda.qcow2
cd
```

Add CSR1000v SD-WAN on EVE-NG

1- SSH to EVE and login as root, from cli and create image directory in the EVE:

```
mkdir /opt/unetlab/addons/qemu/ CSR1000vng-ucmk9.16.12.1d-sdwan
```

2- Upload the downloaded **`CSR1000vng-ucmk9.16.12.1d-sdwan`** image to the EVE using for example FileZilla or WinSCP.
3- Go to image directory and rename original filename to **`virtioa.qcow2`**:

```
cd /opt/unetlab/addons/qemu/CSR1000vng-ucmk9.16.12.1d-sdwan
```

4- Rename original filename to **`virtioa.qcow2`**

```
mv csr1000v-ucmk9.16.12.1d-serial.qcow2 virtioa.qcow2
```

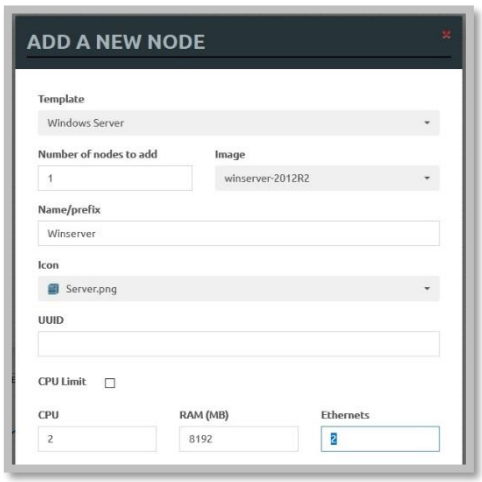
5- Fix permissions:

```
cd
/opt/unetlab/wrappers/unl wrapper -a fixpermissions
```

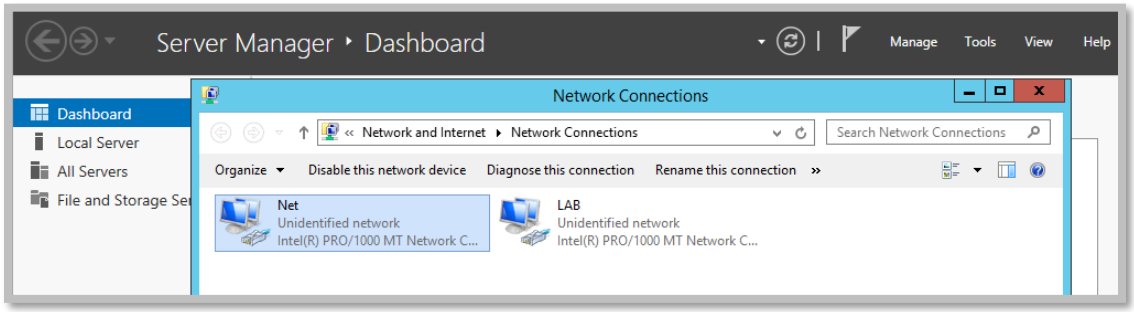
Windows Server Active Directory & Certificate Server

Pre requirement for Active Directory Certificate Server

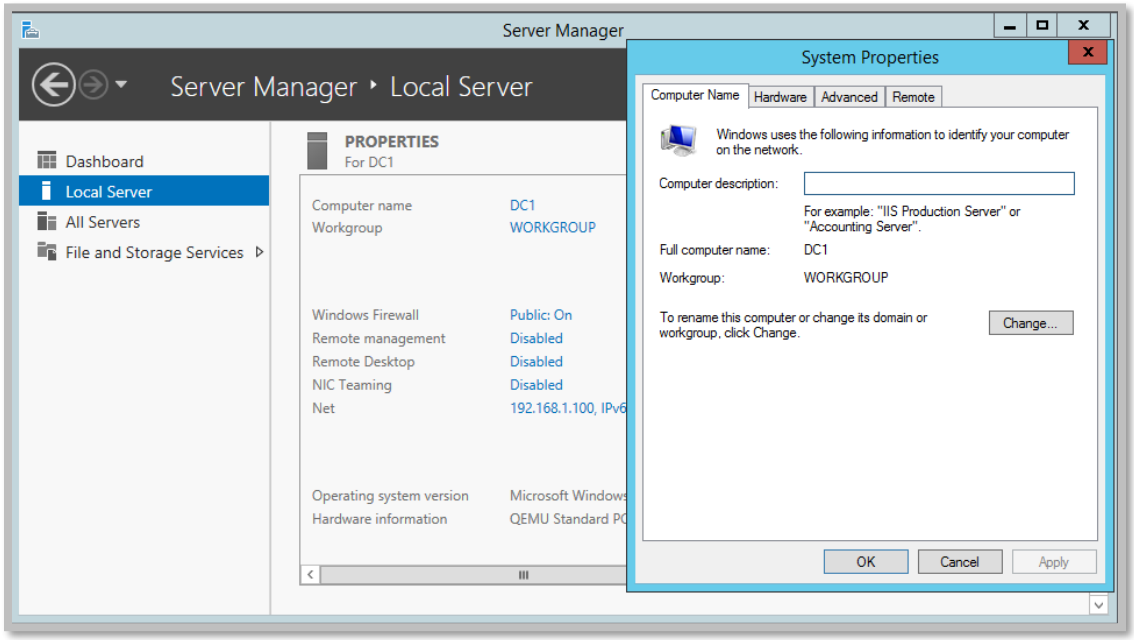
1. Add Node `Windows Server 2012` with `2 Ethernet`
2. Start `Windows Server 2012` `Node,` Then `Login to Windows Server 2012`



3. Set Static `IP` Address for `Lab & Net Network Adaptor`
   Note: LAB network adapter used for connecting SD-WAN lab and Net network adapter for connection to your host

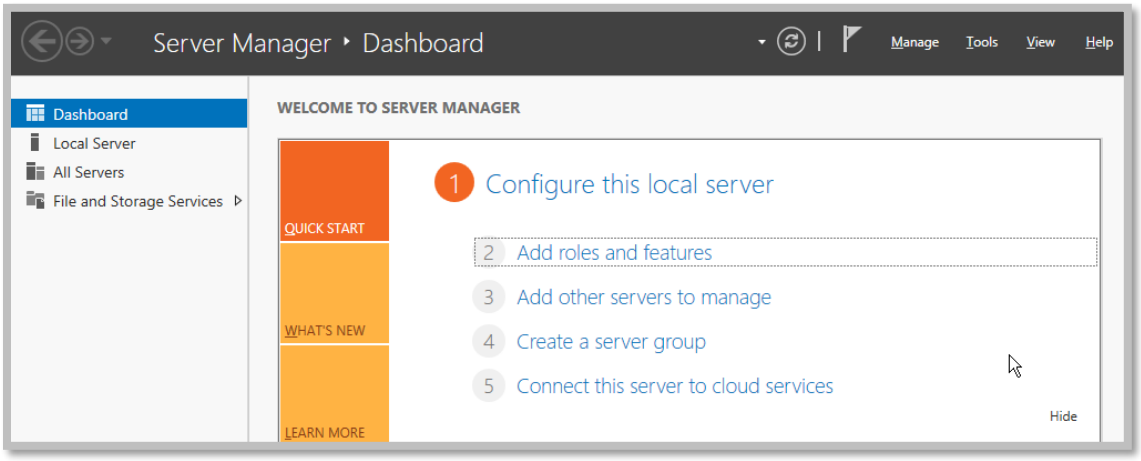


4. On `Server Manager > Local Server` change `Computer Name (Restart required)`

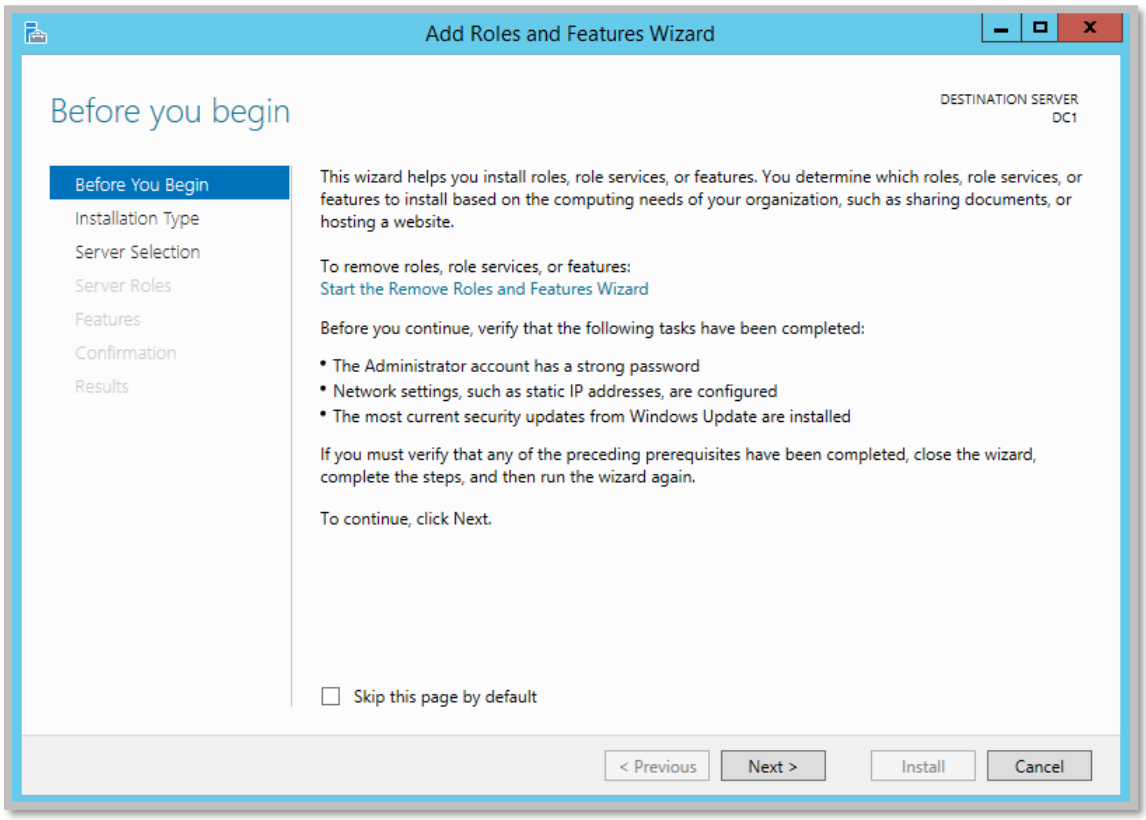


Active Directory Installation

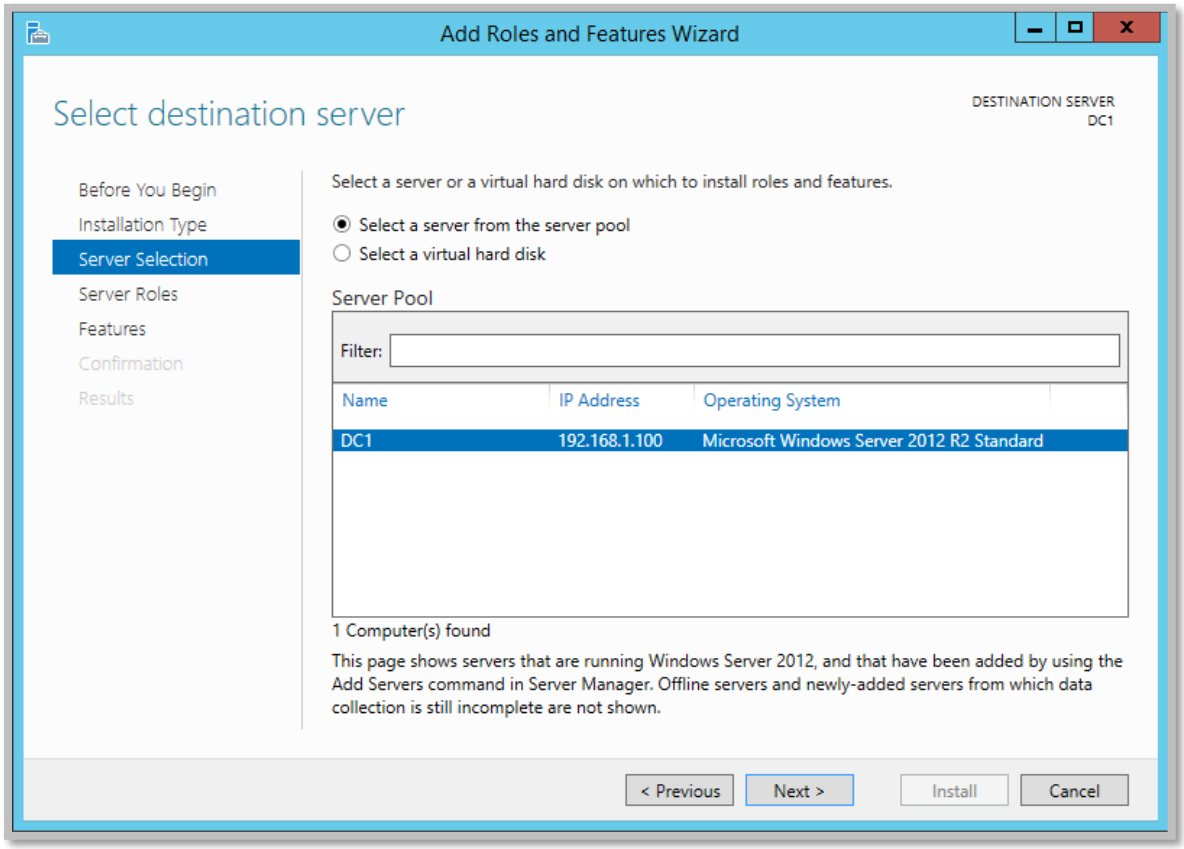
1. On `Server Manager -> Dashboard`
2. Select Add `Role and Feature`



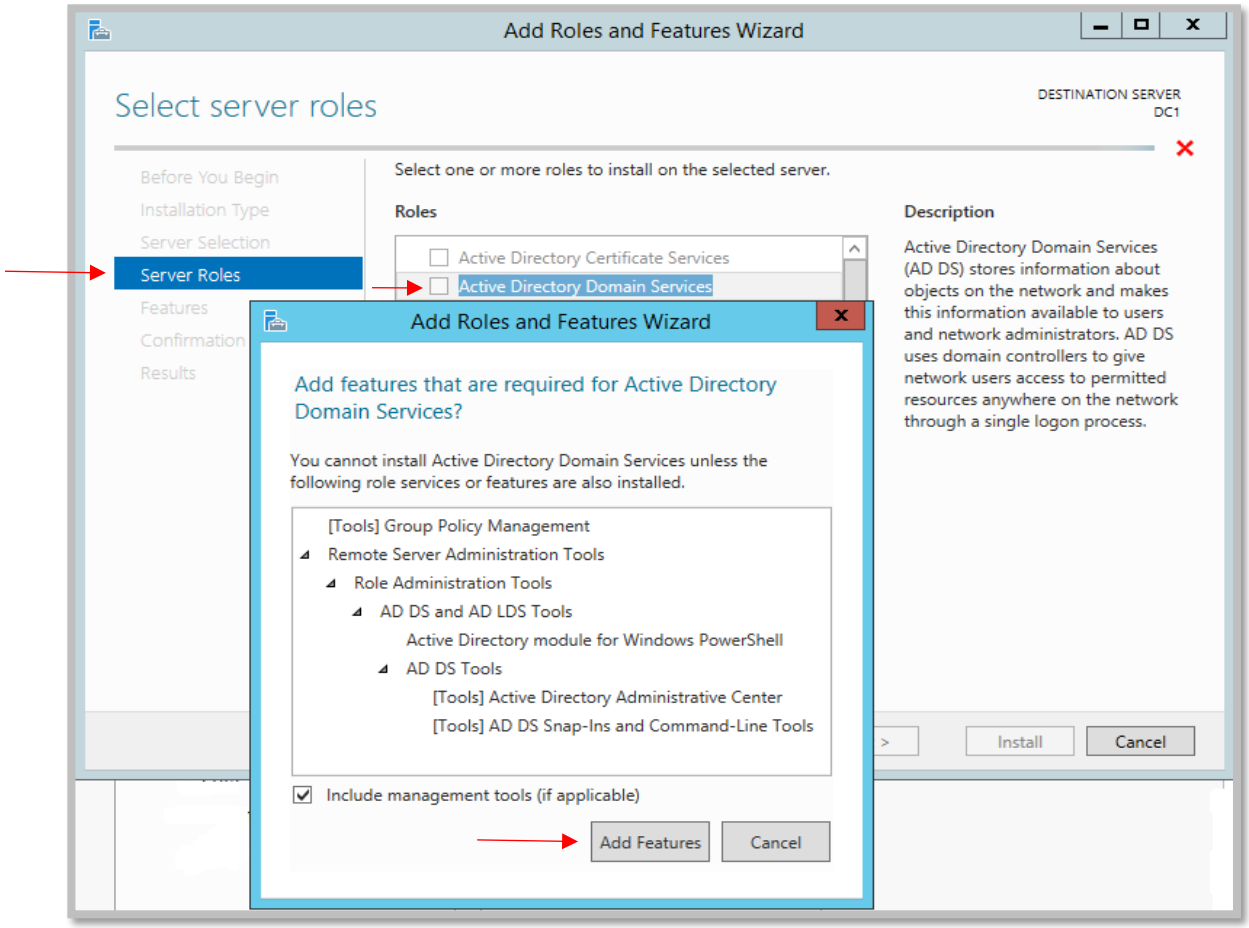
3. On Before You Begin Page Select `Next`



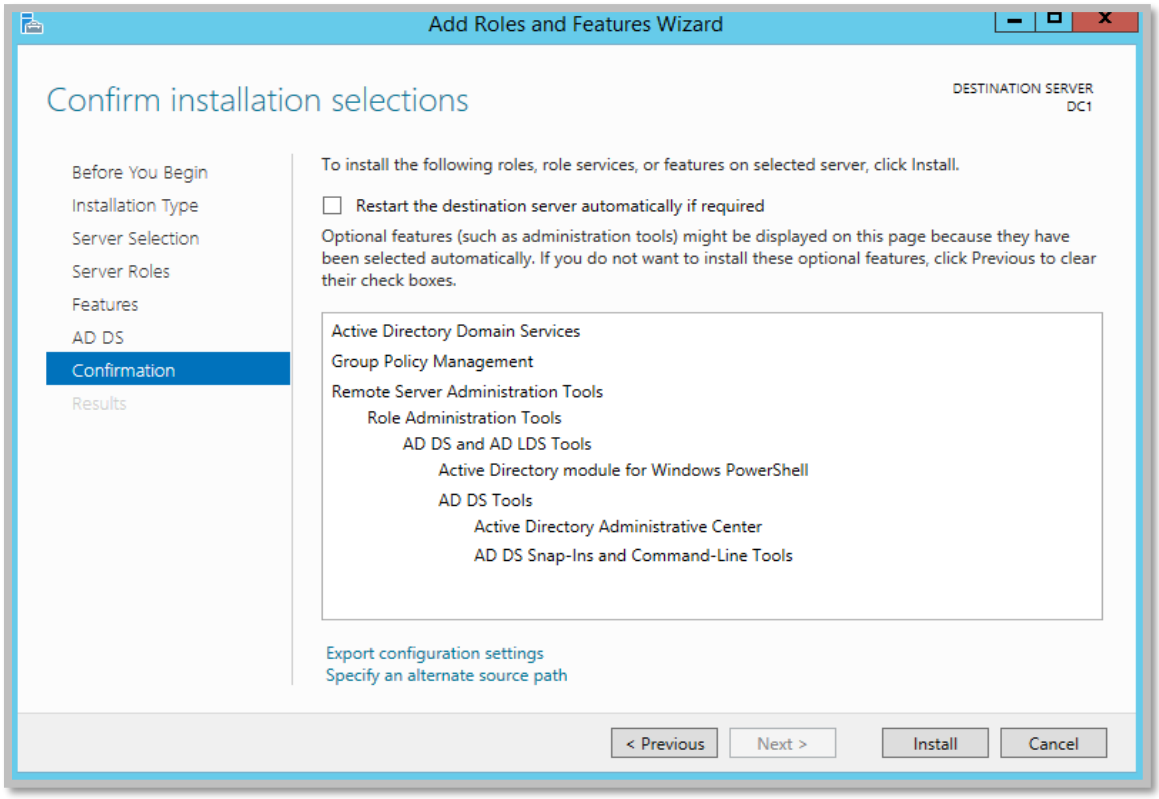
4. On Installation type page, select `Role-base or Feature-base Installation` then Select `Next`
5. On Server selection page, select `DC1` Server then select `Next`



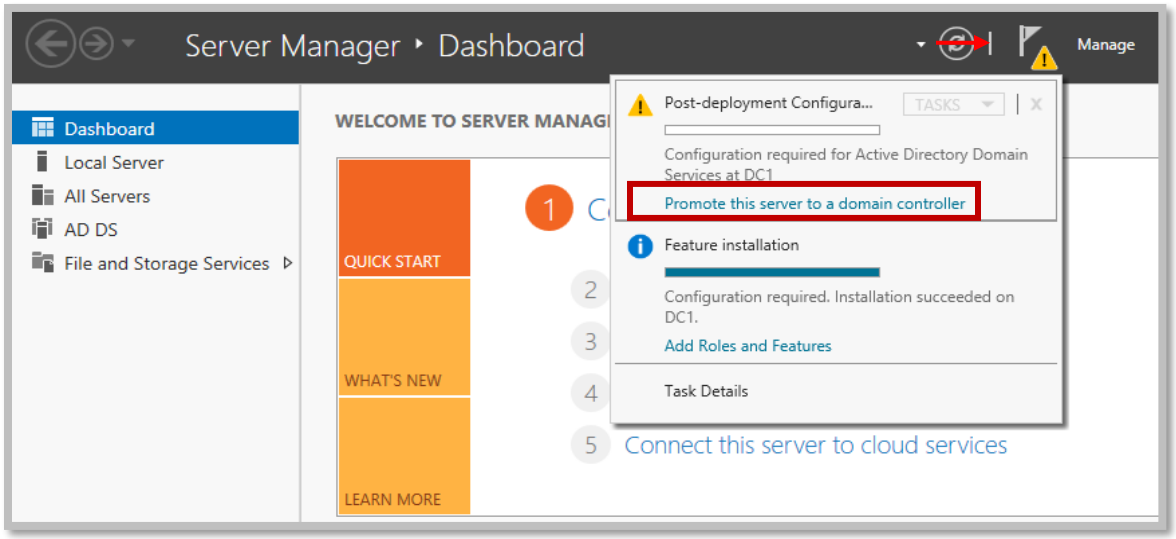
6. on Server Role page, select `Active Directory Domain Services` then click `Add Feature`



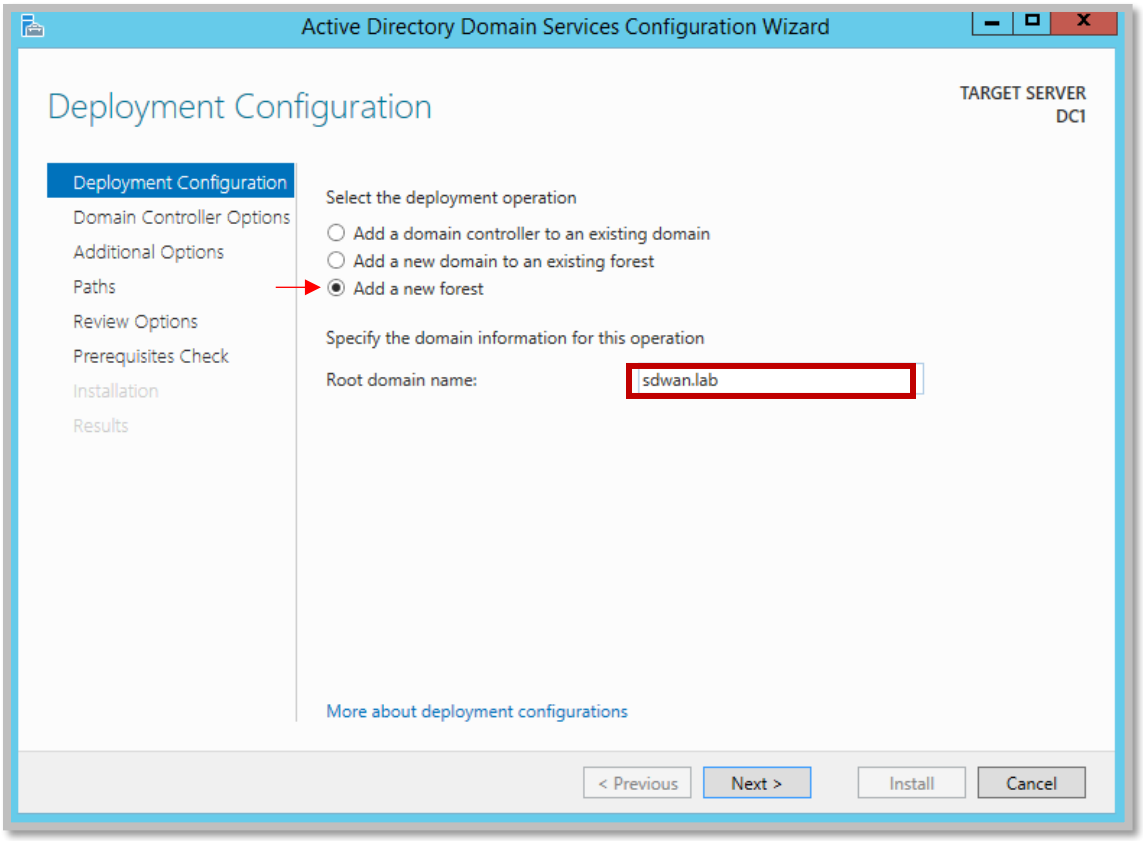
7. Select `Next` on `Features and AD DS` page, then click `Install`



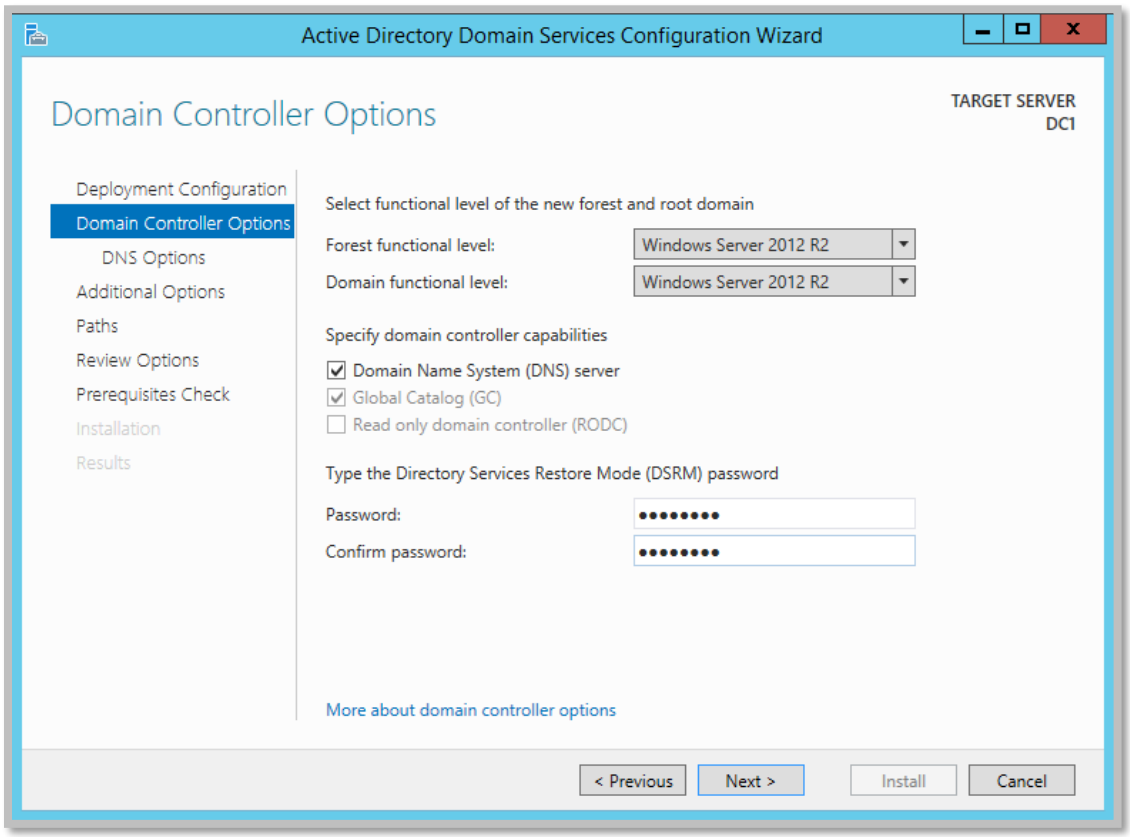
8. Click notification on server manager, select `Promote this Server to a domain Controller`



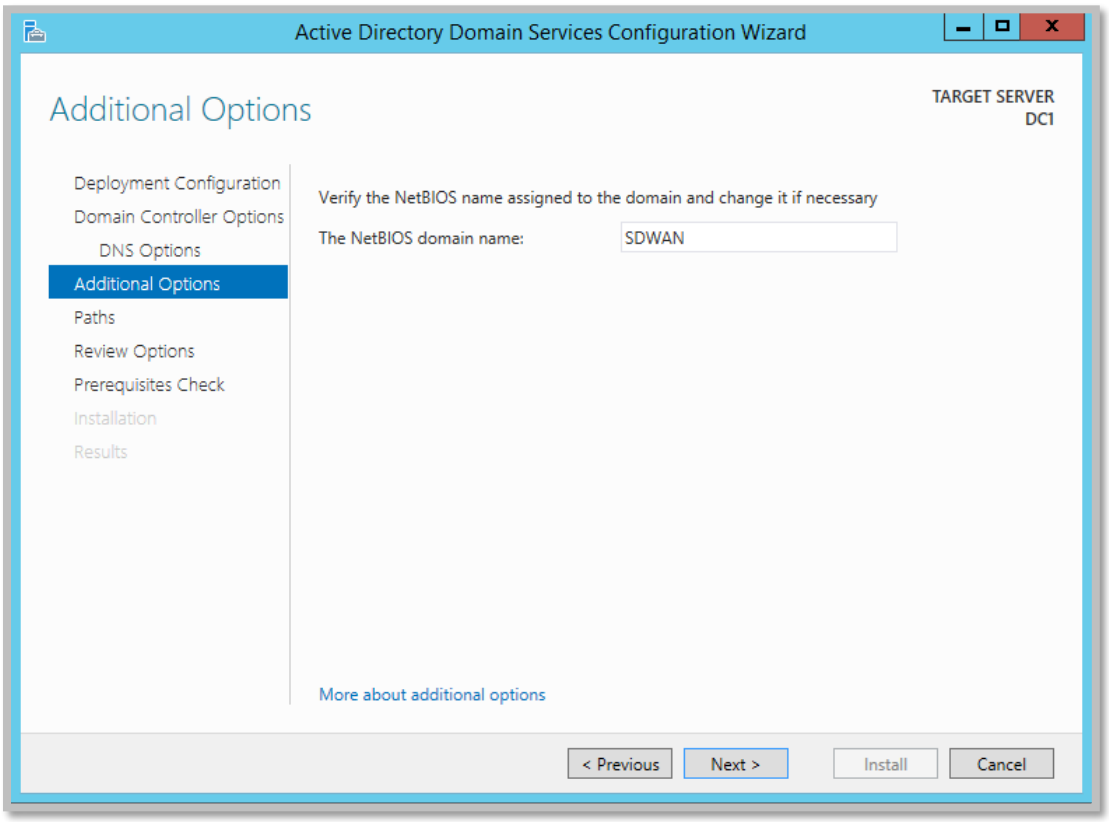
9. Select `Add a new Forest.` Root Domain name: `sdwan.lab`



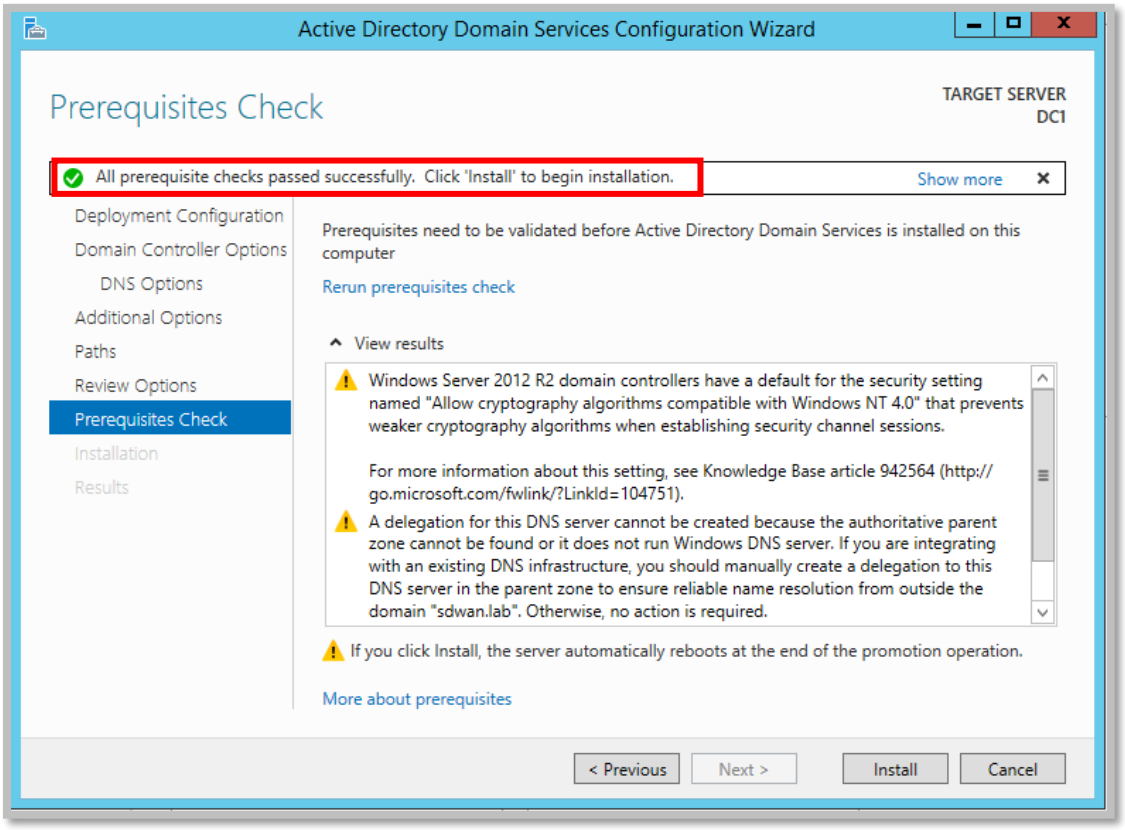
10. on Domain Controller Options, Type DSRM `Password` then click `Next`



11. Select `Next` on `DNS Option` page
12. On Additional option page, Check `NetBIOS Domain name`

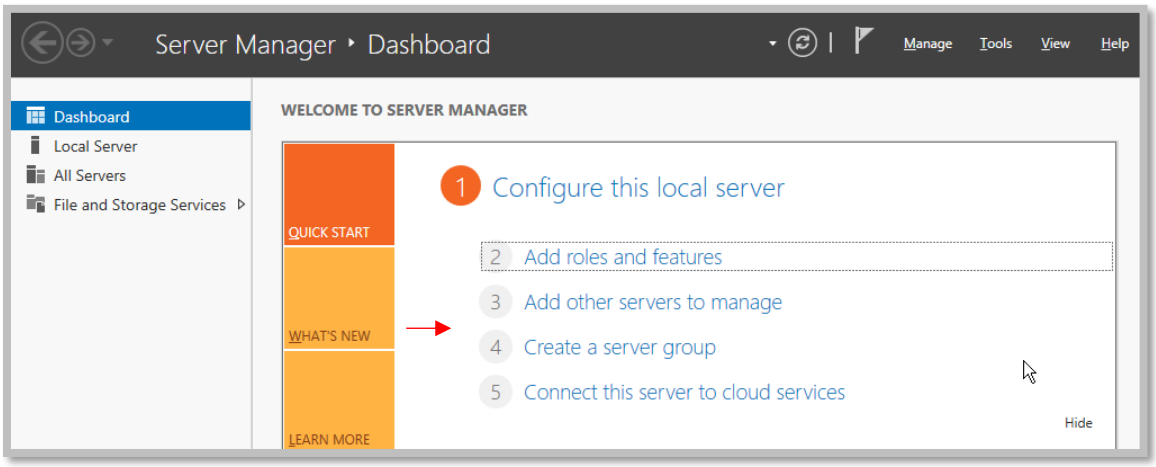


13. On Paths and Review Check page, select `Next`
14. On Prerequisites Check page, if same in the picture, select `Install`

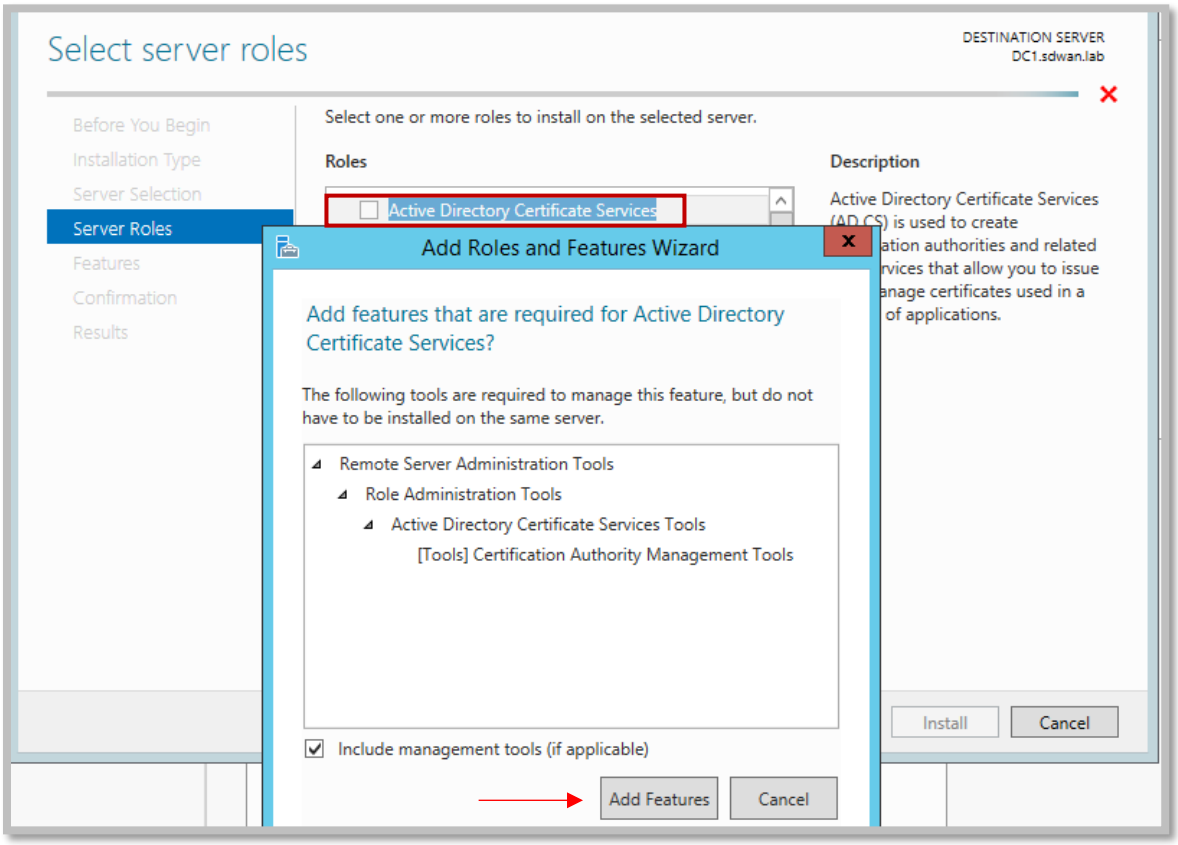


Active Directory Certificate Server Installation

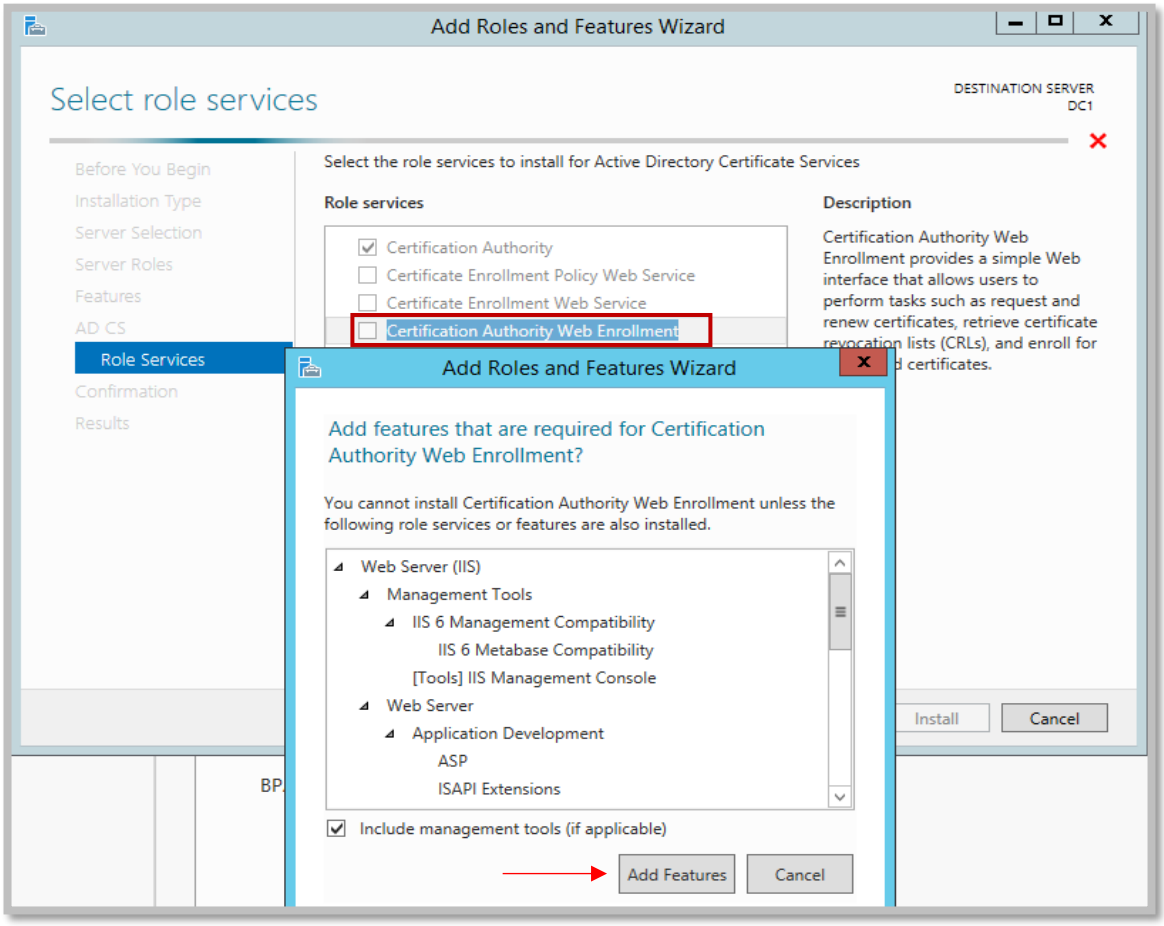
15. Now login to windows server AD Domain
16. On `Server Manager -> Dashboard`
17. Select `Add Role and Feature`



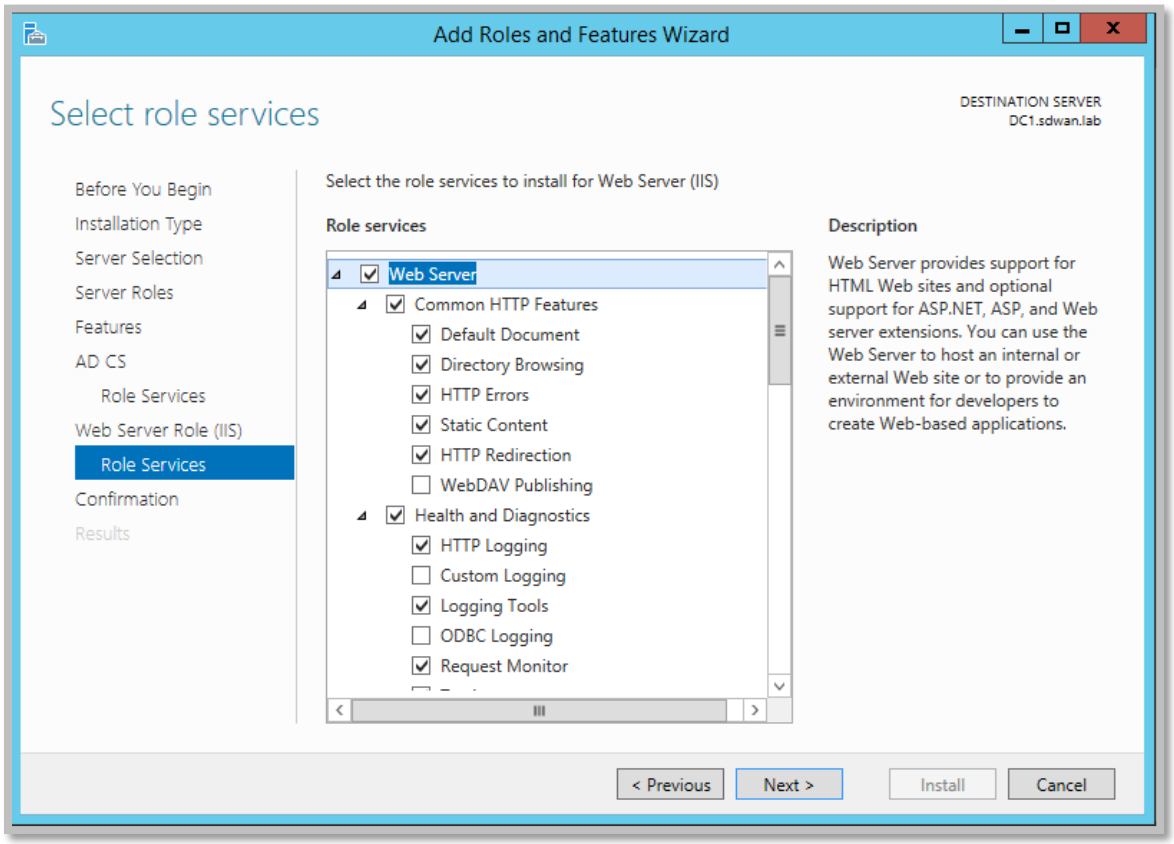
1. Base Steps 9-12 Select `Next`
2. on Server Roles page, Select `Active Directory Certificate Server`
3. Then select `Add Features`



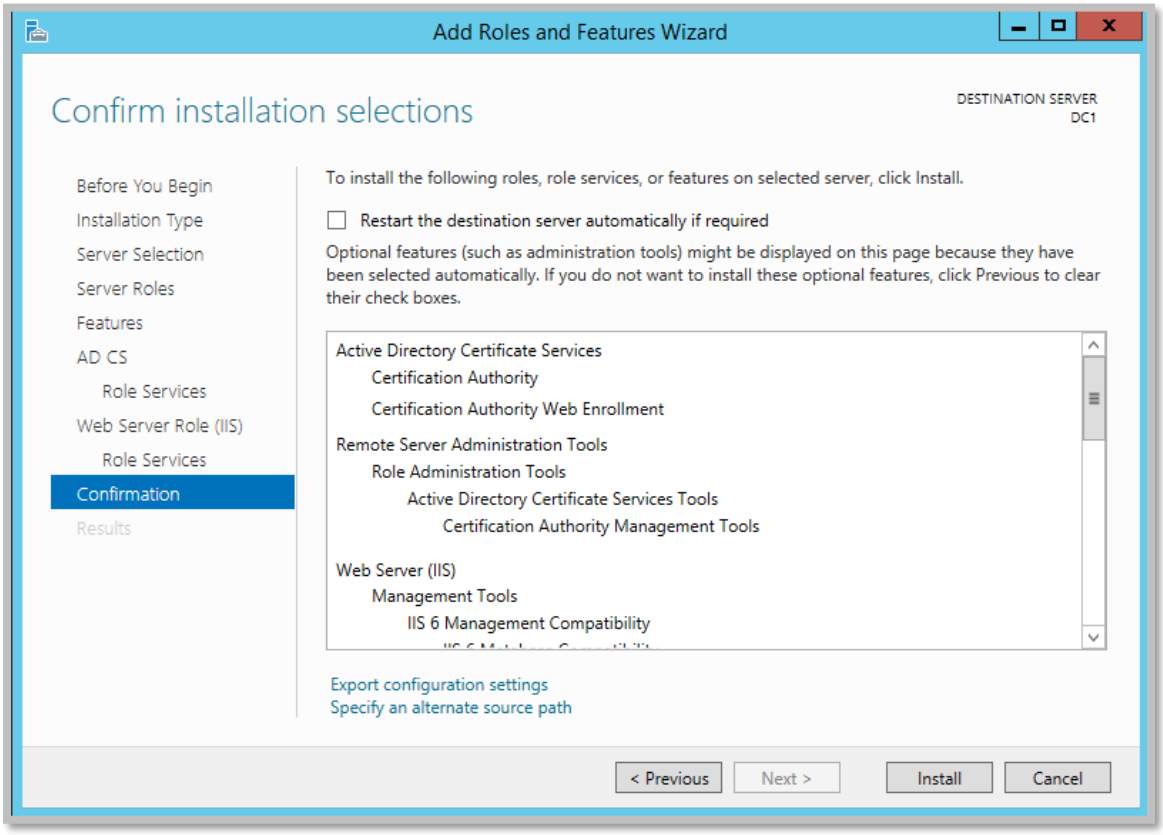
4. Select `Next` on `Features` page
5. On AD CS Role Services page, select `Certificate Authority Web Enrollment, then select Add Features`



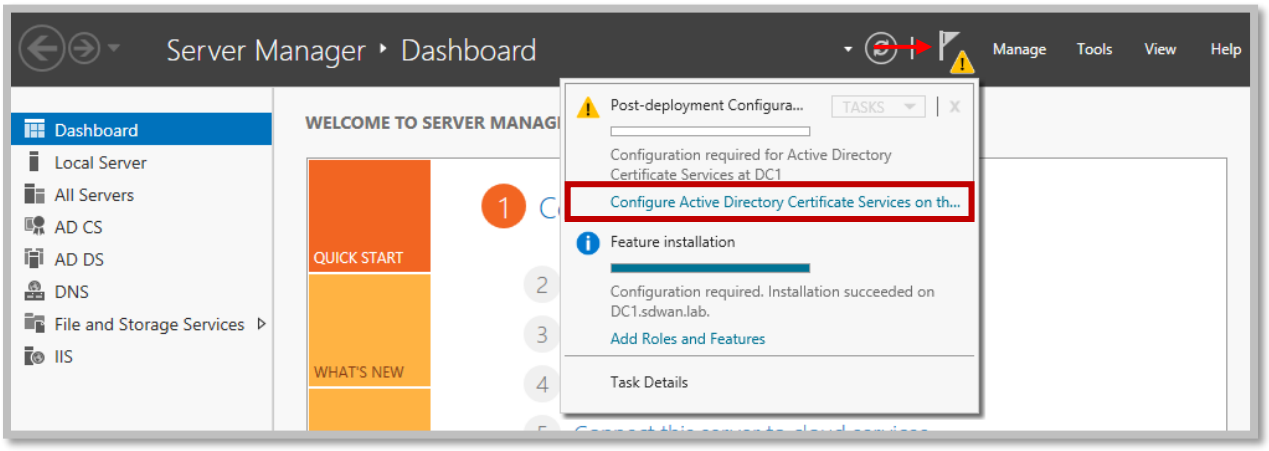
6. Select **`Next`** on **`Web Server Rolle(IIS)`** and **`Role Services`**



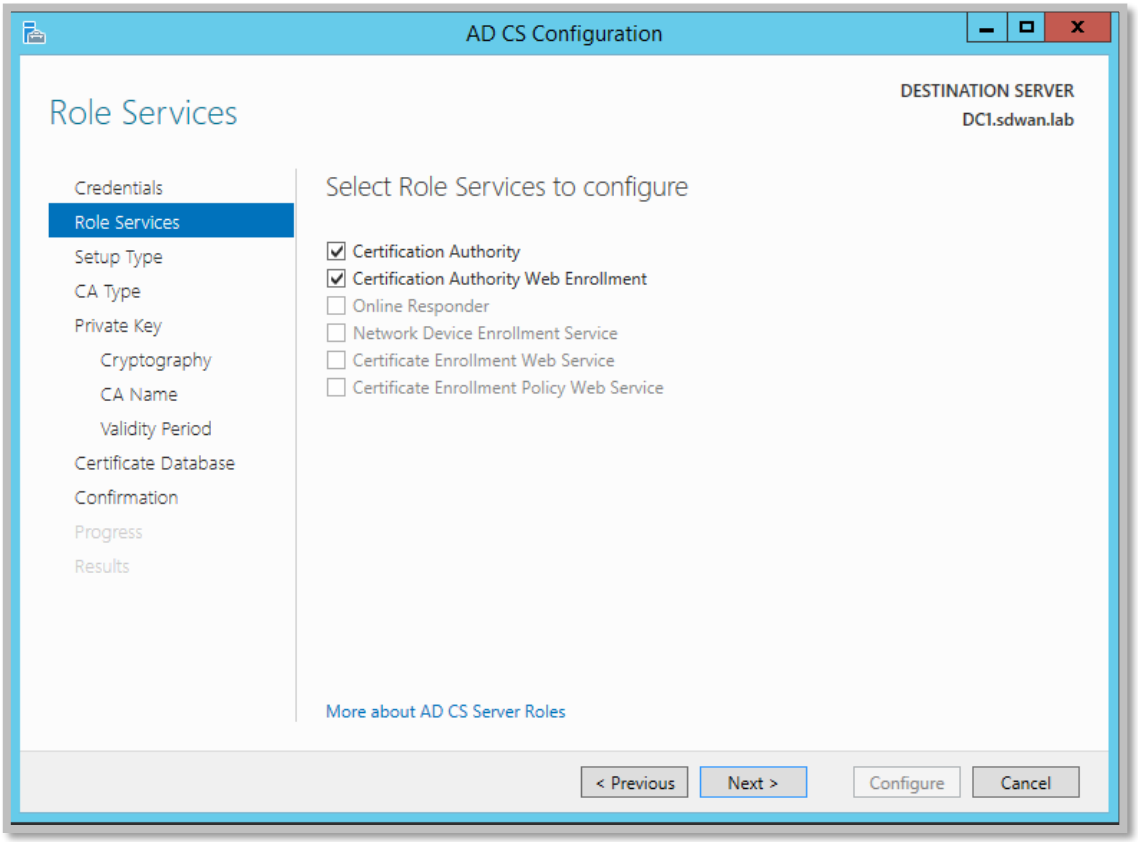
7. On **Confirmation** Page Select **Install**



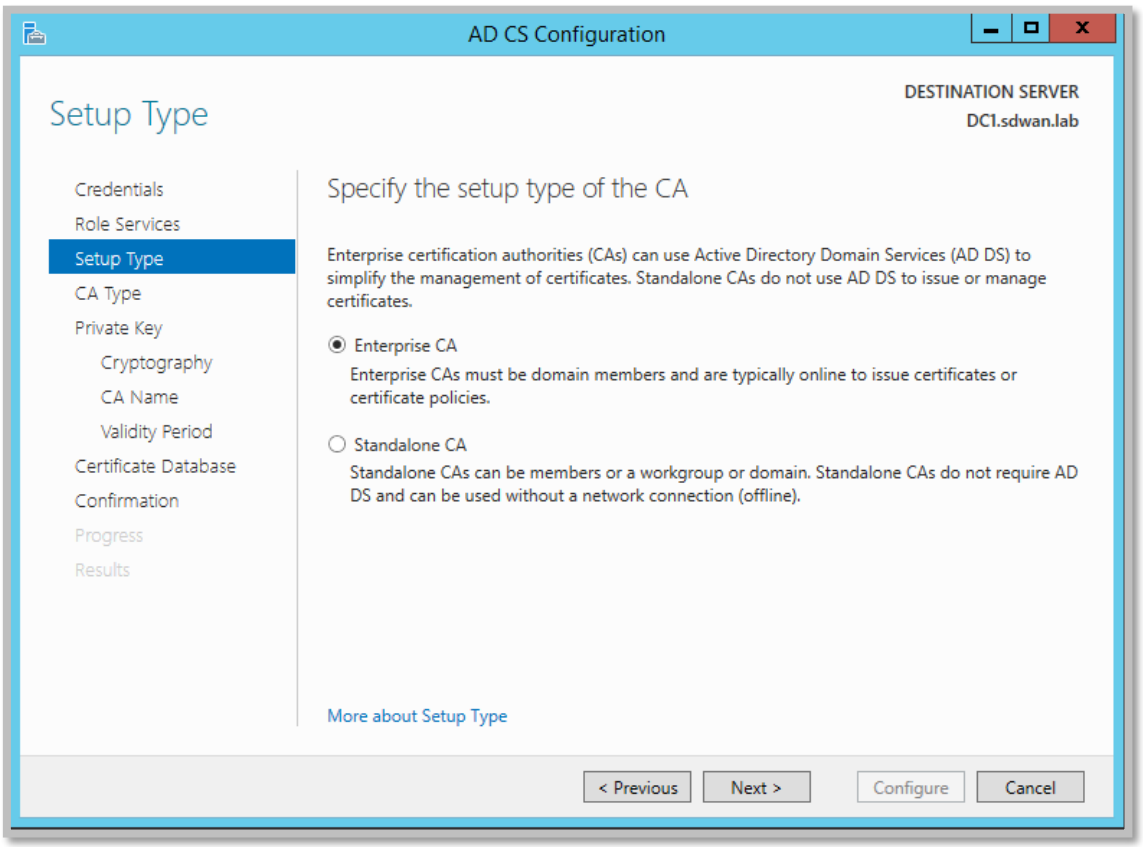
8. Select Notification, then select **Configure Active Directory Certificate Service on th..**



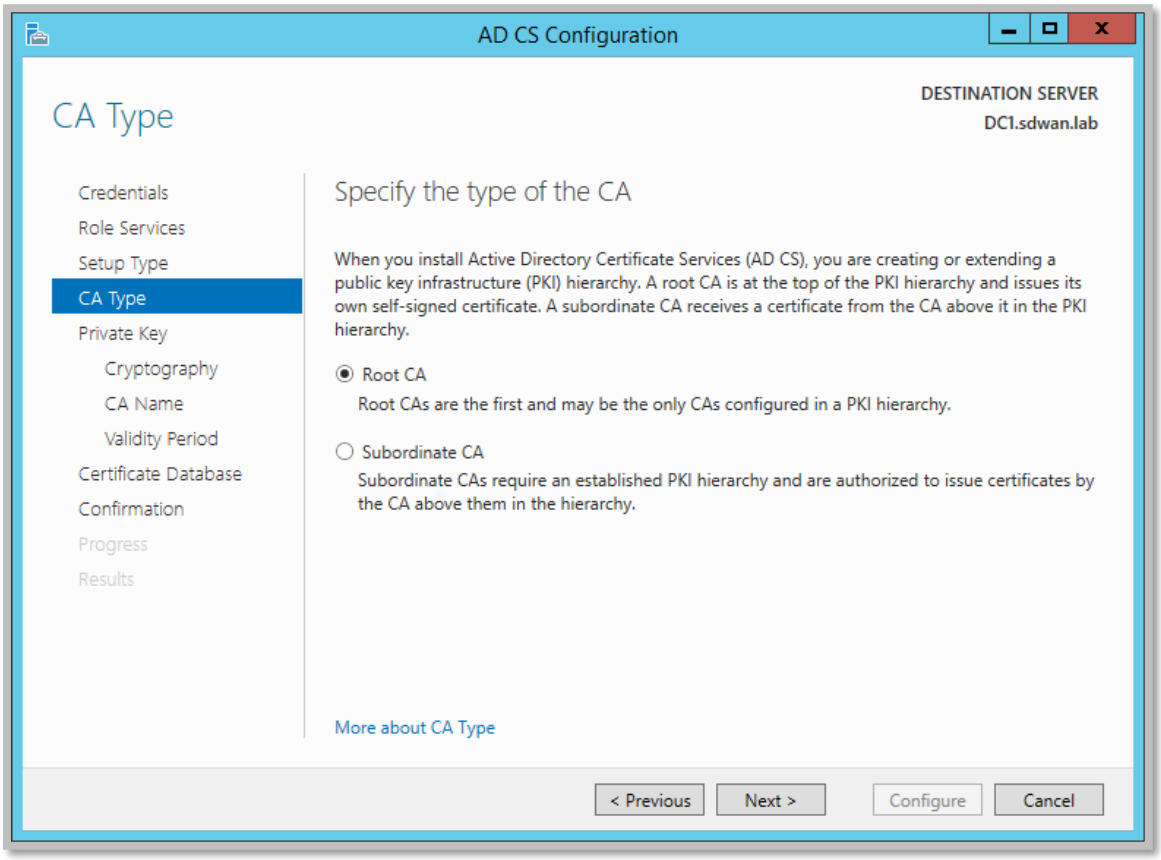
9. On **Credential** page **Click Next**
10. On **role services** page select **Certificate Authority and Certificate Authority Web Enrollment**



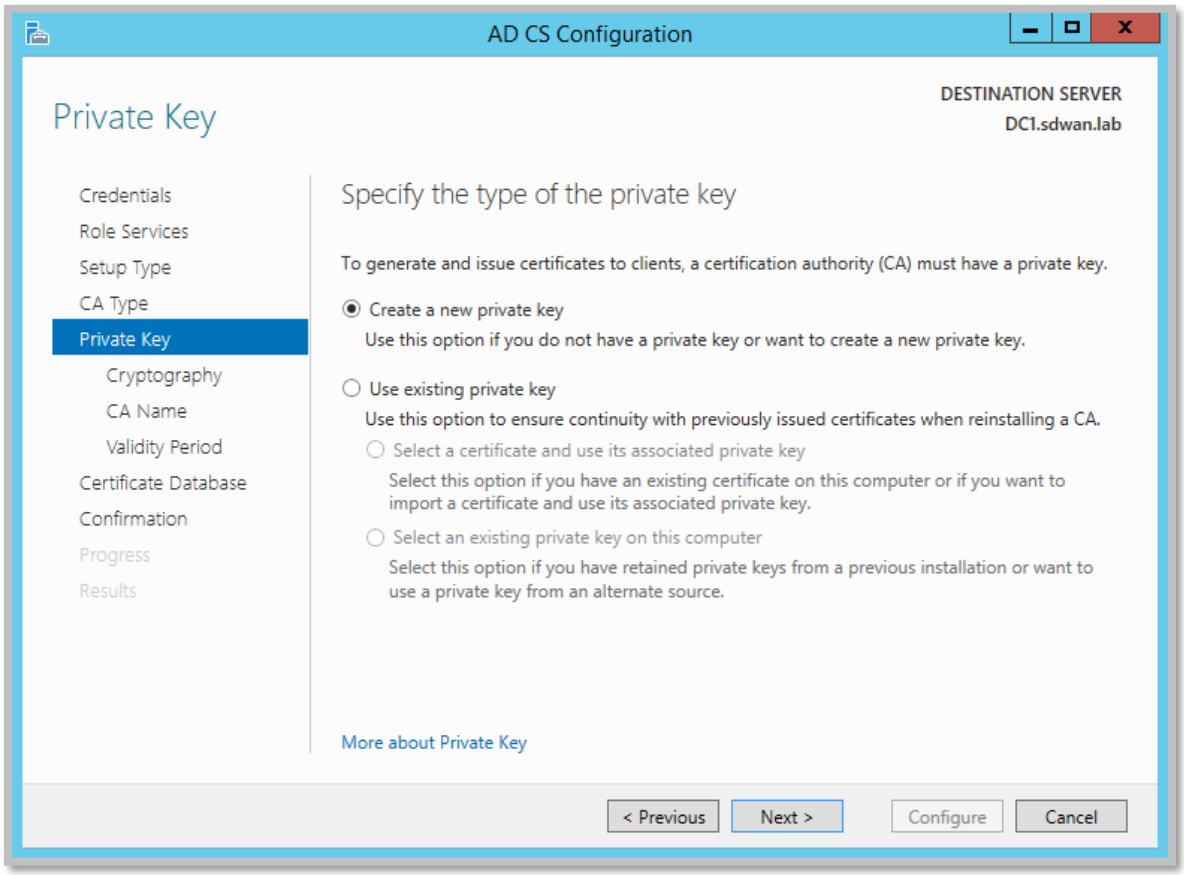
11. On `Setup type` page Select `Enterprise CA` then click Next



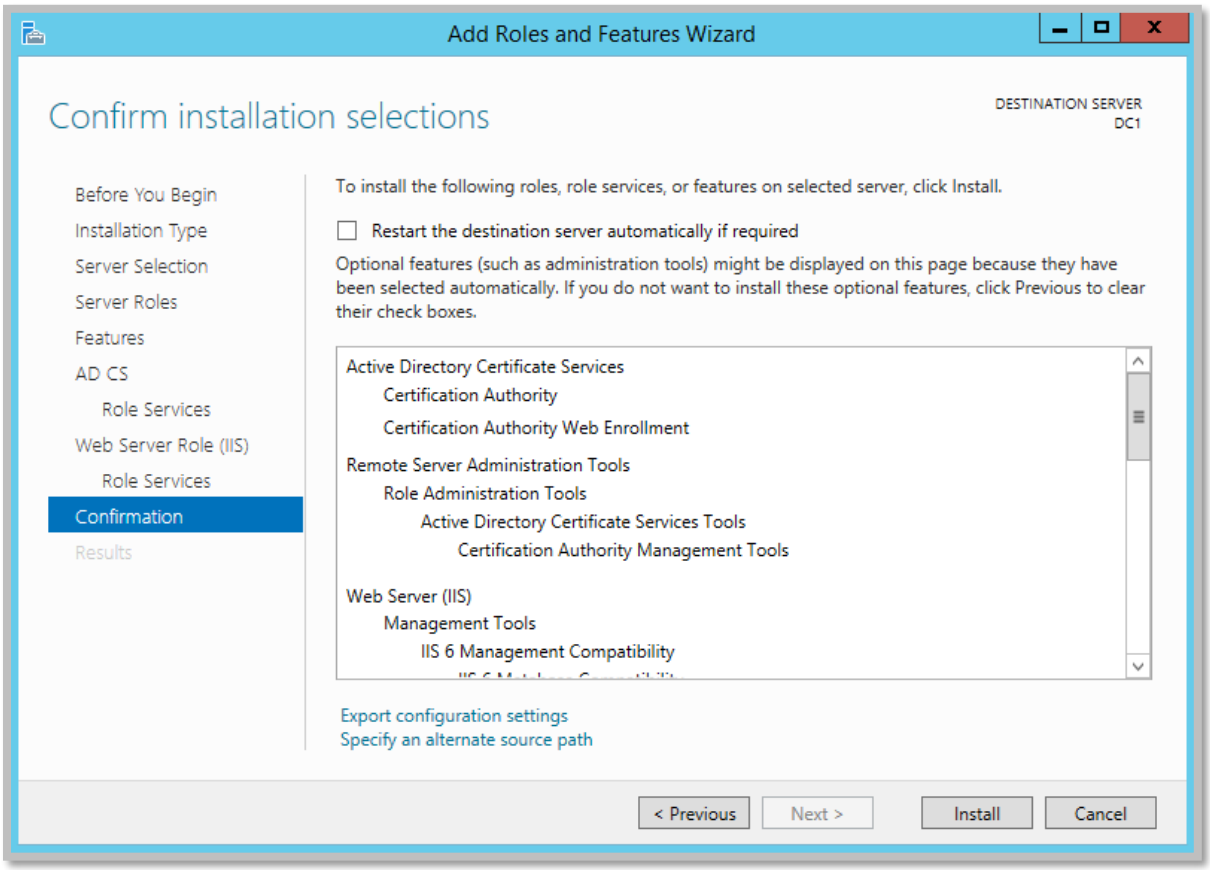
12. On `CA Type` Select `Root CA` and Click `Next`



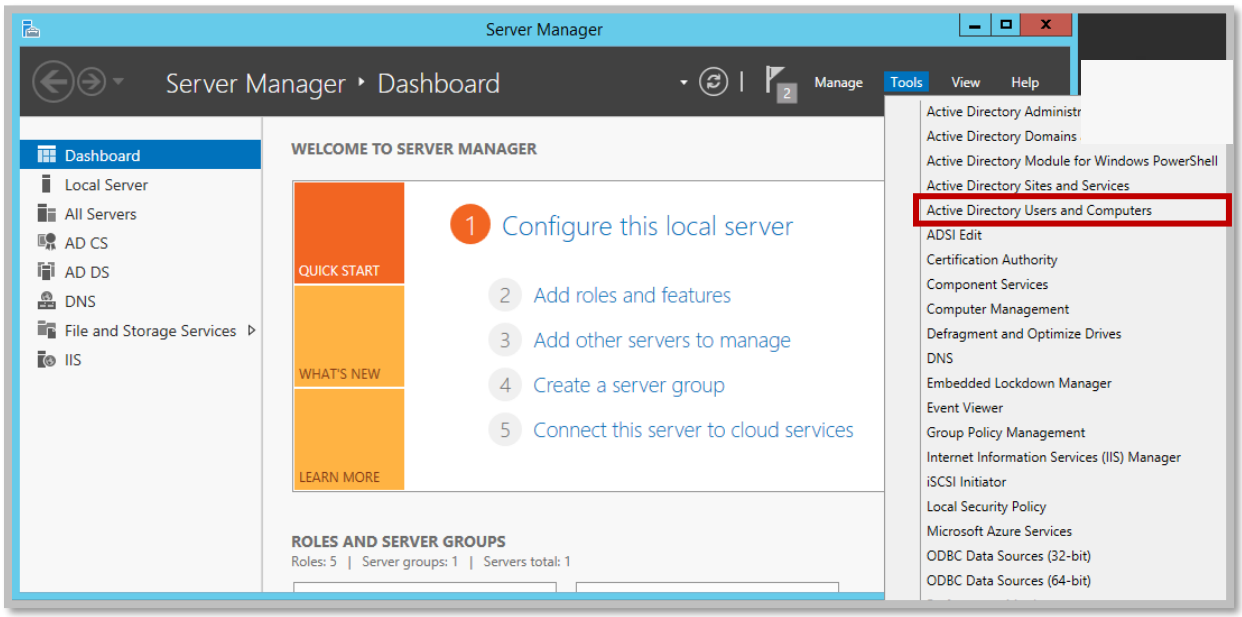
13. On `Private Key` page select `Create a new Private key`



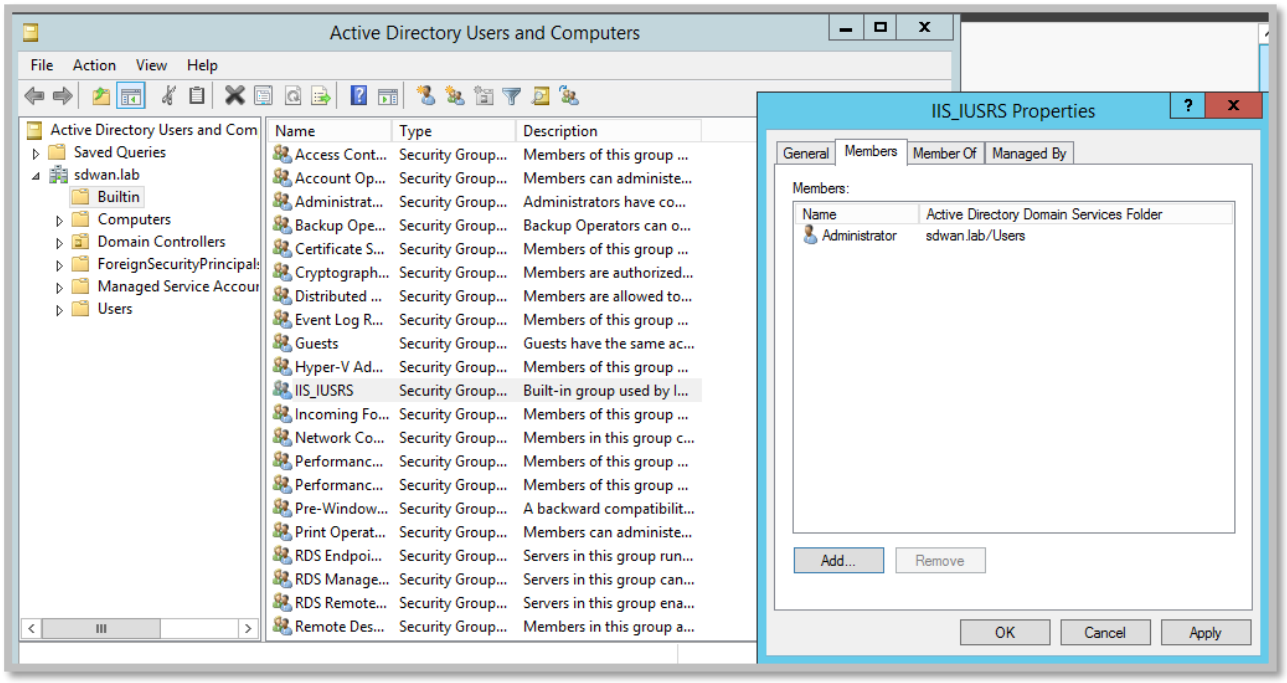
14. On **`Cryptography`** Select **`Next`**
15. On **`CA name`** page, Select **`Next (Nothing Change)`**
16. On **`Validity Period`** page select **`Next`**
17. On **`Certificate Database`** page select **`Next`**
18. On **`Confirmation`** page Click next an **`configure`**



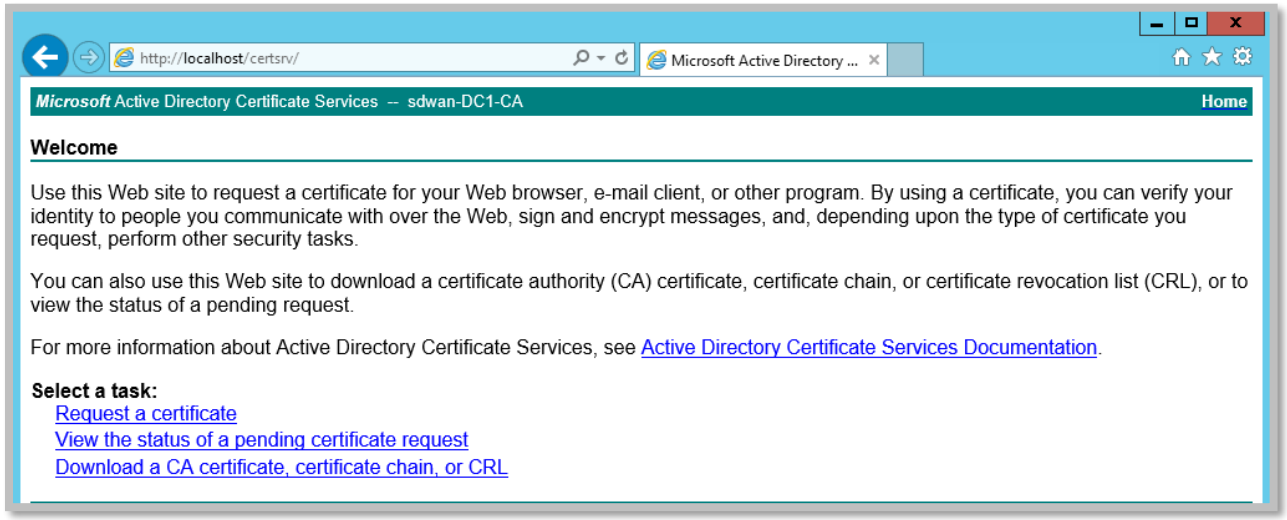
19. Before Get Certificate go to **`Active Directory user and Services`**



20. In `Built-in` select `IIS_IUSRS,` then add `administrator User`



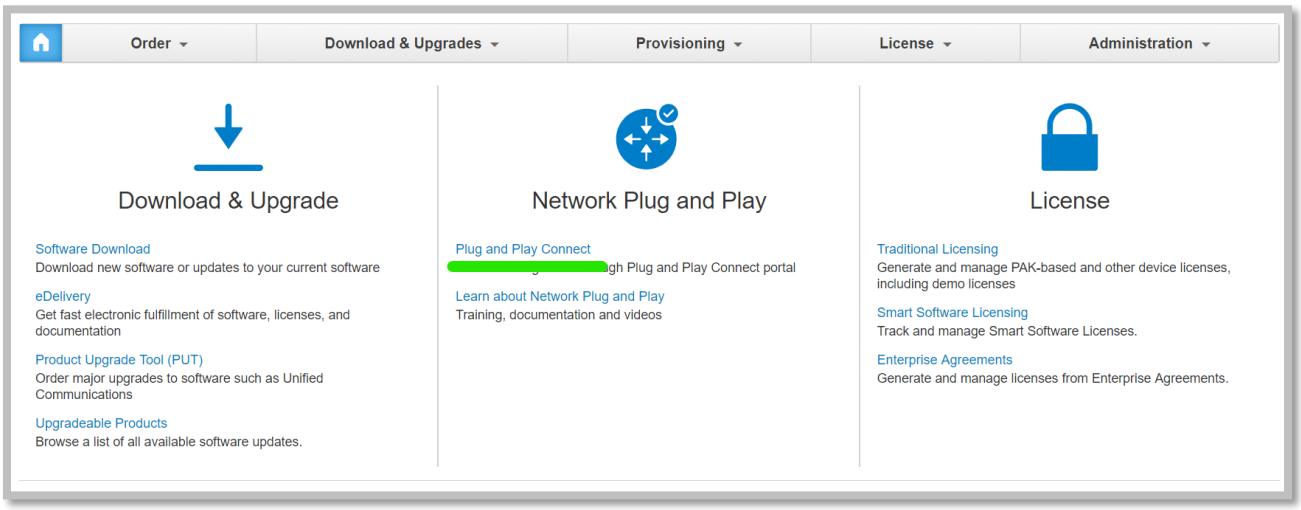
21. Browse URL http://localhost/certsrv to check page loaded correctly



Cisco Smart Account

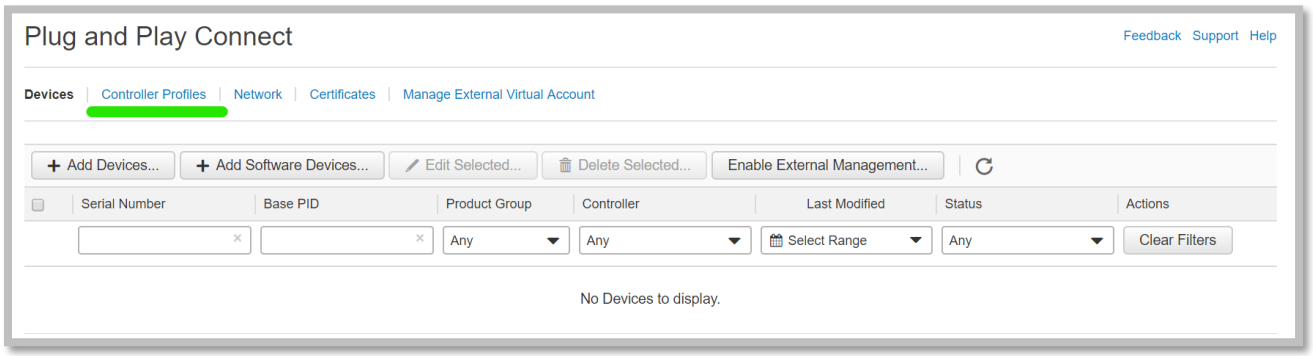
Login Smart Account

1- Navigate to https://software.cisco.com
2- Select **`Plug and Play Connect`**
3- Select **`Default Virtual Accounts`**.

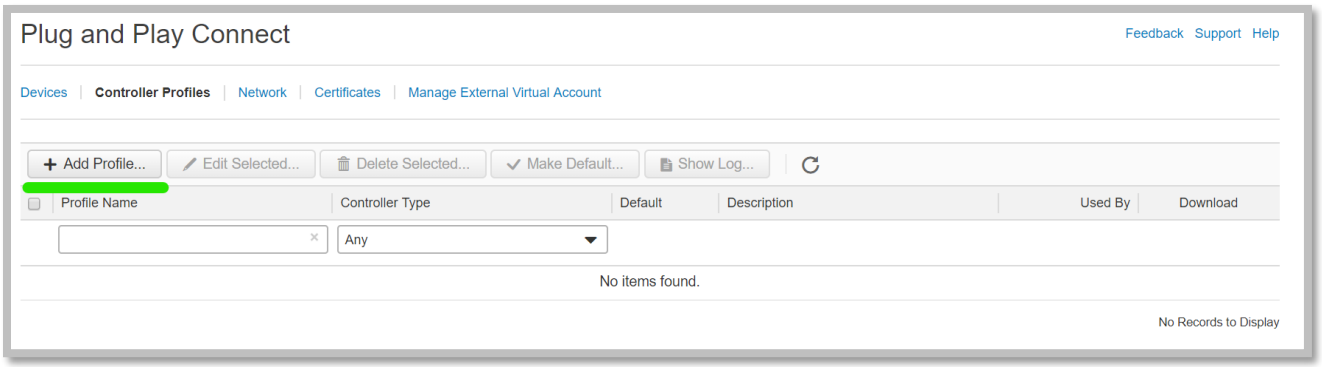


Add Controller Profile

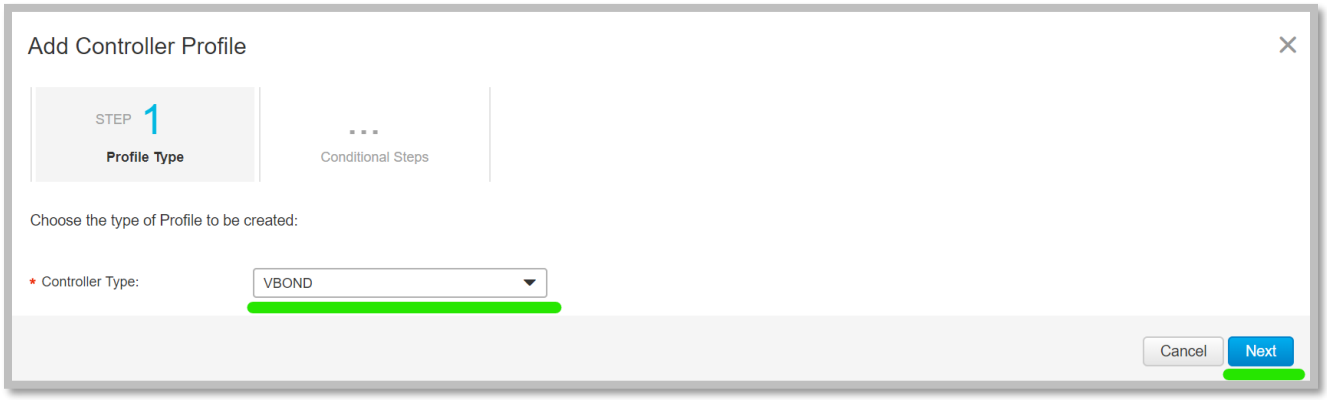
4- Select **`Controller Profiles`**.



5- Select **`Add Profile`**.

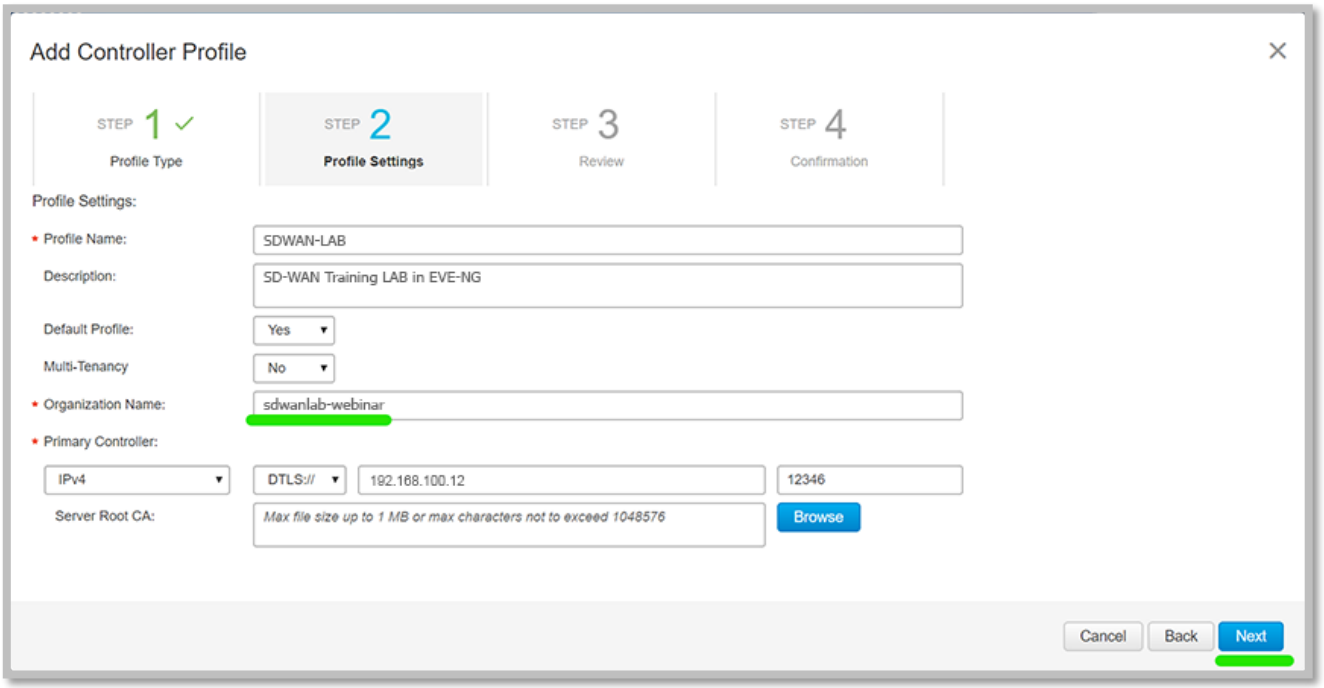


1- Change the controller type to **`VBOND`** then select **`Next`**.

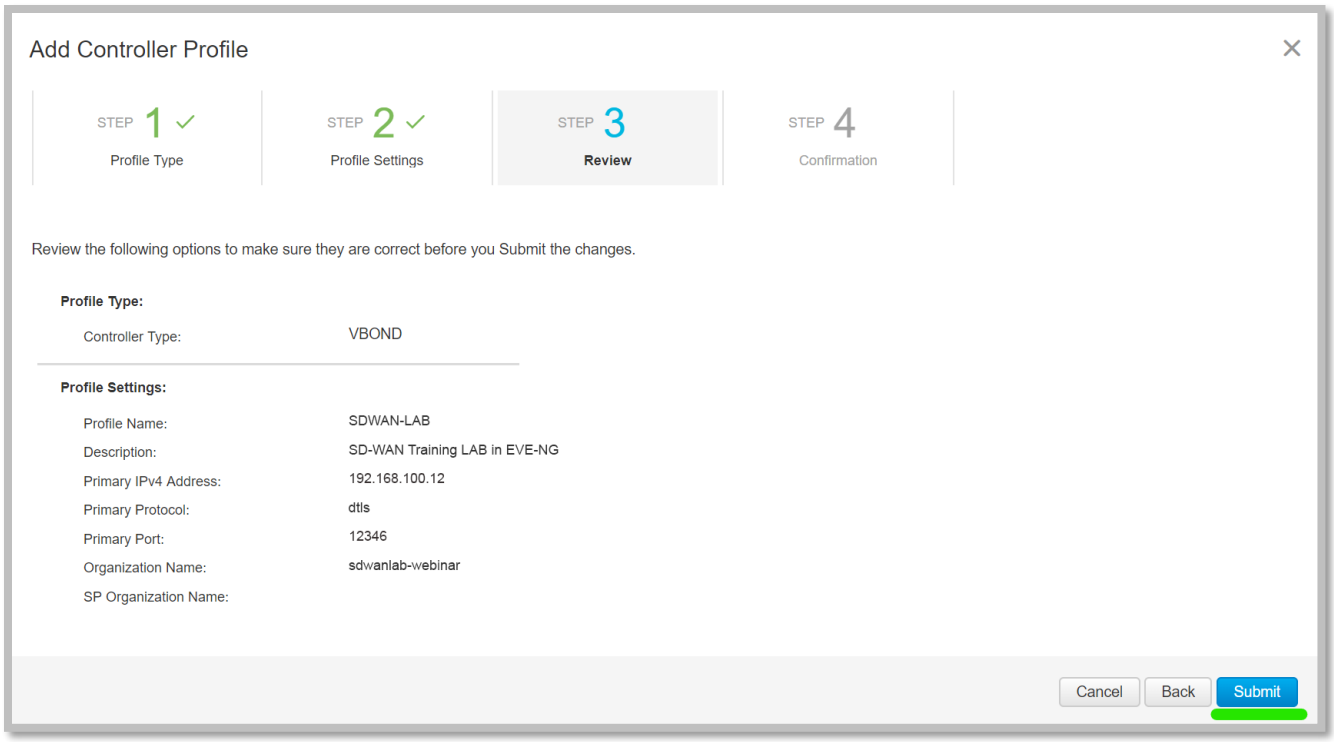


2- Enter the vBond details and select **`Next`**.

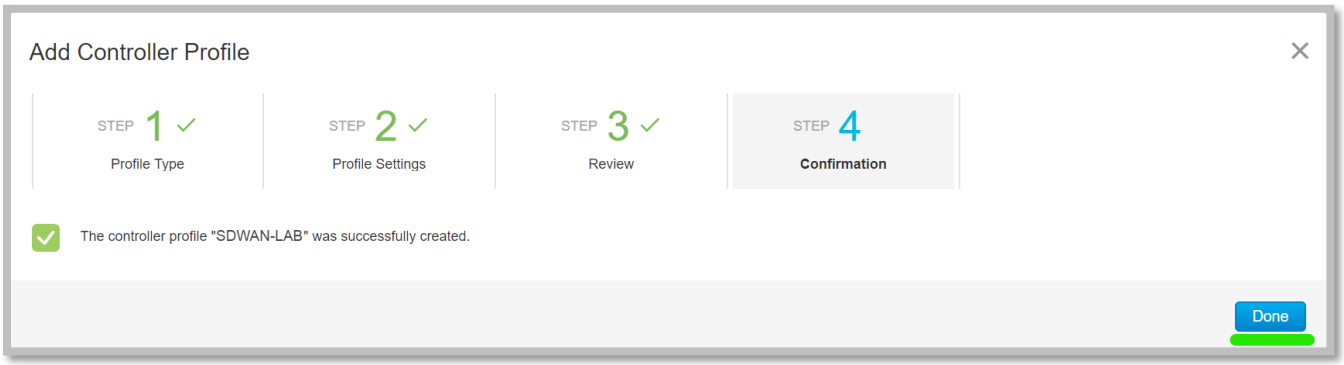
Note: The **`Organization Name`** will need to be unique, the IP address can be anything.



3- Select **Submit**.



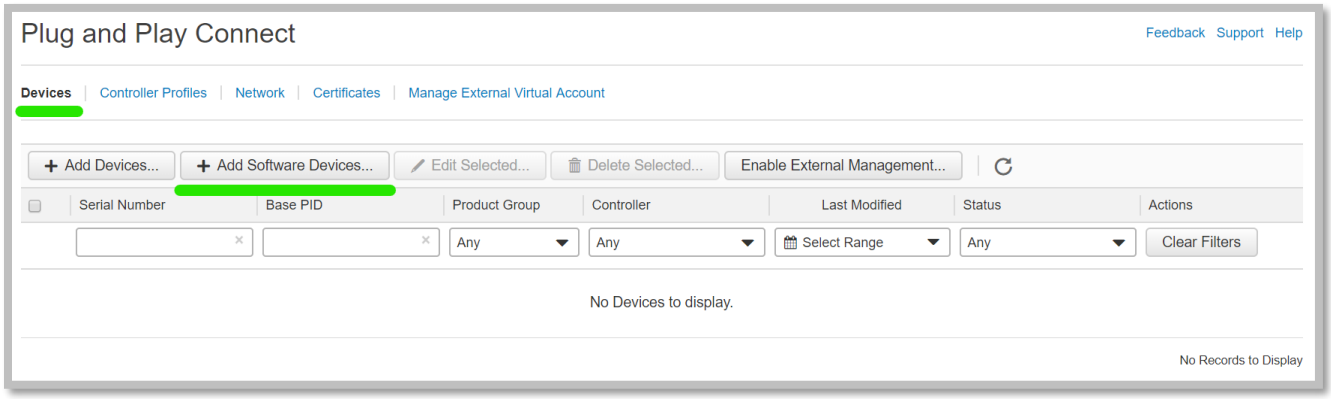
4- Select **Done**.



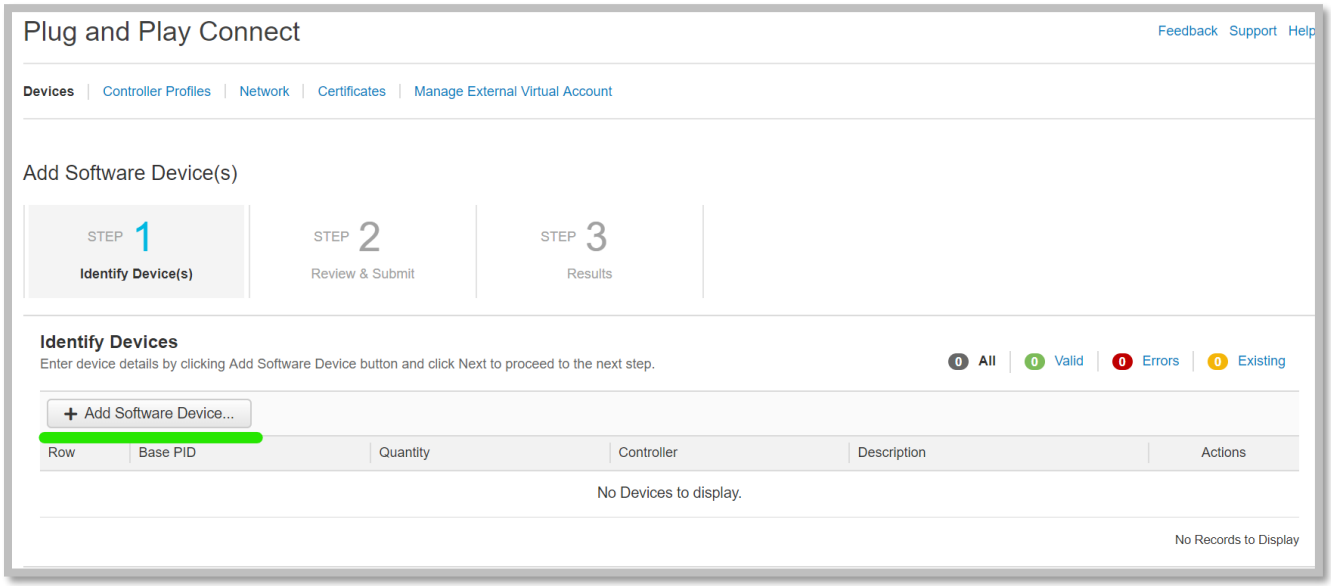
5- You should see your newly created controller profile in the list.

Add Virtual Edges cloud & CSR1000v

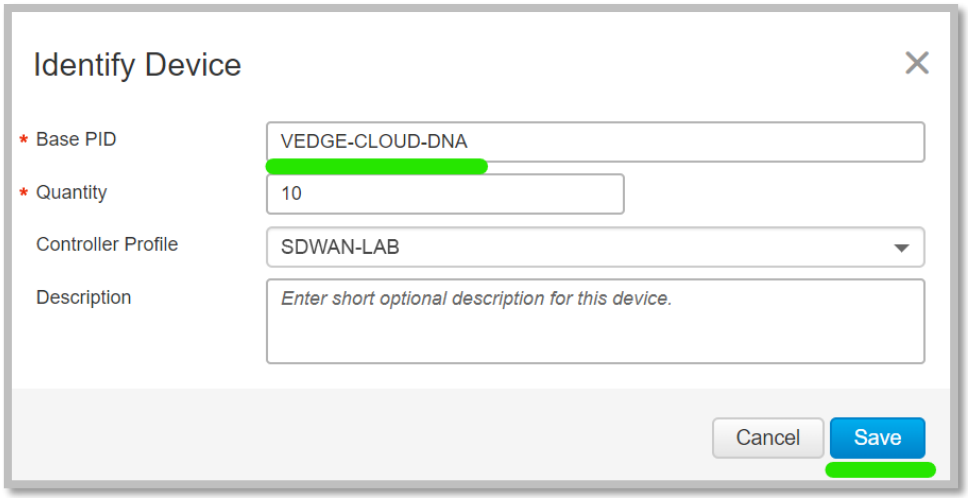
1- Navigate to **`Devices`** and select **`+ Add Software Devices`**.



2- Select **`+ Add Software Device`**.

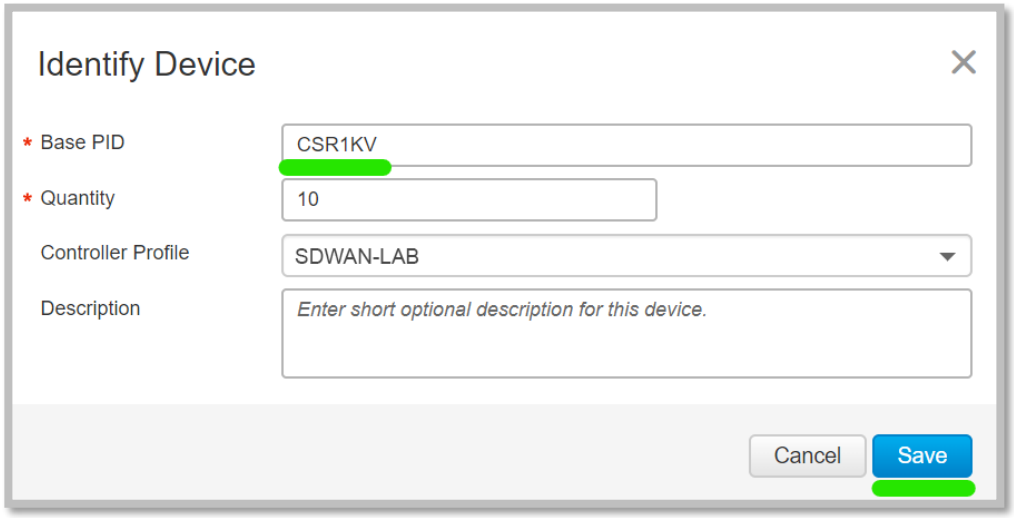


3- Enter the PID **`VEDGE-CLOUD-DNA`** for vEdges, specify the desired quantity and select **`Save`**.

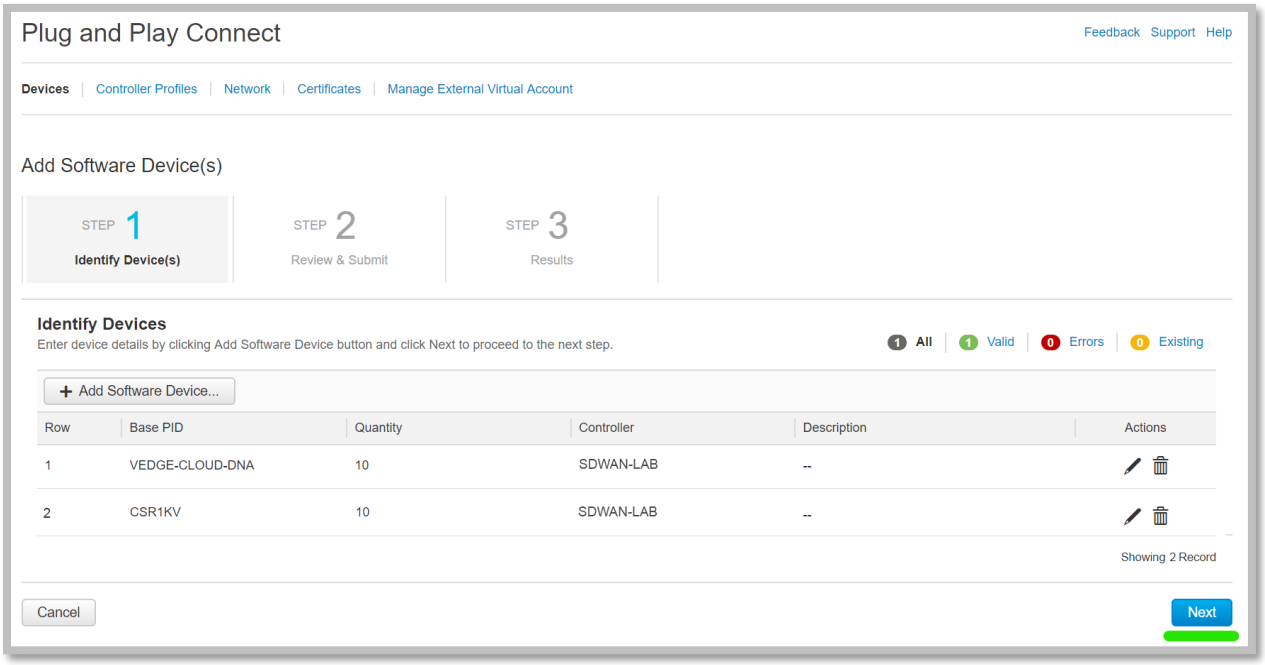


4- Select again **`+ Add Software Device`**.

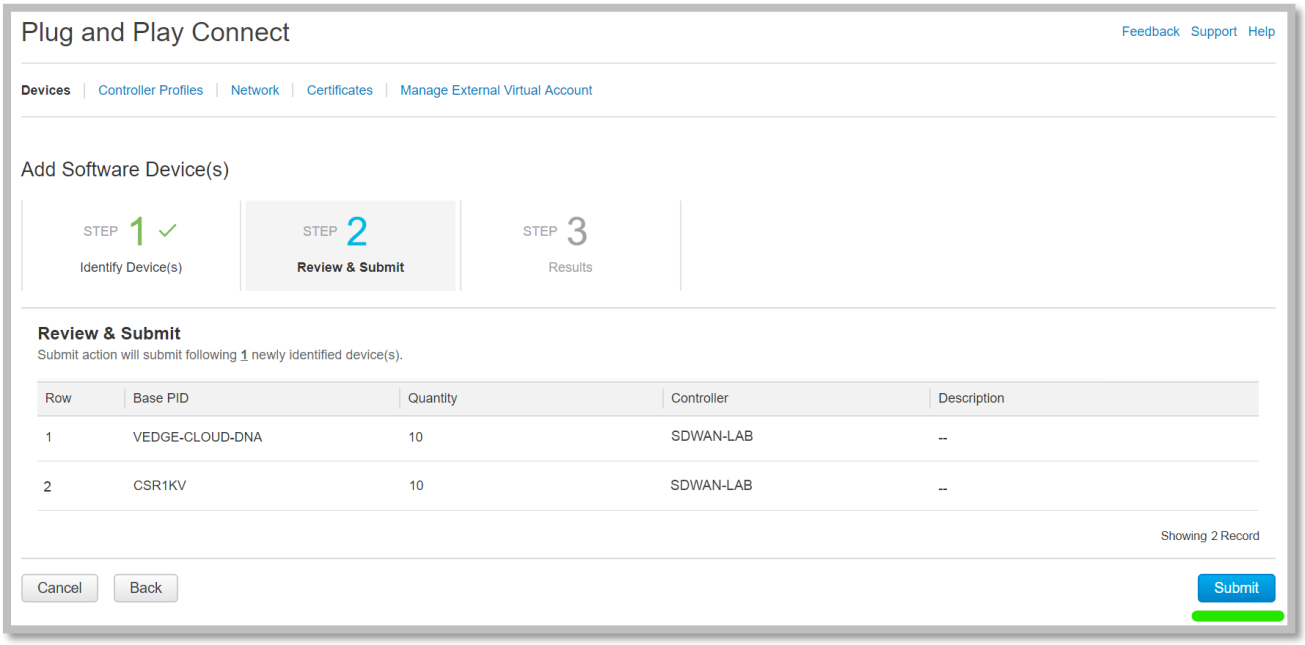
5- Enter the PID **`CSR1KV`** for vEdges, specify the desired quantity and select **`Save`**.



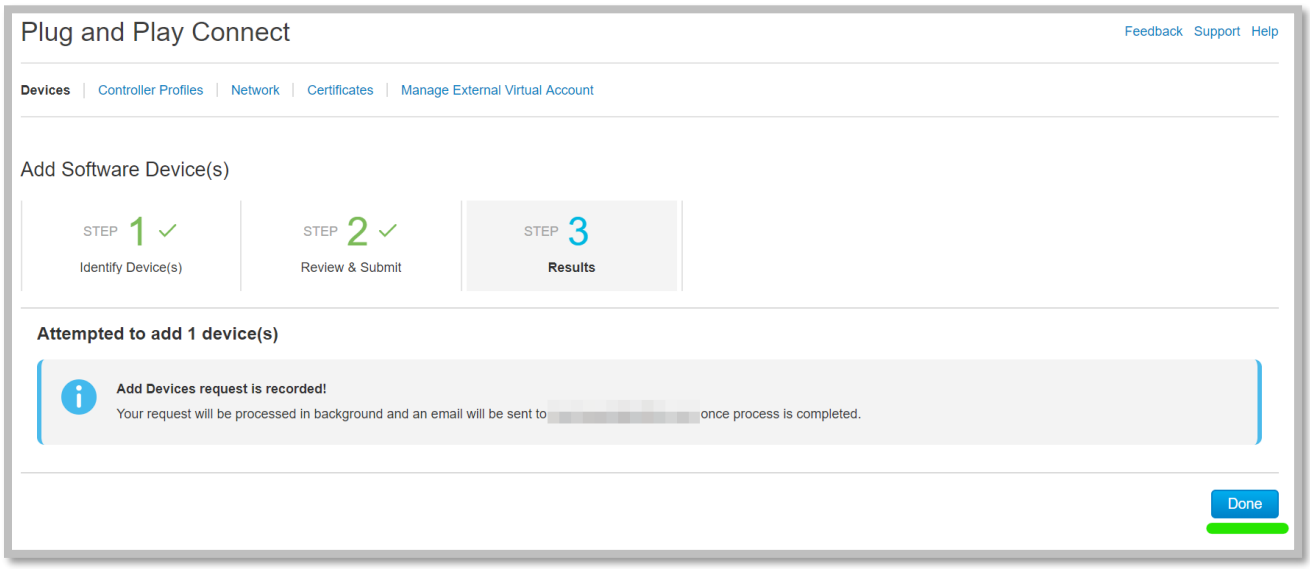
6- Select **`Next`**.



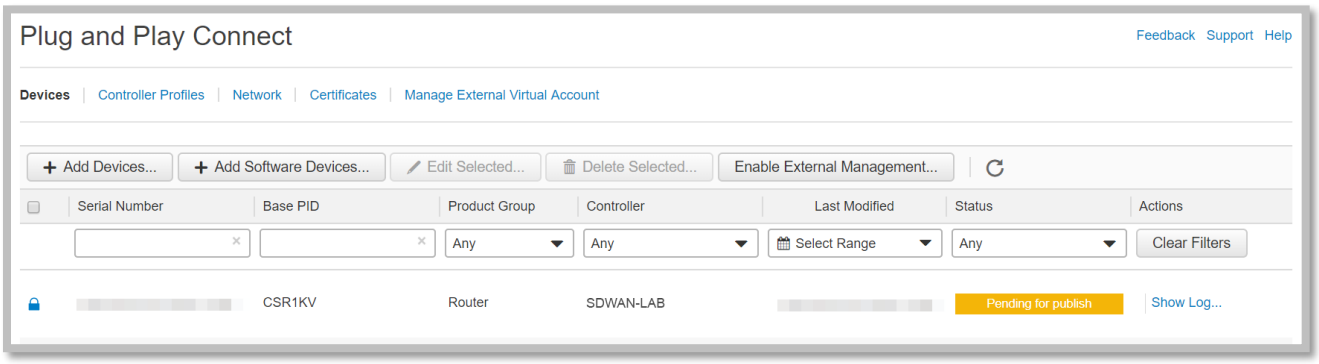
7- Select **`Submit`**.



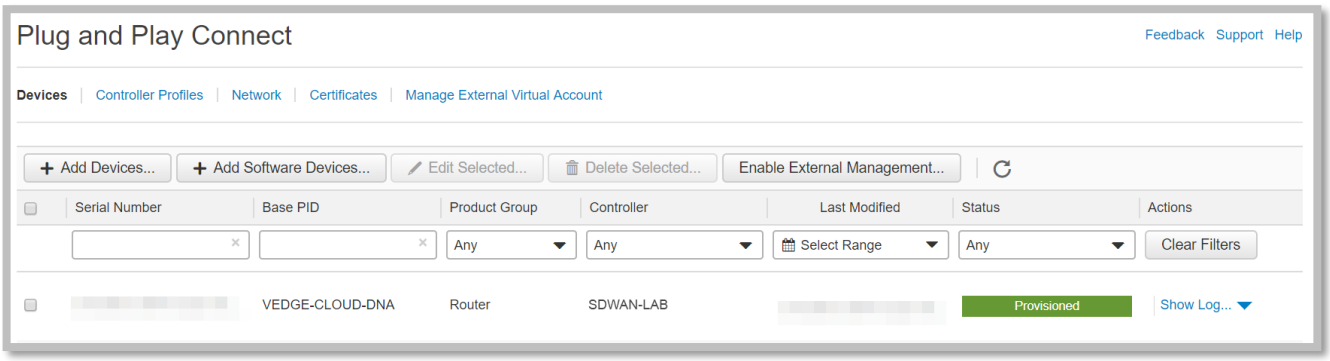
8- Select **`Done`**.



9- Once added devices will be in a **`Pending for publish`** state.

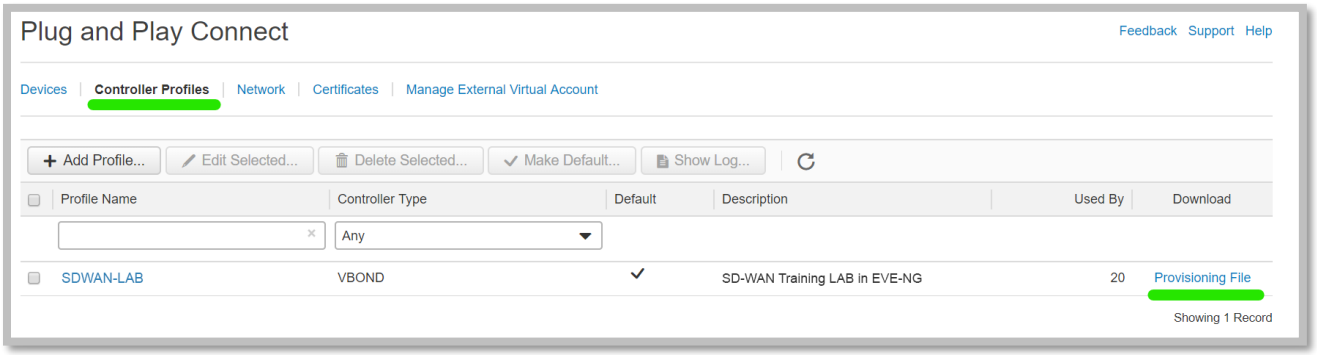


10- After a few minutes they will transition to the **`Provisioned`** state.

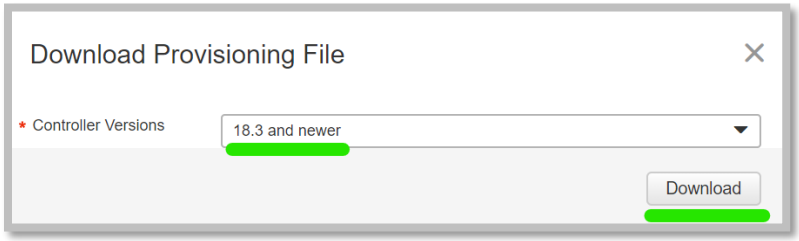


Serial File

1- Navigate to **`Controller Profiles`** and select **`Provisioning File`**.



2- Select **`18.3 and Newer`** from the dropdown and then select **`Download`**. Save the file to a safe location to import into the vManage at a future time.



SD-WAN Controller Configuration on EVE-NG

vManage

1- start **VManage** and attach to a virtual console.

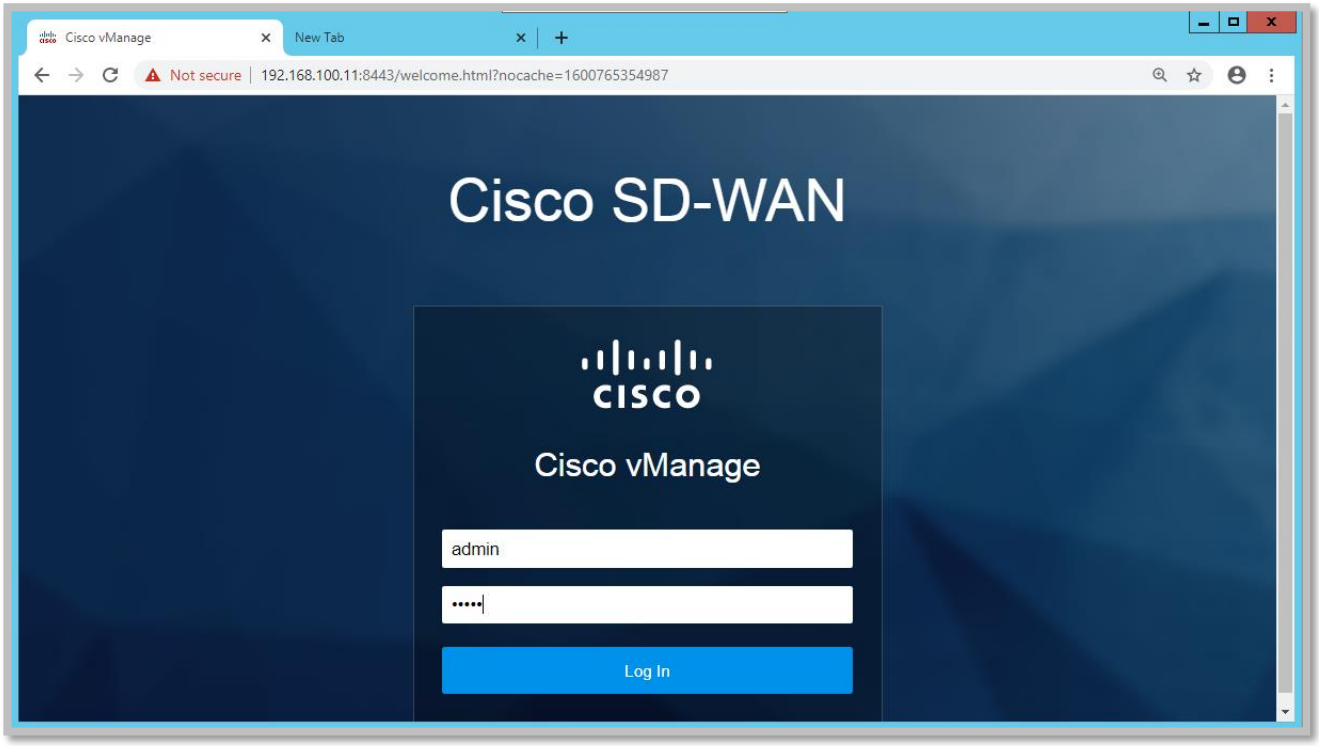
2- When see **System Ready,** login with the username/password **admin**

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

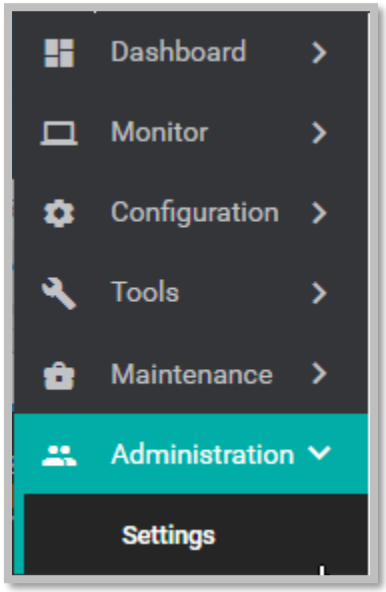
3- Once this is done the VM will reboot. Login again and apply the **bootstrap configuration.**

```
config
system
 system-ip 100.1.1.11
 site-id 100
 organization-name "sdwanlab-webinar"
 clock timezone Asia/Tehran
 vbond 192.168.100.12
!
ntp
  server 172.16.32.10
   version 4
   prefer
  exit

vpn 0
 ip route 0.0.0.0/0 192.168.100.1
 interface eth0
  ip address 192.168.100.11/24
  ipv6 dhcp-client
  no shutdown
 !
!
commit and-quit
```

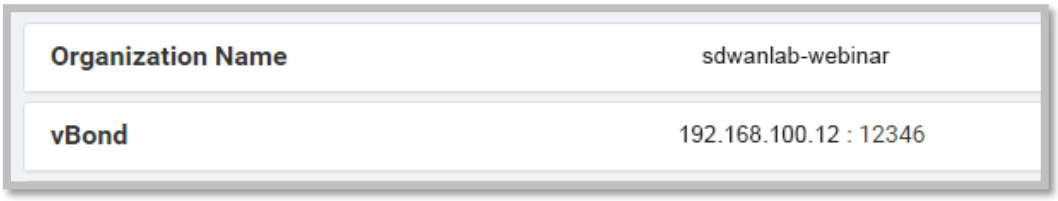
4- Login `http://192.168.100.11:8443 (Chrome browser)`
5- *Windows Server IP Address =192.168.100.10



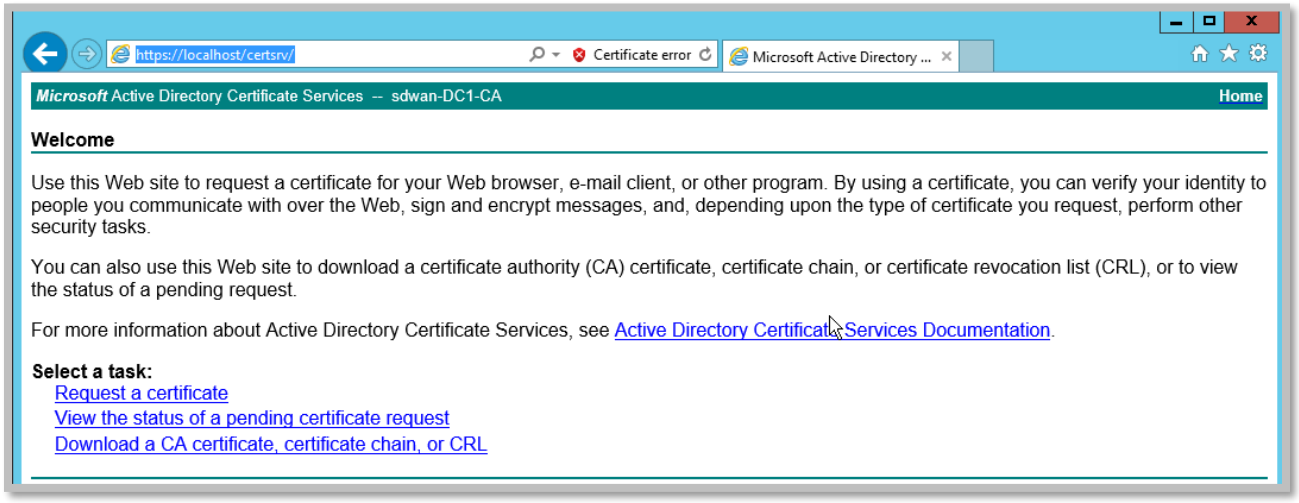
6- Go to `Administration/Setting` in vManage menu



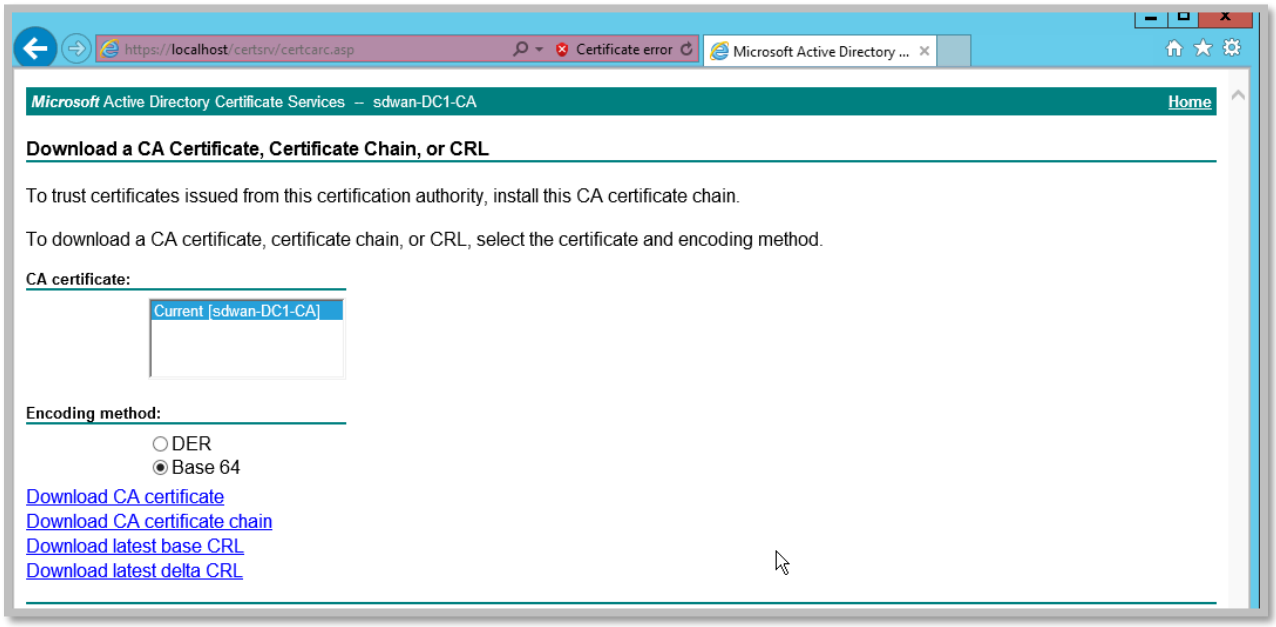
7- Change `Organization name and vBond IP address`



8- Open URL `http://localhost/certsrv (IE Browser)`
9- Select `Download a CA certificate, certificate chain, or CRL`

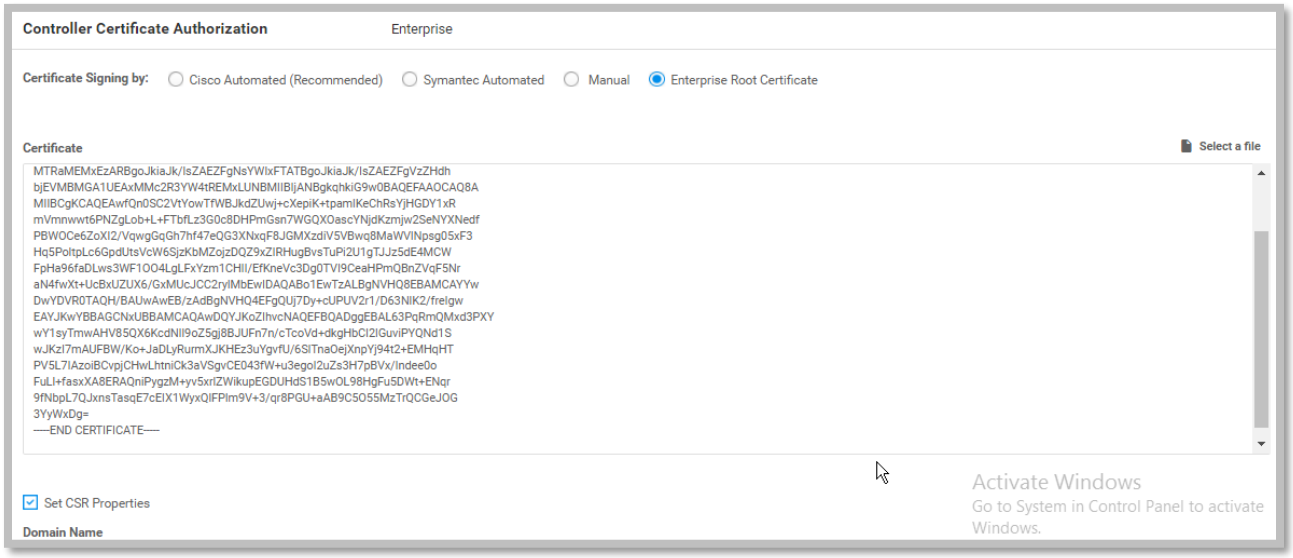


10- Select `Base 64 Then Download CA Certificate`
11- Change name `root.cer`



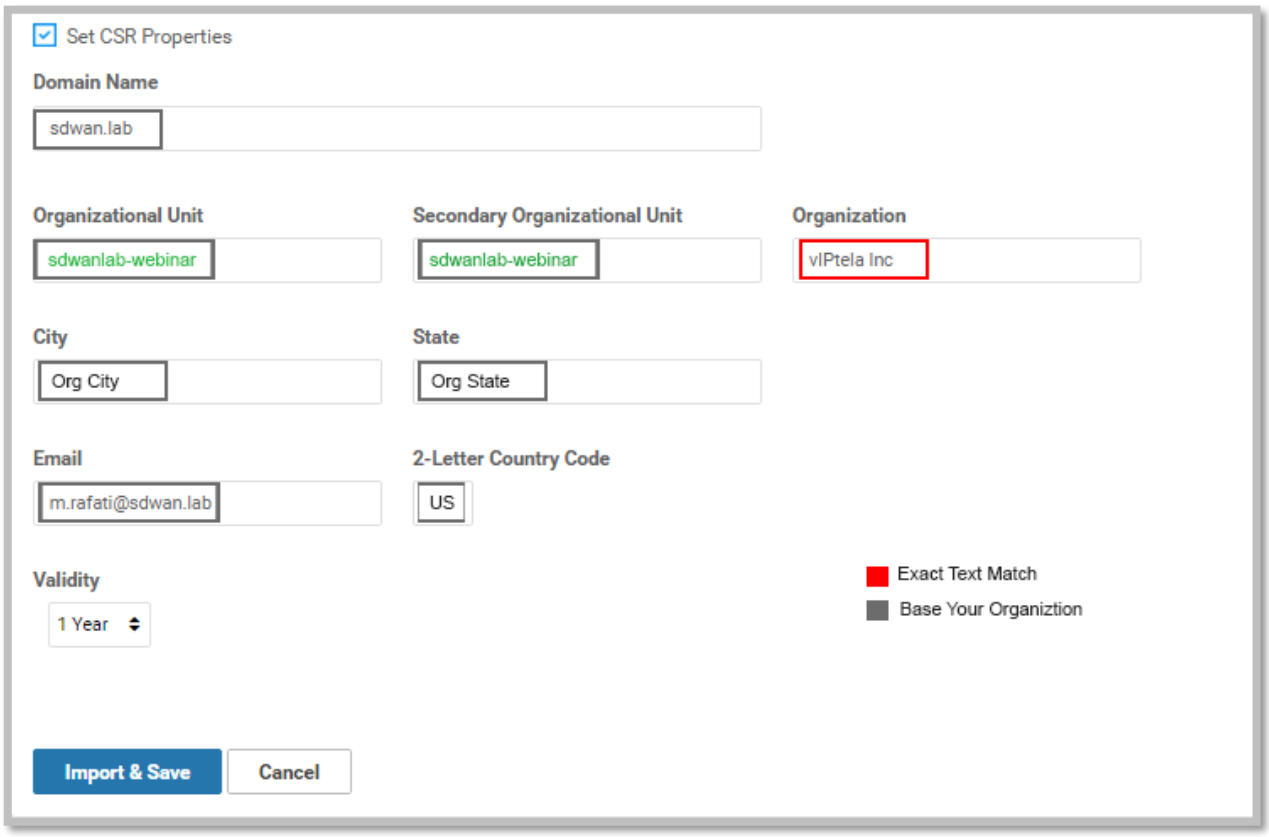
12- In vMange menu select `Administration/Setting`
13- Select `Controller Certificate Authorization`
14- Select `Enterprise Root Certificate`

15- Upload **`Root.cer`** file



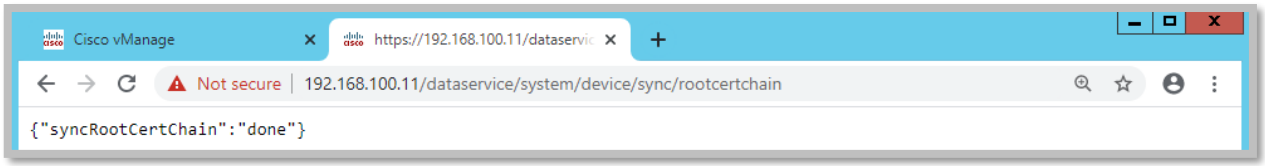
16- Mark **`Set CSR properties`**

17- Fill **`Text boxes`** base of Picture



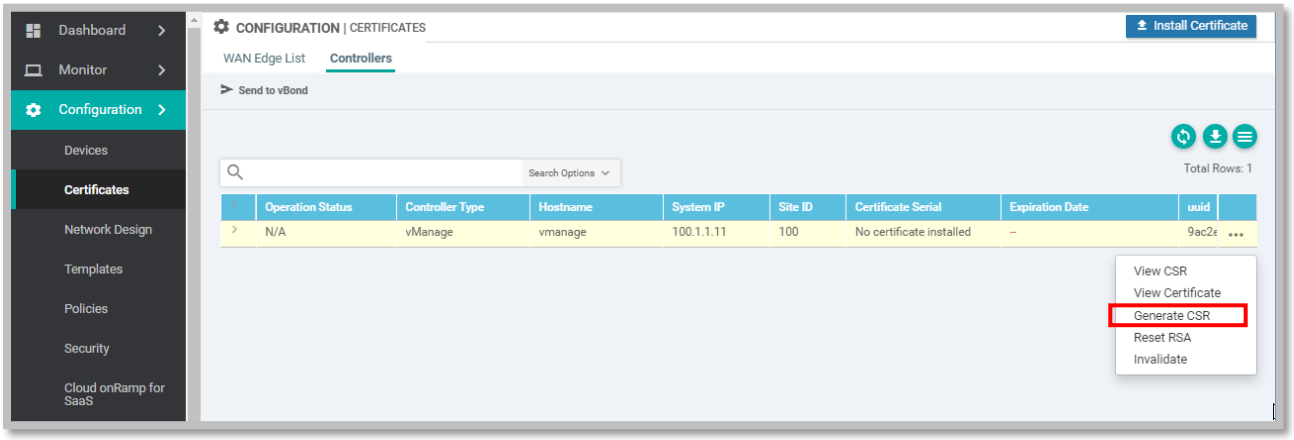
18- Click **`import and Save`**

19- Open new browser tab, then enter
https://192.168.100.11/dataservice/system/device/sync/rootcertchain

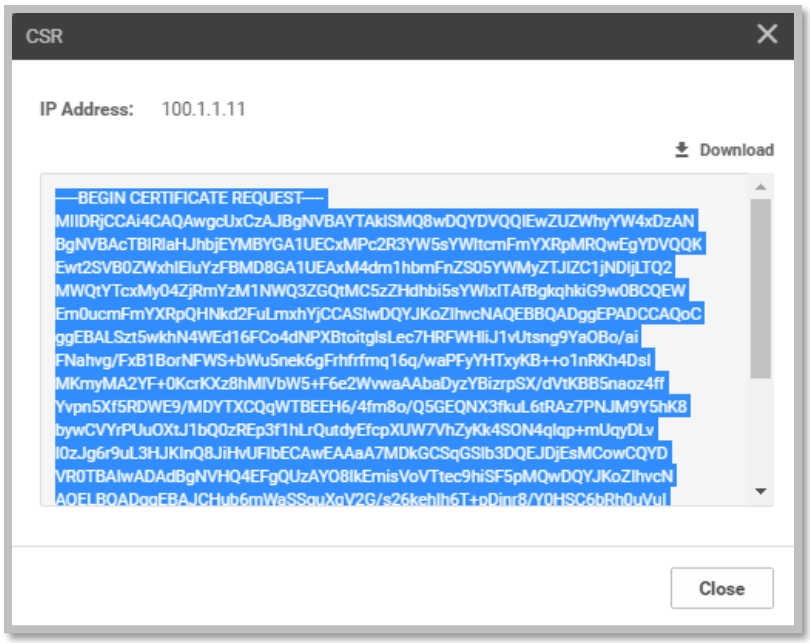


20- on **vManage**, select menu **Configuration->Certificate->Controllers**

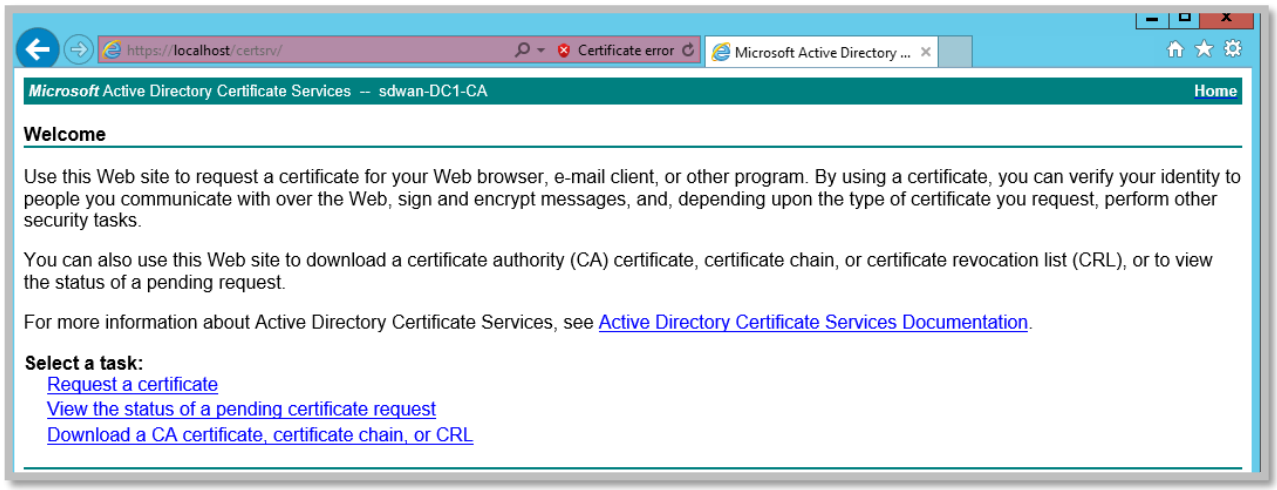
21- Click **...** then select **generate CSR**



22- Copy **PEM** format of Certificate

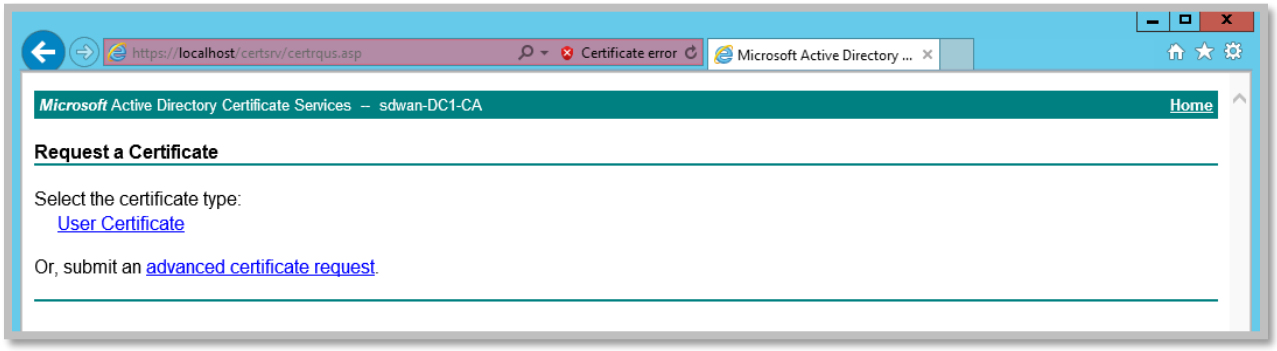


23- Open **Certificate Authority web enrollment URL** http://localhost/certsrv

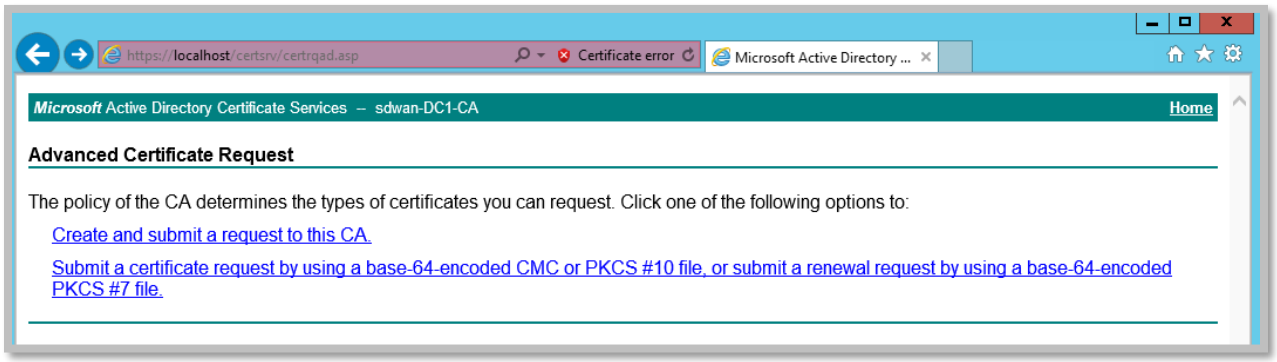


24- Click on **request a certificate**

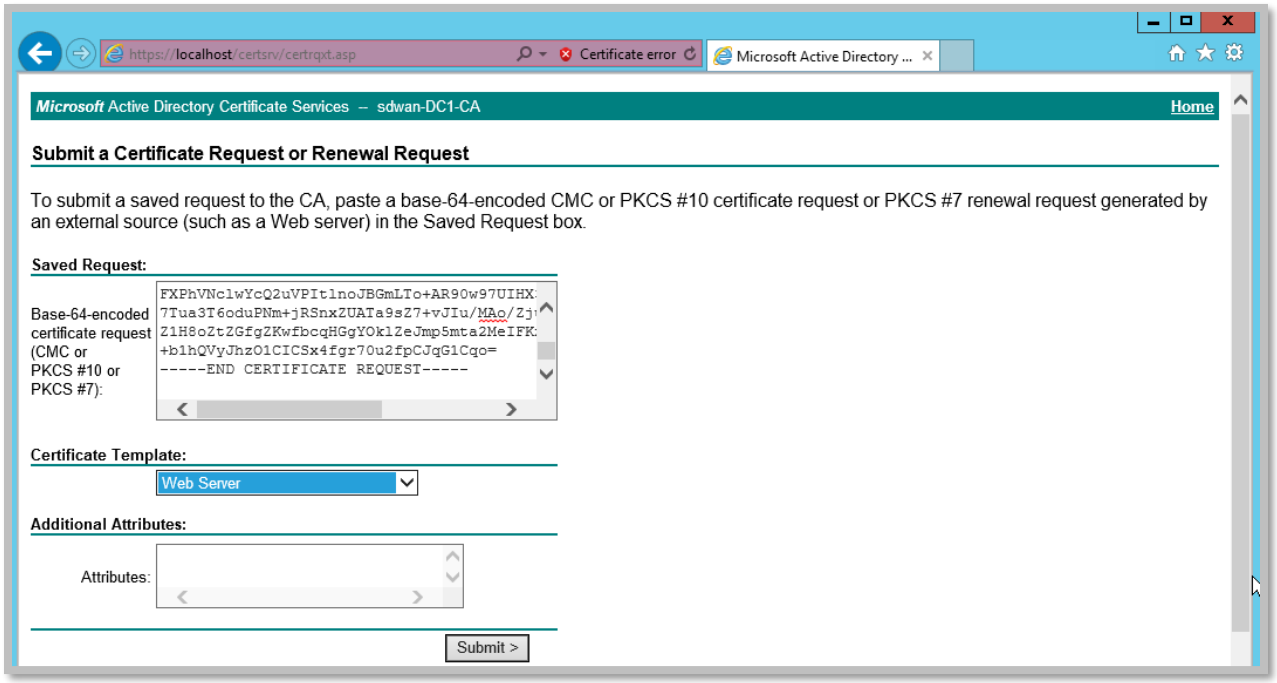
25- Click **advance certificate request**



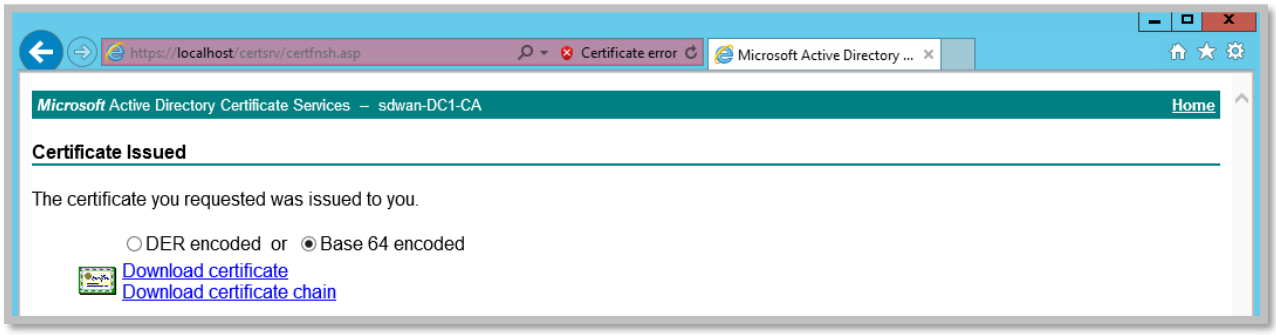
26- Select **submit a certificate request by** ....



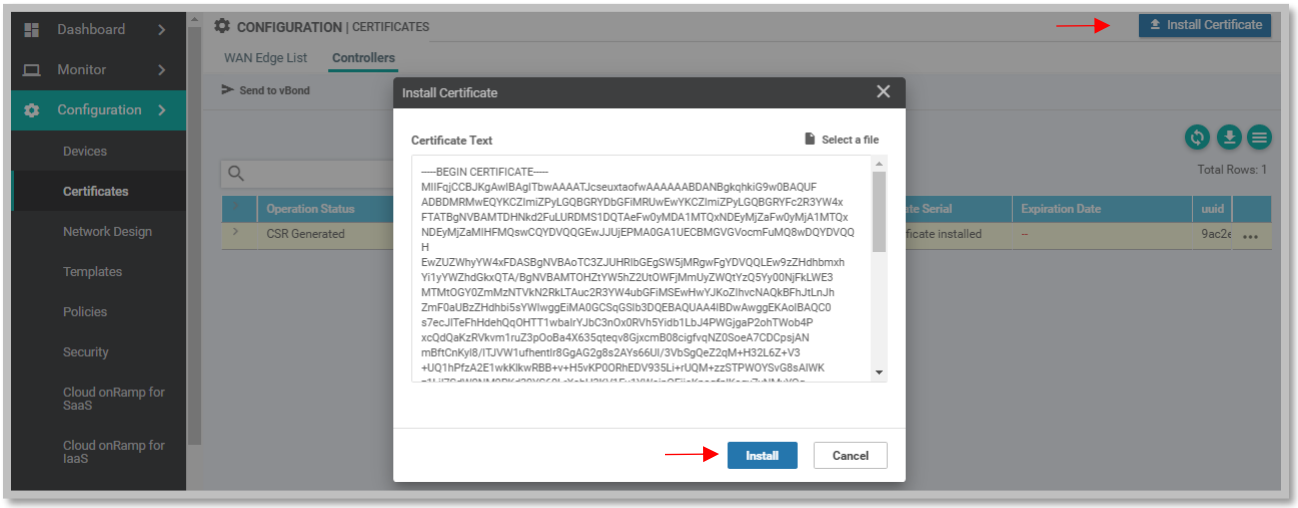
27- Paste CSR and select **certificate Template** Web Server the click **Submit**



28- Download **base 64 encoded Corticate** and change name **vmange.cer**



29- Navigate **vManage GUI** then **Configuration/certificates/Controllers** click **install Certificate** import **vmange.cer** then click **install**



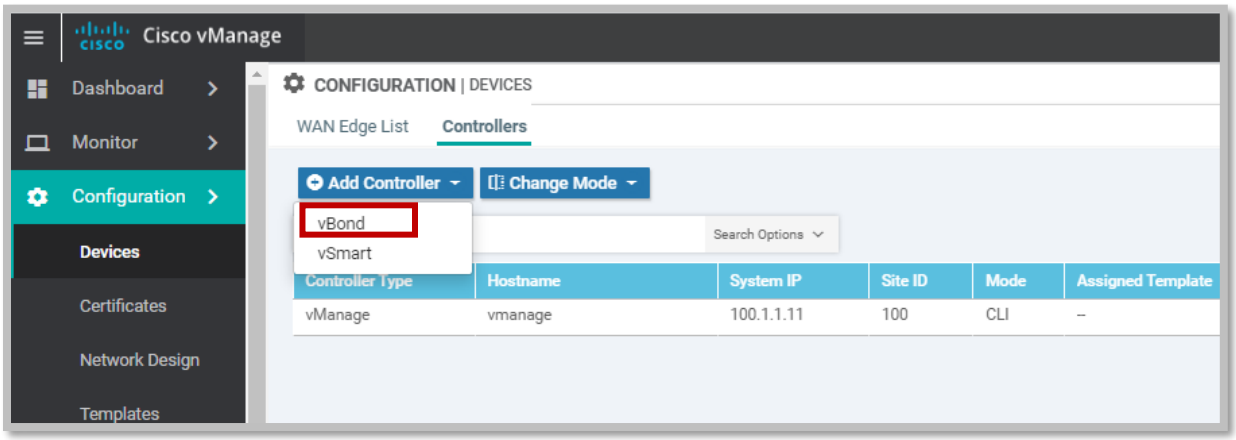
30- successfully **install certificate**

vBond

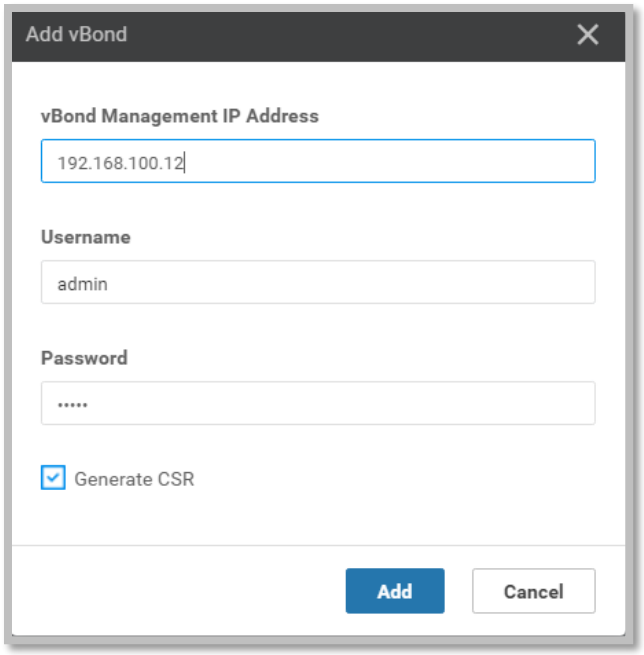
1- Start **`vBond node on EVE-NG`**
2- Once you see the message **`System Ready`** login with the **`username/password admin`** and apply the following **`bootstrap config`**.

```
config
system
 system-ip 100.1.1.12
 site-id 100
 organization-name "sdwanlab-webinar"
 clock timezone Asia/Tehran
 vbond 192.168.100.12 local
!
ntp
  server 172.16.32.10
   version 4
   prefer
  exit

vpn 0
ip route 0.0.0.0/0 192.168.100.1
 interface ge0/0
  ip address 192.168.100.12/24
  no tunnel-interface

!
```

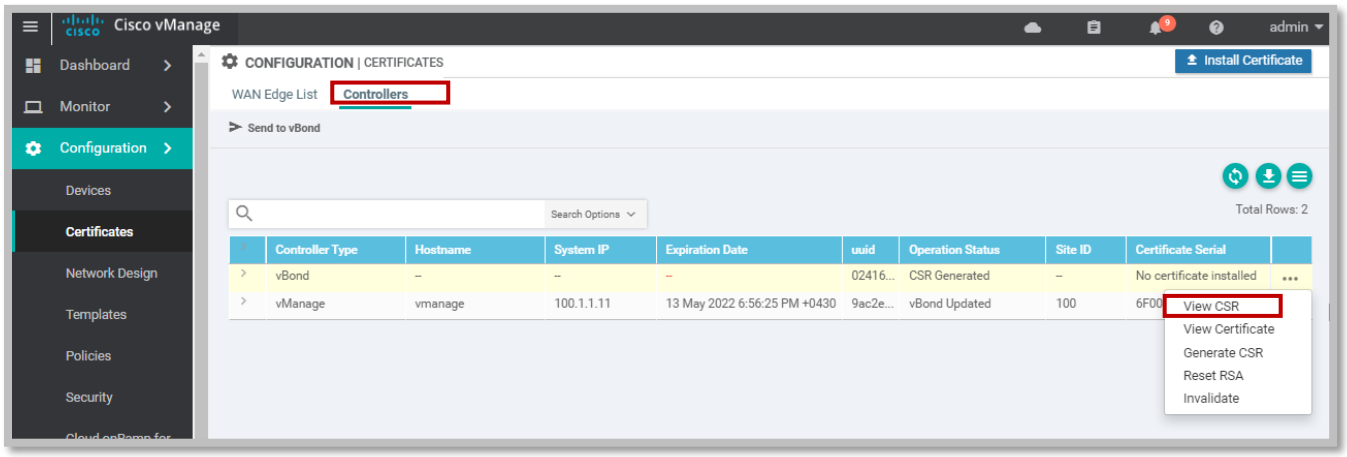
3- Navigate to the **`devices page`** to add the vBond to the vManage.
`Configuration --> Devices --> Controllers --> Add Controller --> vBond`



4- Enter the **vBond details** add click **Add.**



5- Navigate to the **certificates page** to get the **vBond CSR text.**
Configuration --> Certificates --> Controllers --> vBond --> ...
6- select **View CSR**



7- Continue as **vManage section 21-25**
8- Download **base 64 encoded Corticate** and change name **vbond.cer**
9- Navigate **vManage GUI** then **Configuration/certificates/Controllers** click install Certificate **import vbond.cer** then click **install**
10- vBond Should Successfully install

11- Now go to **vManage CLI** and

```
vmanage# show control local-properties
personality                         vmanage
sp-organization-name                sdwanlab-webinar
organization-name                   sdwanlab-webinar
root-ca-chain-status                Installed

certificate-status                  Installed
certificate-validity                Valid
certificate-not-valid-before        May 13 14:26:25 2020 GMT
certificate-not-valid-after         May 13 14:26:25 2022 GMT

dns-name                            192.168.100.12
site-id                             100
domain-id                           0
protocol                            dtls
tls-port                            23456
system-ip                           100.1.1.12
……
```

12- Configure **VPN 0 tunnel interface**

```
vpn 0
 interface eth0
  tunnel-interface
   allow-service all
commit
```

13- Now go to **vBond CLI**

14- Check certificate on vBond command: **show orchestrator local-properties**

```
vBond# show orchestrator local-properties
personality                   vbond
sp-organization-name          sdwanlab-webinar
organization-name             sdwanlab-webinar
system-ip                     100.1.1.12
certificate-status            Installed
root-ca-chain-status          Installed

certificate-validity          Valid
certificate-not-valid-before  May 14 02:18:48 2020 GMT
certificate-not-valid-after   May 14 02:18:48 2022 GMT
chassis-num/unique-id         02416bb3-45a2-4d5b-88a5-c54dad99b652
serial-num                    6F0000000621358062D89ED028000000000006
number-active-wan-interfaces  1
protocol                      dtls

INSTANCE INDEX  PORT  VSMARTS  VMANAGES  STATE
-----------------------------------------------
0        0      12346 0        0         up
```

15- Configure `VPN 0` Tunnel interface

```
vpn 0
 interface ge0/0
  tunnel-interface
   encapsulation ipsec
   allow-service all
commit
```

16- Now the connection between vManage and vBond should UP

`vBond: show orchestrator connections`

`vManage: show control connections`

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	STATE	ORGANIZATION NAME	UPTIME
vmanage	dtls	100.1.1.11	100	0	192.168.100.11	12346	192.168.100.11	12346	default	up	sdwanlab-webinar	0:00:00:05
vmanage	dtls	100.1.1.11	100	0	192.168.100.11	12446	192.168.100.11	12446	default	up	sdwanlab-webinar	0:00:00:03
vmanage	dtls	100.1.1.11	100	0	192.168.100.11	12546	192.168.100.11	12546	default	up	sdwanlab-webinar	0:00:00:03
vmanage	dtls	100.1.1.11	100	0	192.168.100.11	12646	192.168.100.11	12646	default	up	sdwanlab-webinar	0:00:00:03

vSmart

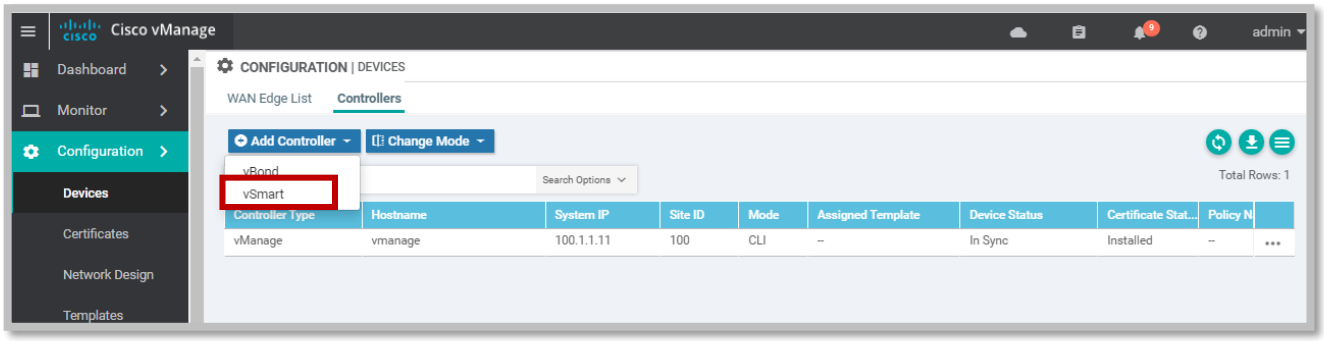
17- Start `vSmart` `node on EVE-NG`

1- Once you see the message `System Ready` login with the `username/password admin` and apply the following `bootstrap config`.

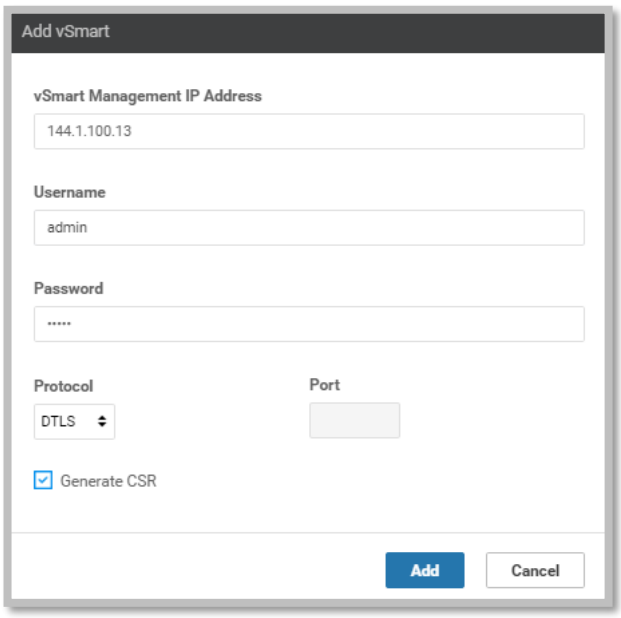
```
config
system
 system-ip 100.1.1.13
 site-id 100
 organization-name "sdwanlab-webinar"
 clock timezone Asia/Tehran
 vbond 192.168.100.12
!
ntp
  server 172.16.32.10
   version 4
   prefer
  exit

vpn 0
ip route 0.0.0.0/0 192.168.100.1
 interface eth0
  no shut
  ip address 192.168.100.13/24

!
```

1- Navigate to the devices page to add the `vSmart` to the vManage.

2- `Configuration--> Devices--> Controllers--> Add Controller--> vSmart`

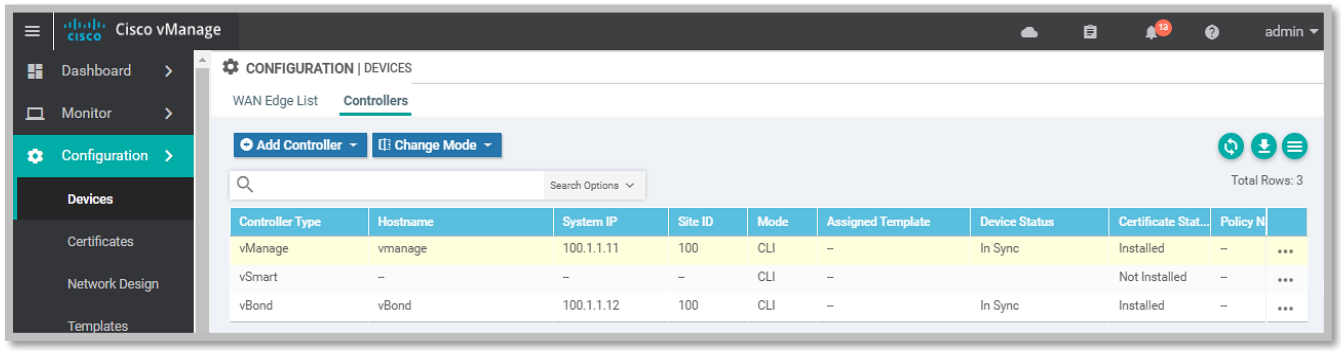


3- Enter the **`vSmart details`** add click Add.



4- Navigate to the certificates page to get the **`vSmart CSR text`**.

`Configuration--> Certificates--> Controllers--> vSmart --> ...--> View CSR`



5- Continue as **`vManage section 21-25`**
6- Download **`base 64 encoded Certificate`** and change name **`vsmart.cer`**
7- Navigate **`vManage GUI`** then **`Configuration/Certificates/Controllers`** click install Certificate **`import vsmart.cer`** then click install
8- vSmart Should Successfully install

9- Navigate **vSmart CLI**

```
vsmart# show control local-properties
personality                         vsmart
sp-organization-name                sdwanlab-webinar
organization-name                   sdwanlab-webinar
root-ca-chain-status                Installed

certificate-status                  Installed
certificate-validity                Valid
certificate-not-valid-before        May 14 03:56:31 2020 GMT
certificate-not-valid-after         May 14 03:56:31 2022 GMT

dns-name                            192.168.100.12
site-id                             100
domain-id                           1
protocol                            dtls
tls-port                            23456
system-ip                           100.1.1.13
……
```

10- Configure **VPN 0 tunnel interface**

```
vpn 0
 interface eth0
  tunnel-interface
commit
```

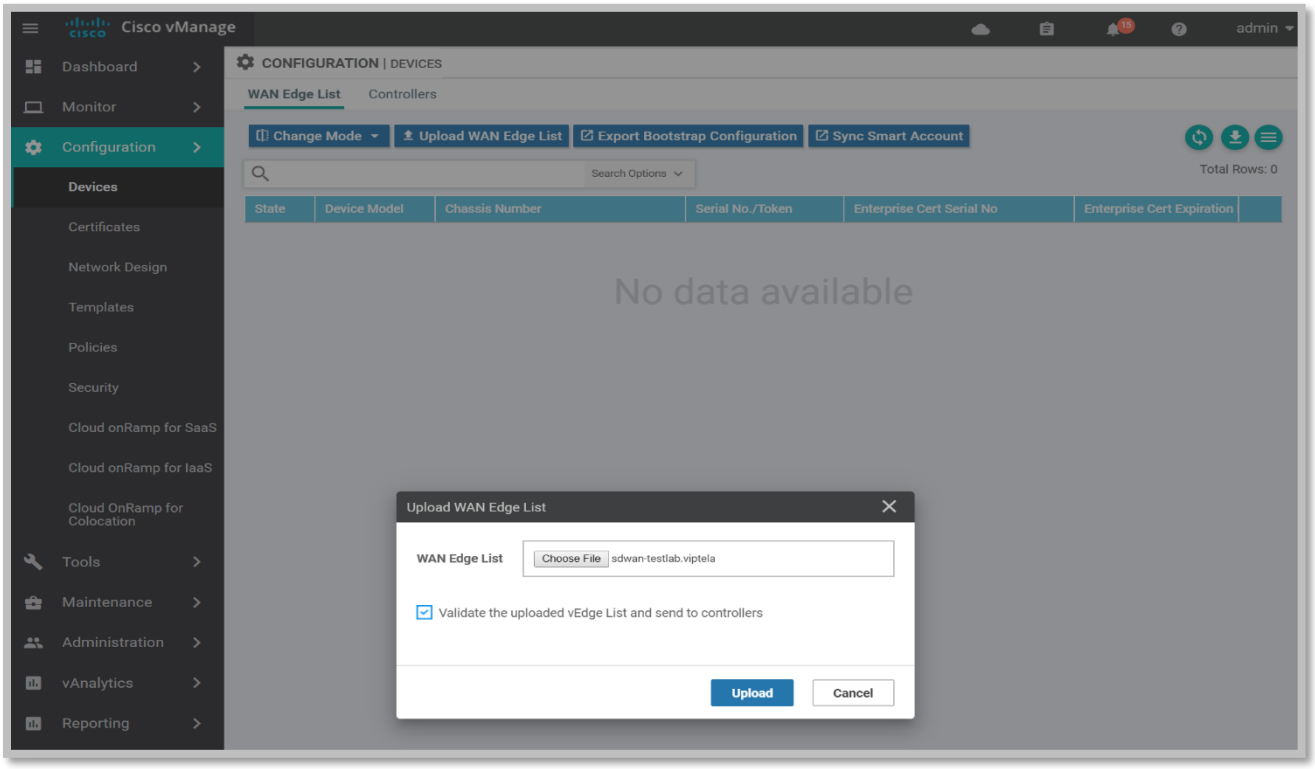
11- show connection in **vSmart show control connections**

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	REMOTE COLOR	STATE	UPTIME
vbond	dtls	0.0.0.0	0	0	192.168.100.12	12346	192.168.100.12	12346	default	up	0:00:00:21
vmanage	dtls	100.1.1.11	100	0	192.168.100.11	12346	192.168.100.11	12346	default	up	0:00:00:03
vbond	dtls	0.0.0.0	0	0	192.168.100.12	12346	192.168.100.12	12346	default	up	0:00:00:20

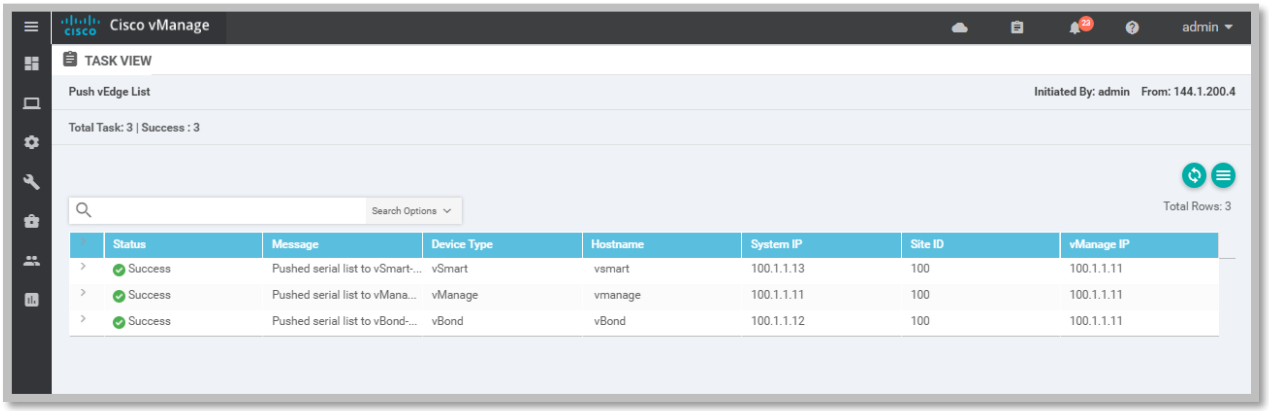
SD-WAN WAN Edges Configuration on EVE-NG

Navigate to the devices page and upload the serial file from the location you save it to previously. Keep the box ticked to validate the list and send to controllers.

1- Configuration > Devices > Upload WAN Edge List



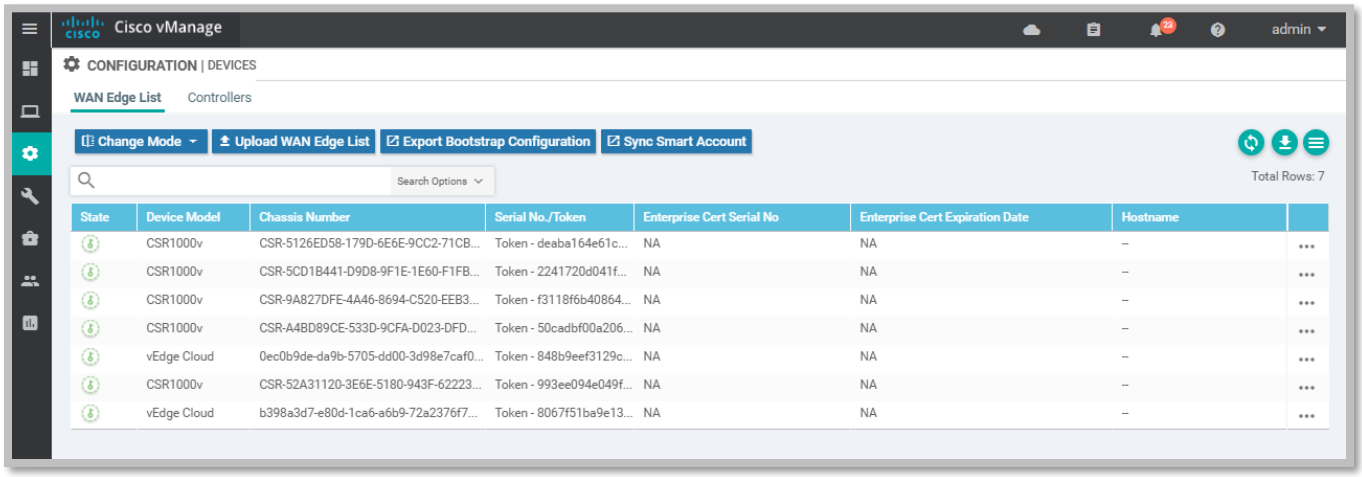
2- A success message looks similar to the below



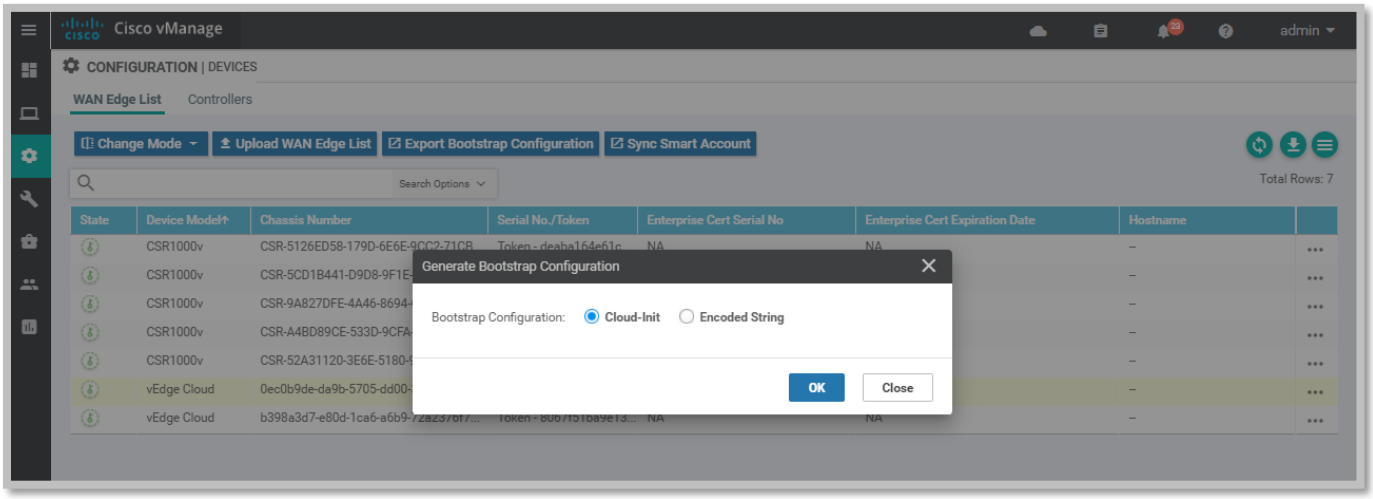
vEdge Cloud

To add a virtual edge you need to generate a bootstrap file. Navigate to the devices page.

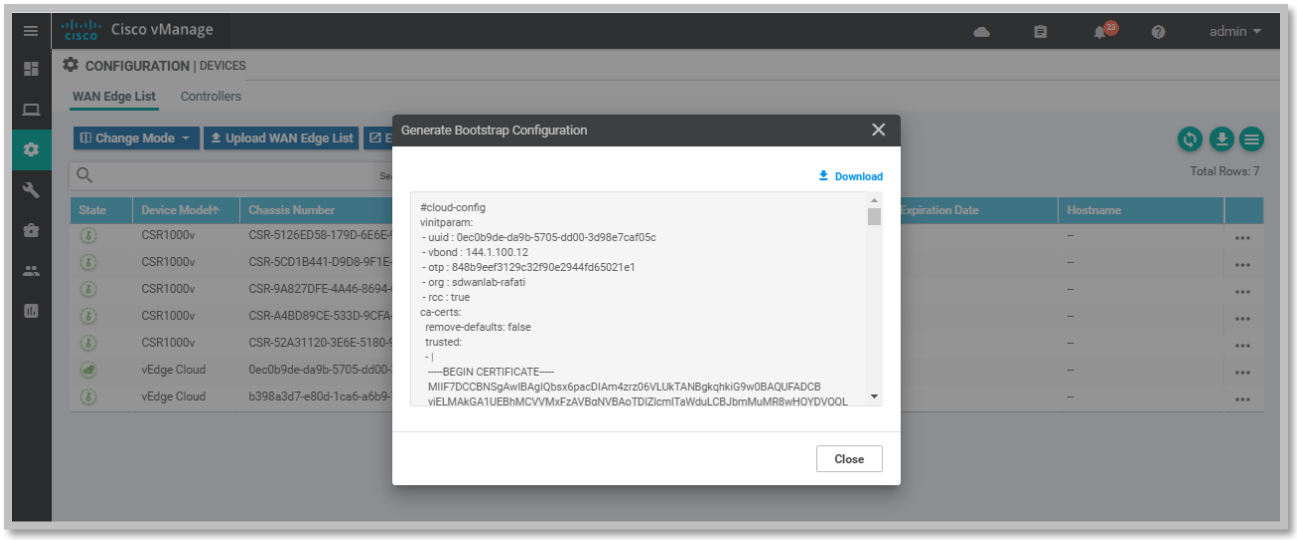
1- **`Configuration--> Devices--> WAN Edge List--> A vEdge Cloud--> ... --> Generate Bootstrap Configuration`**



2- For KVM select Cloud-Init. (VMWare uses Encoded String). Then click OK.



3- You can either download the file and SCP it across to the host server, or copy and paste the contents via a terminal to the server. Use the method you are most comfortable with.



4- Boot up vedge and Once you see the message System Ready login with the username/password admin and apply the following bootstrap config.

```
system
 host-name vEdge
 system-ip 102.1.1.2
 site-id 102
  organization-name "sdwanlab-webinar"
 clock timezone Asia/Tehran
 vbond 192.168.100.12

 ntp
  server 172.16.32.10
   version 4
   prefer
  exit
 !
!
vpn 0
 interface ge0/0
  ip address 172.16.102.2/24
  tunnel-interface
   allow-service all
  !
  no shutdown
 !
 ip route 0.0.0.0/0 172.16.102.1
!
commit
```

5- Copy root.cer on windows server to vEdge with command or Filezila or Winscp

6- Navigate vEdge cli then request install root cetificate

```
vEdge# request root-cert-chain install /home/admin/root.cer
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/root.cer via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

7- check root certificate install

```
vEdge# show certificate root-ca-cert | inc lab
        Issuer: DC=lab, DC=sdwan, CN=sdwan-DC1-CA
        Subject: DC=lab, DC=sdwan, CN=sdwan-DC1-CA
```

8- Now activate the vEdge using the chassis number and the one-time password from the cloud-init file

```
vEdge# request vedge-cloud activate chassis-number XXXXX token
XXXX
```

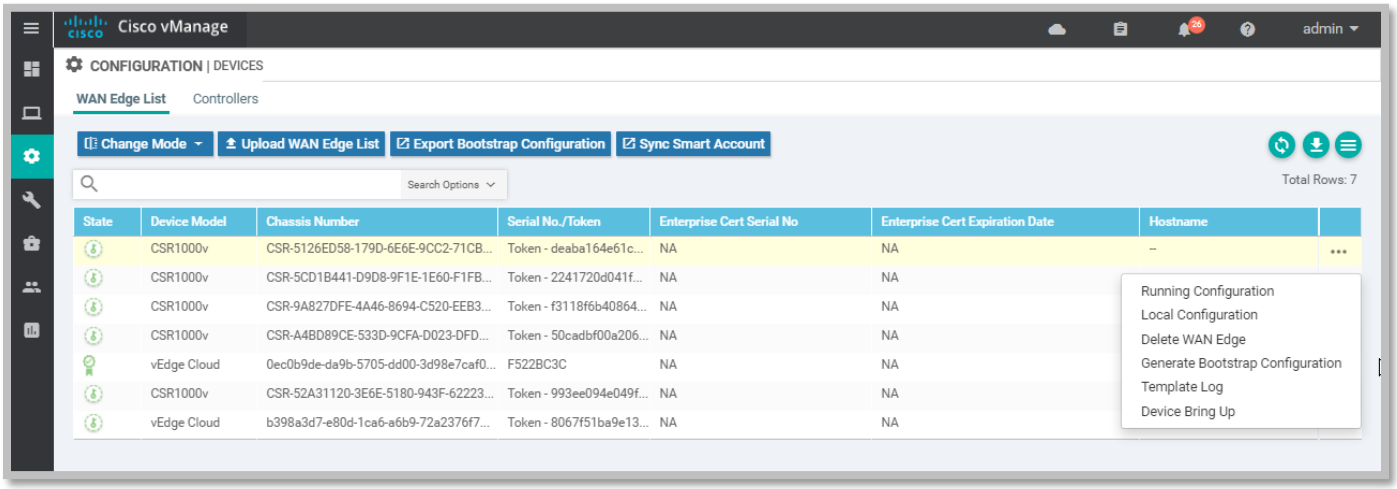
9- It will take a minute or two, but confirm that the control connections are active to the vManage, vBond and vSmart.

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	LOCAL	COLOR	PROXY	STATE	UPTIME	CONTROLLER GROUP ID
vsmart	dtls	100.1.1.13	100	1	192.168.100.13	12346	192.168.100.13	12346	default		No	up	0:00:03:03	0
vbond	dtls	0.0.0.0	0	0	192.168.100.12	12346	192.168.100.12	12346	default		-	up	0:00:03:04	0
vmanage	dtls	100.1.1.11	100	0	192.168.100.11	12546	192.168.100.11	12546	default		No	up	0:00:03:03	0

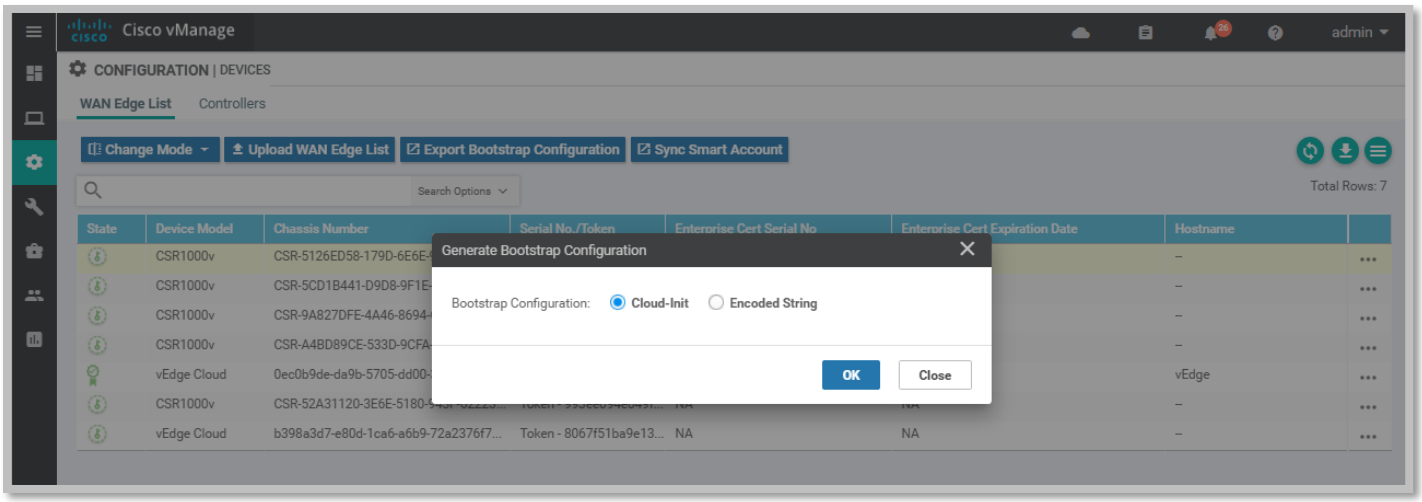
cEdge

1- Navigate to the devices page to generate the bootstrap config for the cEdge.

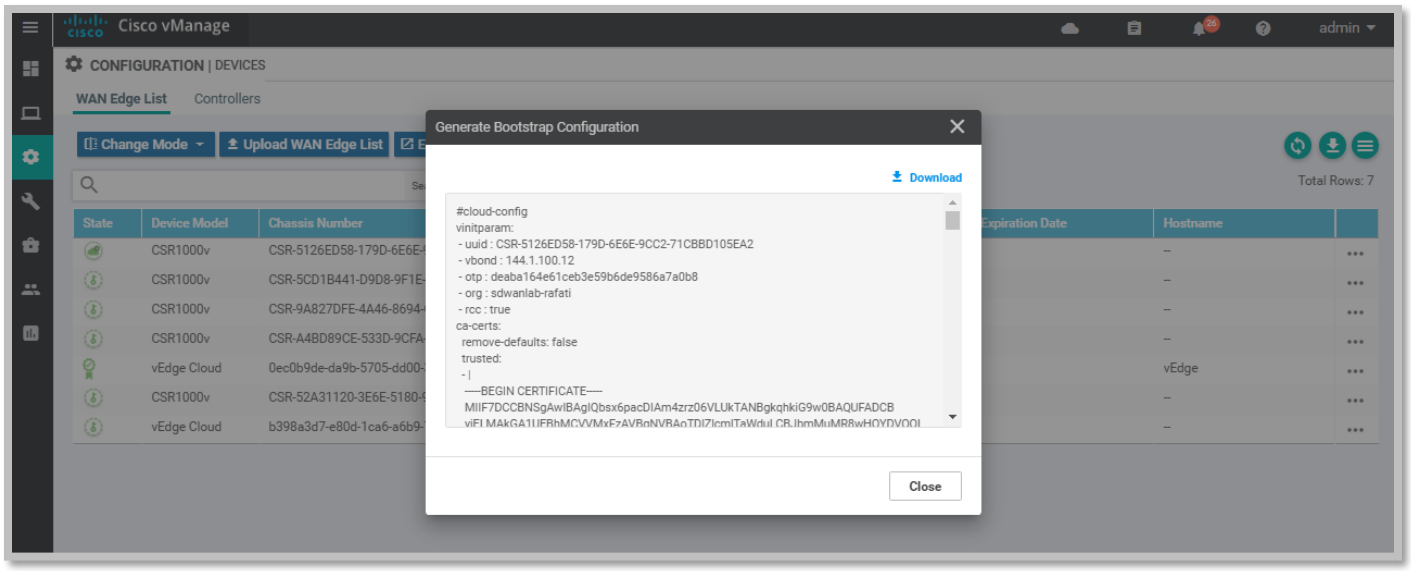
```
Configuration > Devices > WAN Edge List > A cEdge Cloud > ... > Generate
Bootstrap Configuration
```



2- For KVM select Cloud-Init. (VMWare uses Encoded String). Then click OK.



3- You can either download the file and SCP it across to the host server, or copy and paste the contents via a terminal to the server. Use the method you are most comfortable with.



4- Boot up cEdge and Once you see the message System Ready login with the username/password admin and apply the following bootstrap config.

```
config-transaction
!
system
 system-ip 103.1.1.2
 site-id  103
 organization-name "sdwanlab-webinar"
 vbond 192.168.100.12
!
hostname cEdge
username admin privilege 15 secret admin
interface GigabitEthernet1
 no shutdown
 ip address 172.16.103.2 255.255.255.0
exit

interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet1
 tunnel source GigabitEthernet1
 tunnel mode sdwan
exit
sdwan
 interface GigabitEthernet1
  tunnel-interface
   allow-service all
   encapsulation ipsec
  exit
 exit
ip route 0.0.0.0 0.0.0.0 172.16.103.1
```

5- Install the Root CA cert by SCP it from the vManage via the GigabitEthernet1 interface.

```
HQR1# copy scp://admin:admin@192.168.100.11 bootflash:
Address or name of remote host [192.168.100.11]?
Source username [admin]?
Source filename [root.cer]?
Destination filename [root.cer]?
viptela 19.3.0

 Sending file modes: C0644 1254 root.cer
!
1254 bytes copied in 0.607 secs (2066 bytes/sec)
```

6- Now install the Root CA certificate

```
HQR1# request platform software sdwan root-cert-chain install
bootflash:root.cer

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

7- Now activate the vEdge using the chassis number and the one-time password from the cloud-init file
8- using the the chassis number and the one-time password from the cloud-init file

```
HQR1# s XXXXXX Token XXXXXX
```

9- It will take a minute or two, but confirm that the control connections are active to the vManage, vBond and vSmart.

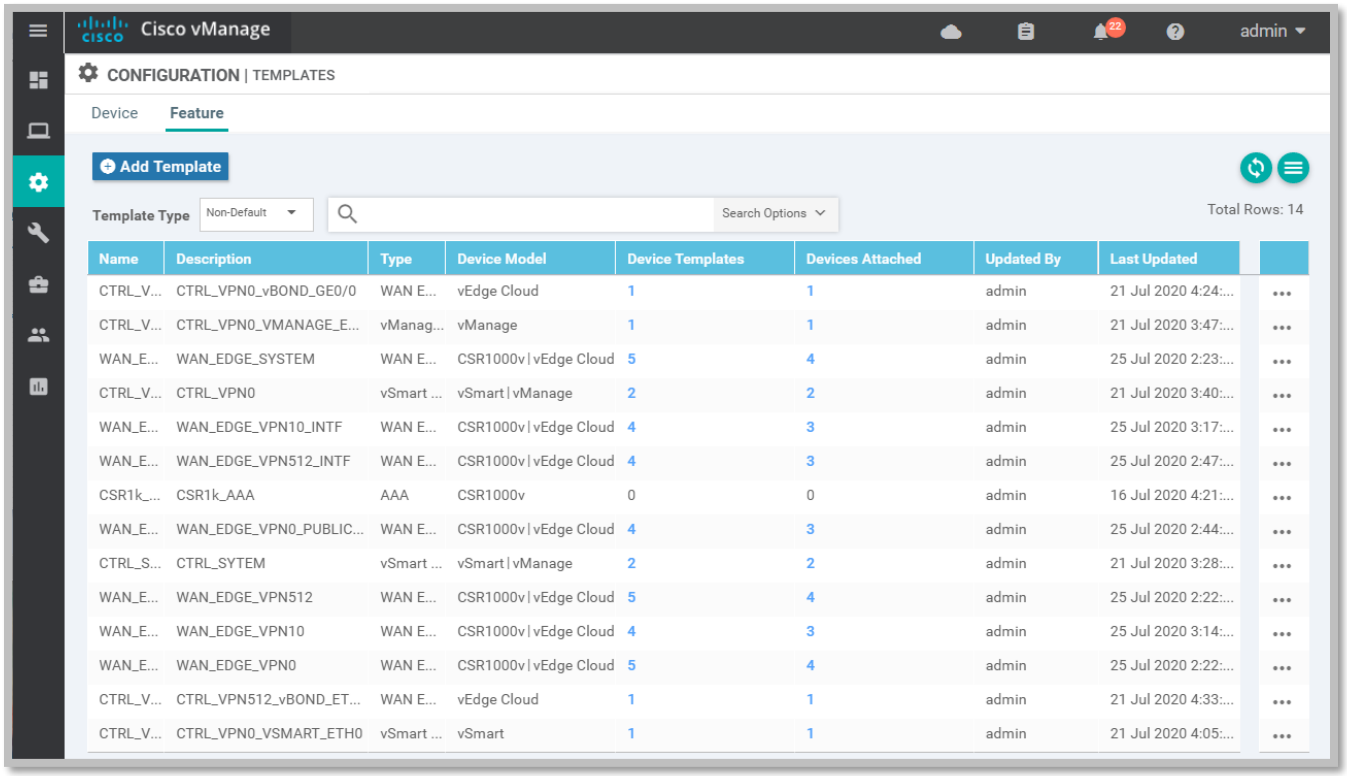
 # show control connections

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	LOCAL	COLOR	PROXY	STATE	UPTIME	CONTROLLER GROUP ID
vsmart	dtls	100.1.1.13	100	1	192.168.100.13	12346	192.168.100.13	12346	default		No	up	0:00:03:03	0
vbond	dtls	0.0.0.0	0	0	192.168.100.12	12346	192.168.100.12	12346	default		-	up	0:00:03:04	0
vmanage	dtls	100.1.1.11	100	0	192.168.100.11	12546	192.168.100.11	12546	default		No	up	0:00:03:03	0

Note: For HQR1, HQR2 same process but different Bootstrap config

SD-WAN Templates

Controllers Templates



➢ Configuration --> Template --> Feature --> Add template --> **vManage & vSmart** --> Select

System Feature

1- Template Name: `LAB _CTRL_SYSTEM`
2- Template Description: `LAB_SYSTEM_CTRL`
3- Select System
4- Change Time zone `Asia/Tehran`
5- Click Save

VPN Feature

1. Template Name: `LAB_VPN0_CTRL`
2. Template Description: `LAB_VPN0_CTRL`
3. Select VPN
4. ***Basic Configuration***
   4.1. Select `VPN0`
   4.2. Select Name Global: `Write Description`
5. ***DNS***
   5.1. Primary Address Global: `Write DNS Server`
6. ***IPv4 Route***
   6.1. Write Prefix `Default` and set Next hop

6.2. Click add

7. Click Save

➢ Configuration --> Template --> Feature --> Add template --> **vManage** --> Select

VPN Interface Ethernet feature

1. Select --> VPN Interface Ethernet
2. Template Name: LAB _VMANAGE_INT _ETH0
3. ***Basic Configuration***
   3.1. Shutdown: **`Global & NO`**
   3.2. Interface Name: **`eth0`**
   3.3. Description: **`VPN0 INT`**
4. ***IPV4 Configuration***
   `4.1.` Static **`(192.168.100.11/24)`**
   4.2. IPV4 Address: Device Specific "**`vpn0_if_ip_address`**"
5. ***Tunnel***
   `5.1.` Tunnel Interface: **`Global & on`**
   5.2. Allow Service: **`All`**

➢ Configuration --> Template --> Feature --> Add template --> **vSmart** --> Select

VPN Interface Ethernet feature

1. Select --> **`VPN Interface Ethernet`**
2. Template Name: **`LAB _VSMART_INT _ETH0`**
3. ***Basic Configuration***
   3.1. Shutdown: **`Global & NO`**
   3.2. Interface Name: **`eth0`**
   3.3. Description: **`VPN0 INT`**
4. ***IPV4 Configuration***
   4.1. Static **`(192.168.100.13/24)`**
   4.2. IPV4 Address: Device Specific **`vpn0_if_ip_address`**
5. ***Tunnel***
   5.1. Tunnel Interface: **`Global & on`**
   5.2. Allow Service: **`All`**

➢ Configuration --> Template --> Feature --> Add template --> **vEdge Cloud(vBond)** --> Select

System Feature

1- Template Name: **`LAB _WEDGE_SYSTEM`**
2- Template Description: **`LAB _WEDGE_SYSTEM`**
3- Select System
4- Change Time zone **`(Base on Location)`**
5- Click Save

VPN0 Feature

1. Template Name: **`LAB_WEDGE_VPN0`**
2. Template Description: **`LAB_WEDGE_VPN0`**
3. Select VPN
4. ***Basic Configuration***
   4.1. Select **`VPN0`**
   4.2. Select Name Global: **`VPN0 Overlay`**
5. ***DNS***
   5.1. Primary Address Global: **`192.168.100.10`**
6. ***IPv4 Route***
   6.1. Write Prefix **`0.0.0.0/0`** and set **`192.168.100.1`**
   6.2. Click add
7. Click Save

VPN512 Feature

1. Template Name**`: LAB_WEDGE_VPN512`**
2. Template Description: **`LAB_WEDGE_VPN512`**
3. Select VPN
4. Basic Configuration
   4.1. Select **`VPN512`**
   4.2. Select Name Global: **`VPN512 MGMT`**
5. Click Save

VPN0 Interface Ethernet feature

1. Select --> **`VPN Interface Ethernet`**
2. Template Name: **`LAB_VMANAGE_INT _GE0/0`**
3. ***Basic Configuration***
   3.1. Shutdown: **`Global & NO`**
   3.2. Interface Name: **`ge0/0`**
   3.3. Description: **`VPN0 INT`**
4. ***IPV4 Configuration***
   4.1. Static **`(192.168.100.12/24)`**
   4.2. IPV4 Address: Device Specific "**`vpn0_if_ip_address`**
5. ***Tunnel***
   5.1. Tunnel Interface: **`Global & on`**
   5.2. Color: **`Global & public-internet`**
   5.3. Allow Service: **`All`**
   5.4. PMTU Discovery: **`On`**

VPN512 Interface Ethernet feature

1. Select --> **`VPN Interface Ethernet`**
2. Template Name: **`LAB_VMANAGE_INT _ETH0`**
3. ***Basic Configuration***
   3.1. Shutdown: **`Global & NO`**
   3.2. Interface Name: **`eth0`**
   3.3. Description: **`VPN512 MGMT`**
4. ***IPV4 Configuration***
   4.1. dhcp

WAN Edge Templates

- Configuration --> Template --> Feature --> Add template --> **CSR1000v & vEdge Cloud** --> Select

System Feature

1- Template Name: `LAB_WEDGE_SYSTEM`
2- Template Description: `WEDGE_SYSTEM`
3- Select System IP, Site ID, Hostname `Device Specific`
4- Change Time zone `(Base on Location)`
5- Click Save

VPN0 Feature

8. Template Name: `LAB_WEDGE_VPN0`
9. Template Description: `LAB_WEDGE_VPN0`
10. Select VPN
11. ***Basic Configuration***
    11.1. Select `VPN0`
    11.2. Select Name Global: `Write Description`
12. ***DNS***
    `12.1.` Primary Address Global: `Write DNS Server`
13. ***IPv4 Route***
    13.1. Write Prefix `Default` and set `Next hop`
    13.2. Click add
14. Click Save

VPN512 Feature

1. Template Name: `LAB_WEDGE_VPN512`
2. Template Description: `LAB_WEDGE_VPN512`
3. Select VPN
4. ***Basic Configuration***
   4.1. Select `VPN512`
   4.2. Select Name Global: `Write Description`
5. Click Save

VPN0 Interface Ethernet feature `vEdge Cloud`

6. Select --> `VPN Interface Ethernet`
7. Template Name: `LAB_VEDGE_GE0/0_INET`
8. ***Basic Configuration***
   8.1. Shutdown: `Global & NO`
   8.2. Interface Name: `ge0/0`
   8.3. Description:
9. ***IPV4 Configuration***
   9.1. Static
   9.2. IPV4 Address: Device Specific `vpn0_if_ip_address`
10. ***Tunnel***
    10.1. Tunnel Interface: `Global & on`
    10.2. Color: `Global & public-internet`
    10.3. Allow Service: `All`
    10.4. PMTU Discovery: `On`

VPN512 Interface Ethernet feature `vEdge Cloud`

5. Select --> `VPN Interface Ethernet`
6. Template Name: `LAB_VMANAGE_INT_ETH0`
7. ***Basic Configuration***
   7.1. Shutdown: `Global & NO`
   7.2. Interface Name: `eth0`
   7.3. Description: `VPN512 MGMT`

VPN0 Interface Ethernet feature `CSR1000v`

11. Select --> `VPN Interface Ethernet`
12. Template Name: `LAB_VEDGE_G1_INET`
13. ***Basic Configuration***
    13.1. Shutdown: `Global & NO`
    13.2. Interface Name: `GigabitEthrent1`
    13.3. Description:
14. ***IPV4 Configuration***
    14.1. Static
    14.2. IPV4 Address: Device Specific `vpn0_if_ip_address`
15. ***Tunnel***
    15.1. Tunnel Interface: `Global & on`
    15.2. Color: `Global & public-internet`
    15.3. Allow Service: `All`
    15.4. PMTU Discovery: `On`

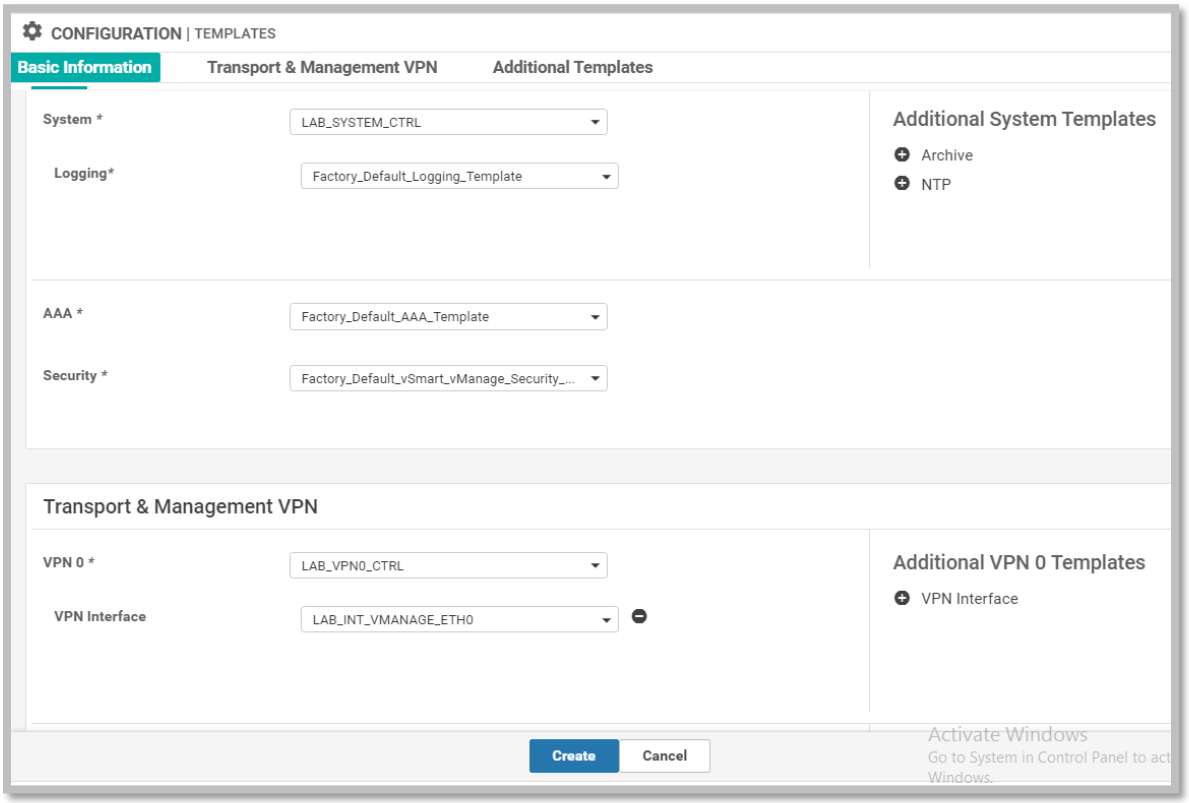
Device Template

Controllers

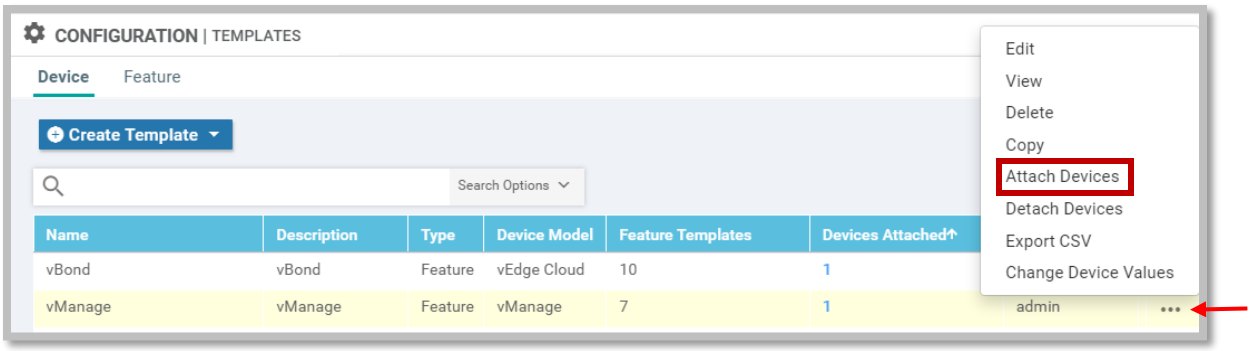
➢ Configuration --> Template --> Device --> Create template -->
--> Select

Device Model: vManage

1- Template Name: `vManage`
2- System: `LAB_CTRL_SYSTEM`
3- VPN0: `LAB_CTRL_VPN0`
4- Click ⊕ `VPN Interface`
5- VPN Interface: `LAB_INT_VMANAGE_ETH0`
6- Click `Create`

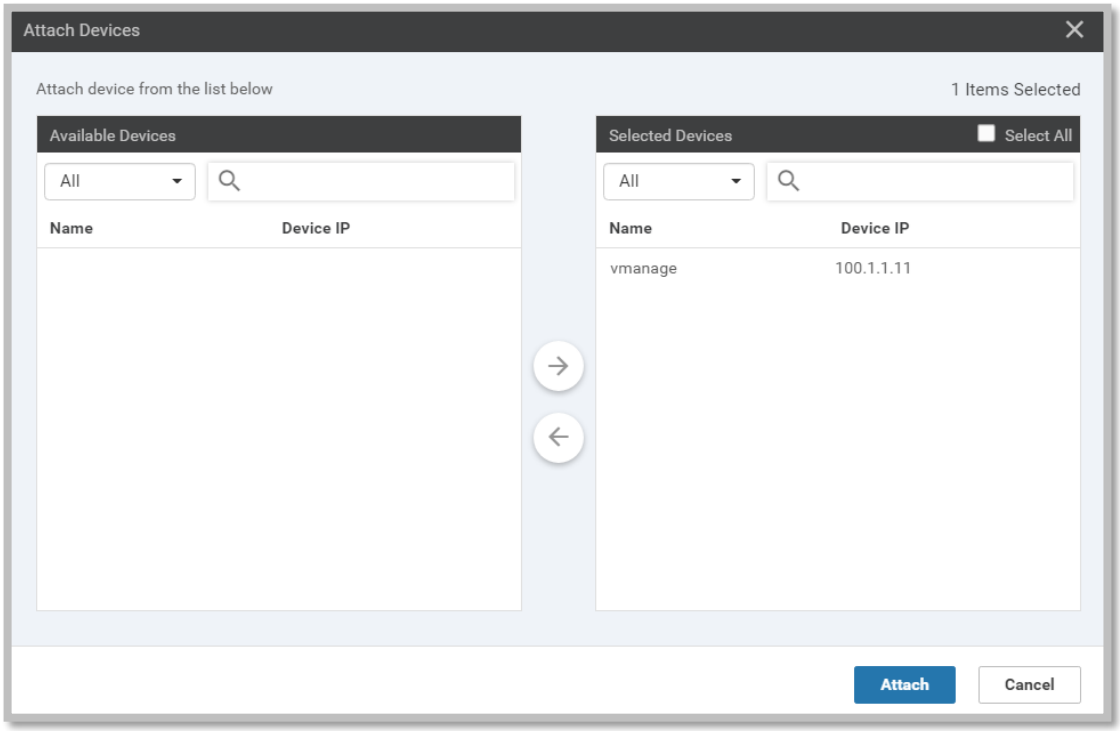


7- Click on …



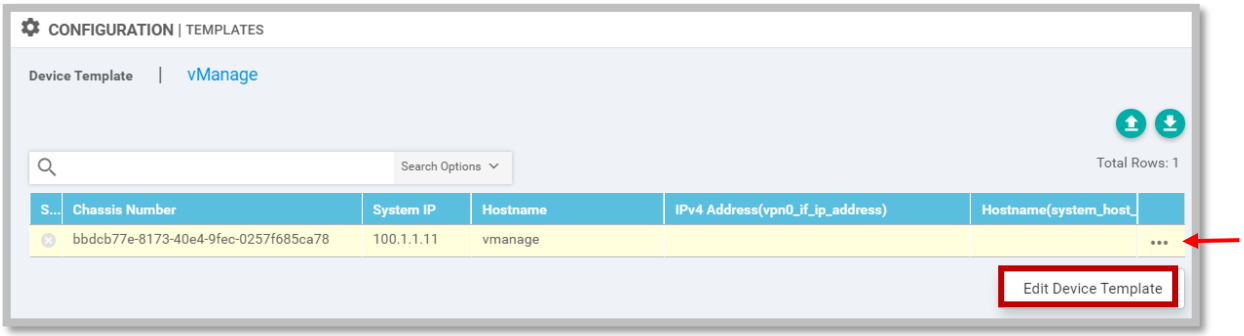
8- Select **`Attach Device`**

9- add **`vManage`** form Available Device to Selected Device

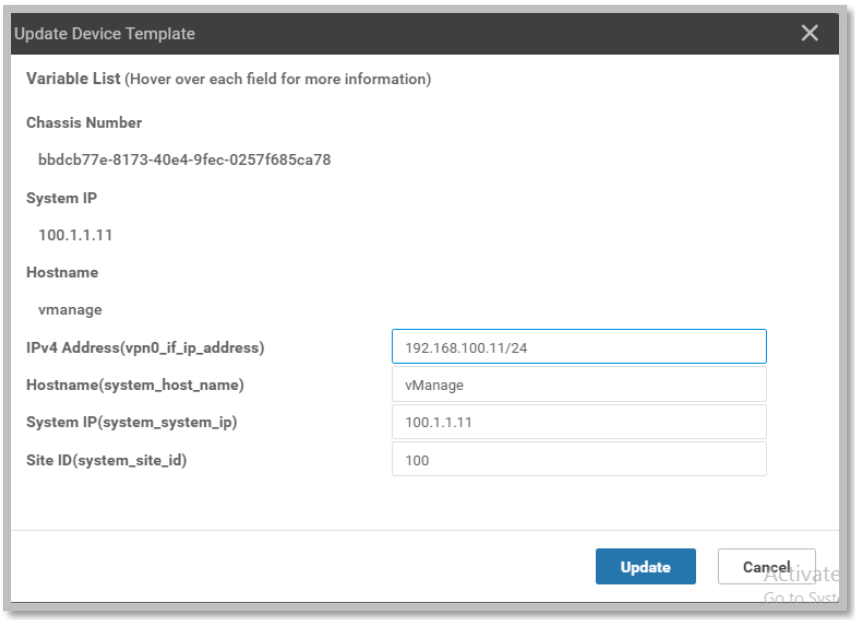


10- Click **`Attach`**

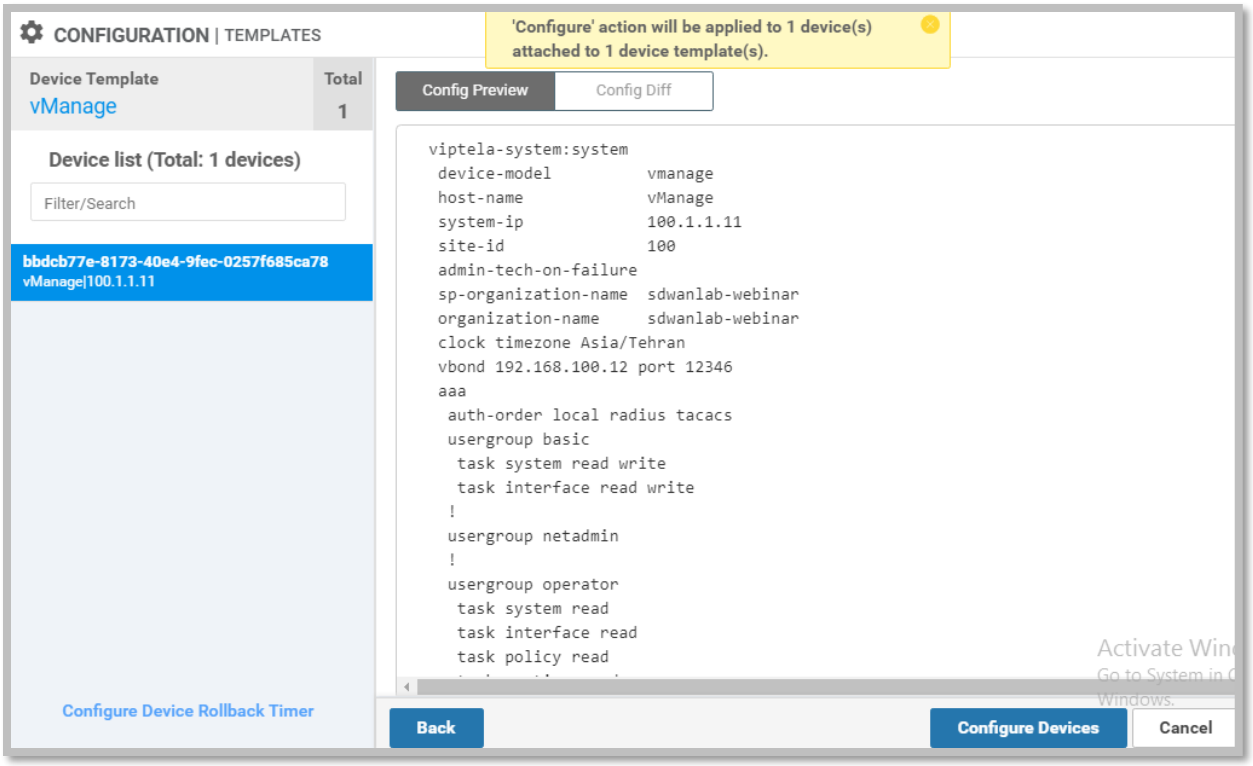
11- Click on … then **`Edit Device template`**



12- Fill require Field then Click Update



13- Review the Configuration and click Configure Device



Device Model: vSmart

1- Template Name: **`vSmart`**
2- System: **`LAB_CTRL_ SYSTEM`**
3- VPN0: **`LAB_CTRL_VPN0`**
4- Click ⊕ **`VPN Interface`**
5- VPN Interface: **`LAB_INT_VMANAGE_ETH0`**
6- Click Create
7- Click on **`…`**
8- Select **`Attach`** Device
9- add **`vSmart`** form Available Device to Selected Device
10- Click **`Attach`**
11- Click on … then edit Device template and fill require Field then Click Update
12- Review Configuration and click Configure Device

Device Model: vBond

1- Template Name: vBond
2- System: **`LAB_WEDGE_SYSTEM`**
3- VPN0: **`LAB_WEDGE_VPN0`**
4- Click ⊕ **`VPN Interface`**
5- VPN Interface: **`LAB_INT_WEDGE_GE0/0_INET`**
6- VPN512: **`LAB_WEDGE_VPN512`**
7- Click ⊕ **`VPN Interface`**
8- VPN Interface: **`LAB_VMANAGE_INT_ETH0`**
9- Click **`Create`**
10- Click on **`…`**
11- Select **`Attach`** Device
12- add **`vBond (vEdge)`** form Available Device to Selected Device
13- Click Attach
14- Click on … then edit Device template and fill require Field then Click **`Update`**

WAN Edges

- Configuration --> Template --> Device --> Create template --> Select -- >

Device Model: vEdge Cloud

1- Template Name: **vEdge Cloud**
2- System: **LAB_WEDGE_SYSTEM**
3- VPN0: **LAB_WEDGE_VPN0**
4- Click ⊕ **VPN Interface**
5- VPN Interface: **LAB_WEDGE _GE0/0 _INET**
6- VPN512: **LAB_WEDGE_VPN512**
7- Click ⊕ **VPN Interface**
8- VPN Interface: **LAB_VMANAGE_INT_ETH0**
9- Click **Create**
10- Click on **…**
11- Select **Attach Device**
12- Move vEdge form Available Device to Selected Device
13- Click **Attach**
14- Click on **…** then edit Device template
15- Fill require Field then Click **Update**
16- Review the Configuration and click **Configure Device**

Device Model: CSR1000v

1- Template Name: vEdge Cloud
2- System: **LAB_VEDGE_SYSTEM**
3- VPN0: **LAB_WEDGE_VPN0**
4- Click ⊕ **VPN Interface**
5- VPN Interface: **LAB_VEDGE_G1_INET**
6- Click **Create**
7- Click on **…**
8- Select **Attach Device**
9- Move cEdge form Available Device to Selected Device
10- Click **Attach**
11- Click on **…** then edit Device template
12- Fill require Field then Click **Update**
13- Review the Configuration and click **Configure Device**