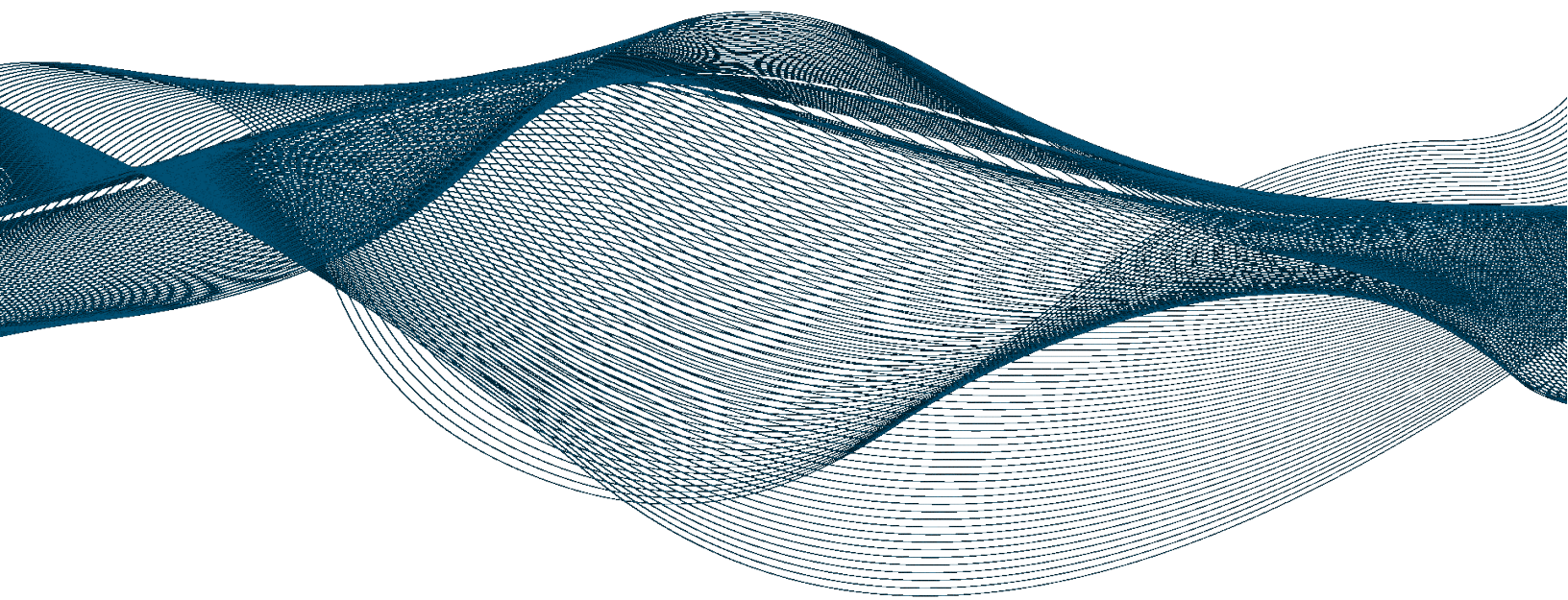




Deployment CISCO SD-WAN LAB ON EVE-NG



Mostafa-Rafati

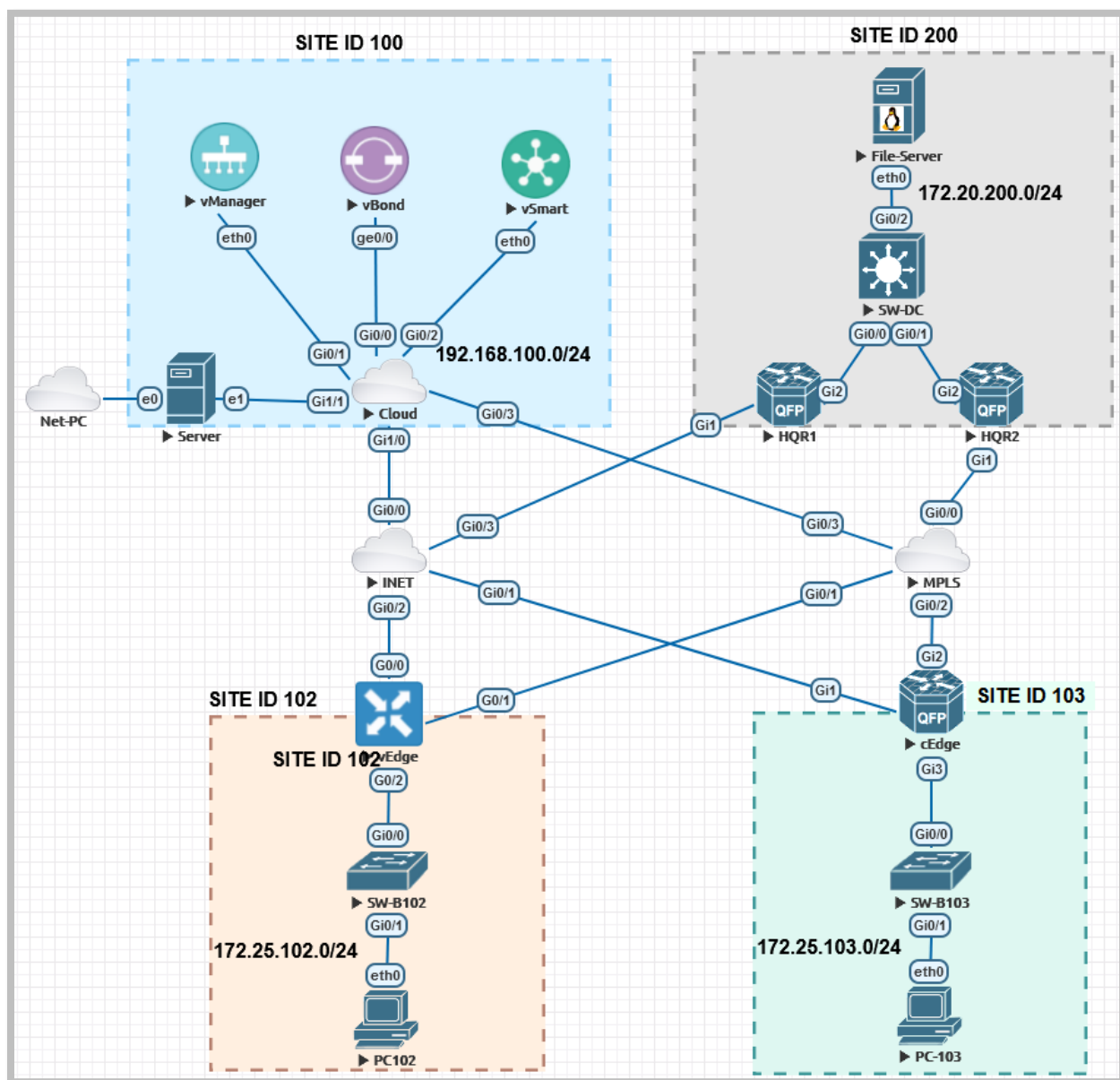
SD-WAN LAB on Eve-ng

EVE-NG Requirements (Cisco SD-WAN)	3
SD-WAN LAB Diagram on EVE-NG	3
Add Viptela Controller on EVE-NG	4
Deployment of Cisco Viptela vManage 19.3 image.....	4
Deployment of Cisco Viptela vSmart 19.3 image	4
Deployment of Cisco Viptela vBond 19.3 image	4
Add WAN-Edge on EVE-NG	5
Add Viptela vEdge 19.3 image on EVE-NG	5
Add CSR1000v SD-WAN on EVE-NG	5
Windows Server Active Directory & Certificate Server	6
Pre requirement for Active Directory Certificate Server	6
Active Directory Installation.....	7
Active Directory Certificate Server Installation	12
Cisco Smart Account	19
Login Smart Account	19
Add Controller Profile	19
Add Virtual Edges cloud & CSR1000v	22
Serial File	25
SD-WAN Controller Configuration on EVE-NG	26
vManage.....	26
vBond	33
vSmart.....	37
SD-WAN WAN Edges Configuration on EVE-NG	40
vEdge Cloud	41
cEdge	44
SD-WAN Templates	47
Controllers Templates	47
WAN Edge Templates	50
Device Template.....	52

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
```

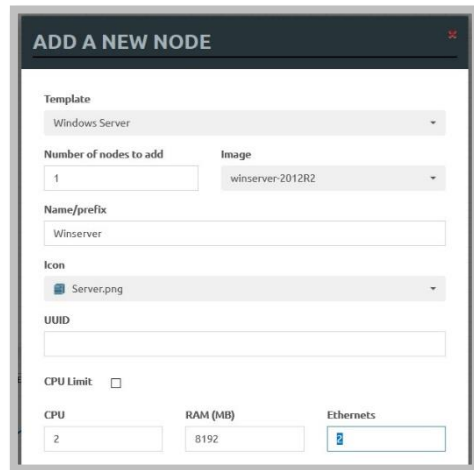
- 5- Fix permissions:

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

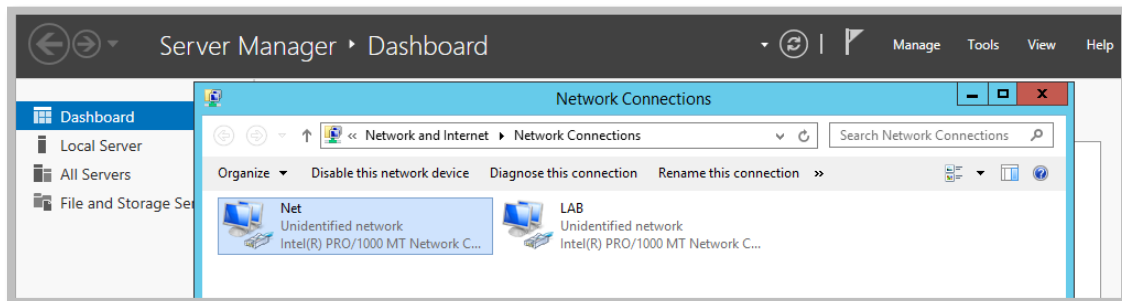
Windows Server Active Directory & Certificate Server

Pre requirement for Active Directory Certificate Server

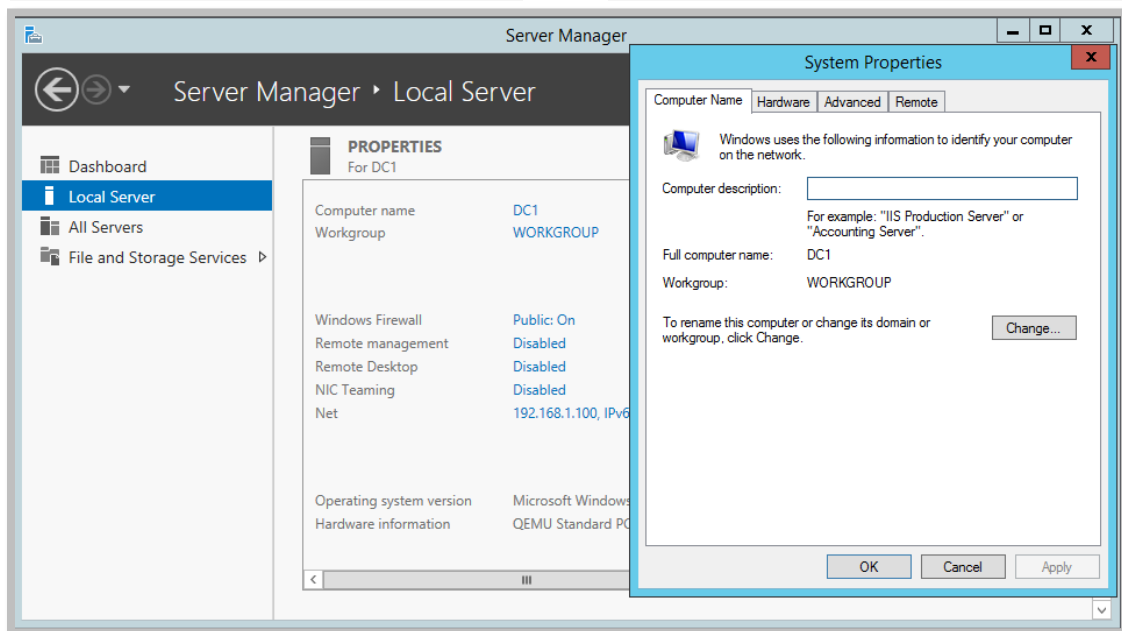
1. Add Node Windows Server 2012 with 2 Ethernet
2. Start Windows Server 2012 Node, Then Login to Windows Server 2012



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

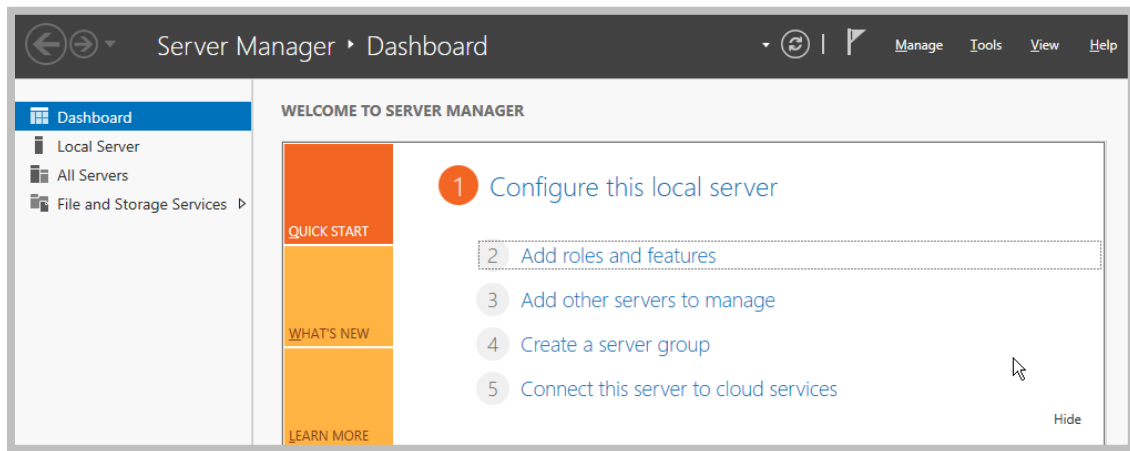


4. On Server Manager > Local Server change Computer Name (Restart required)

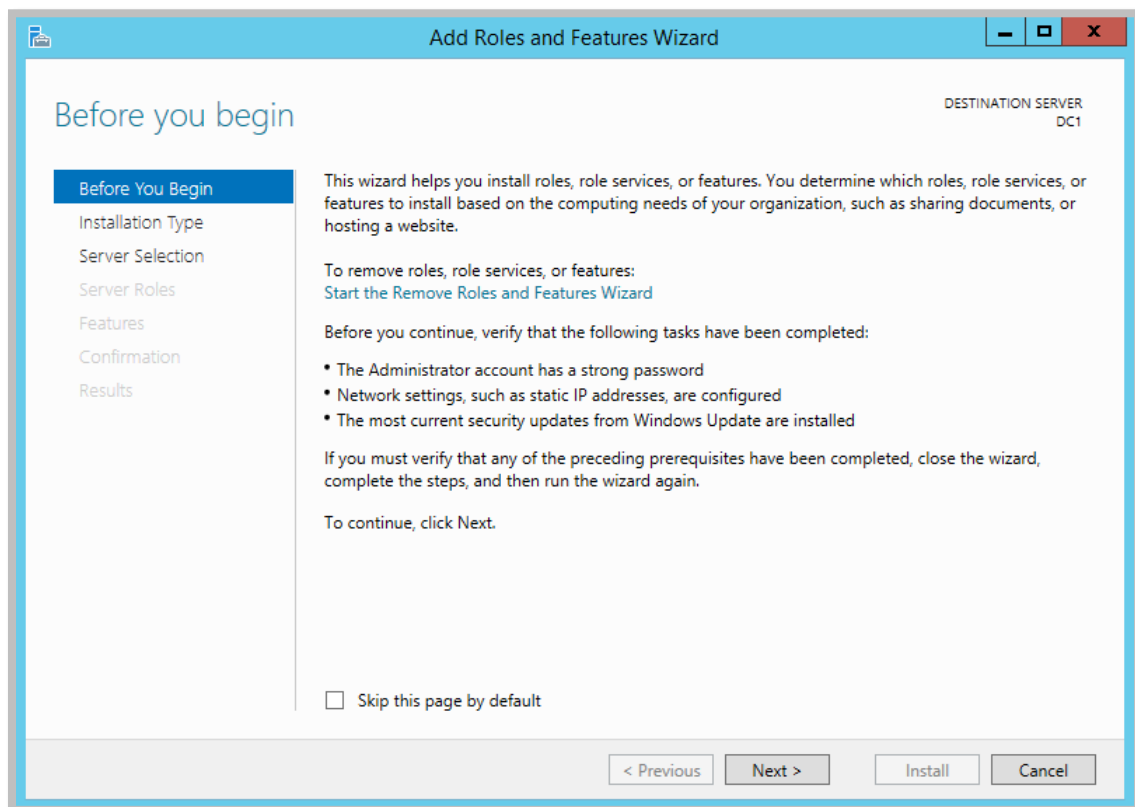


Active Directory Installation

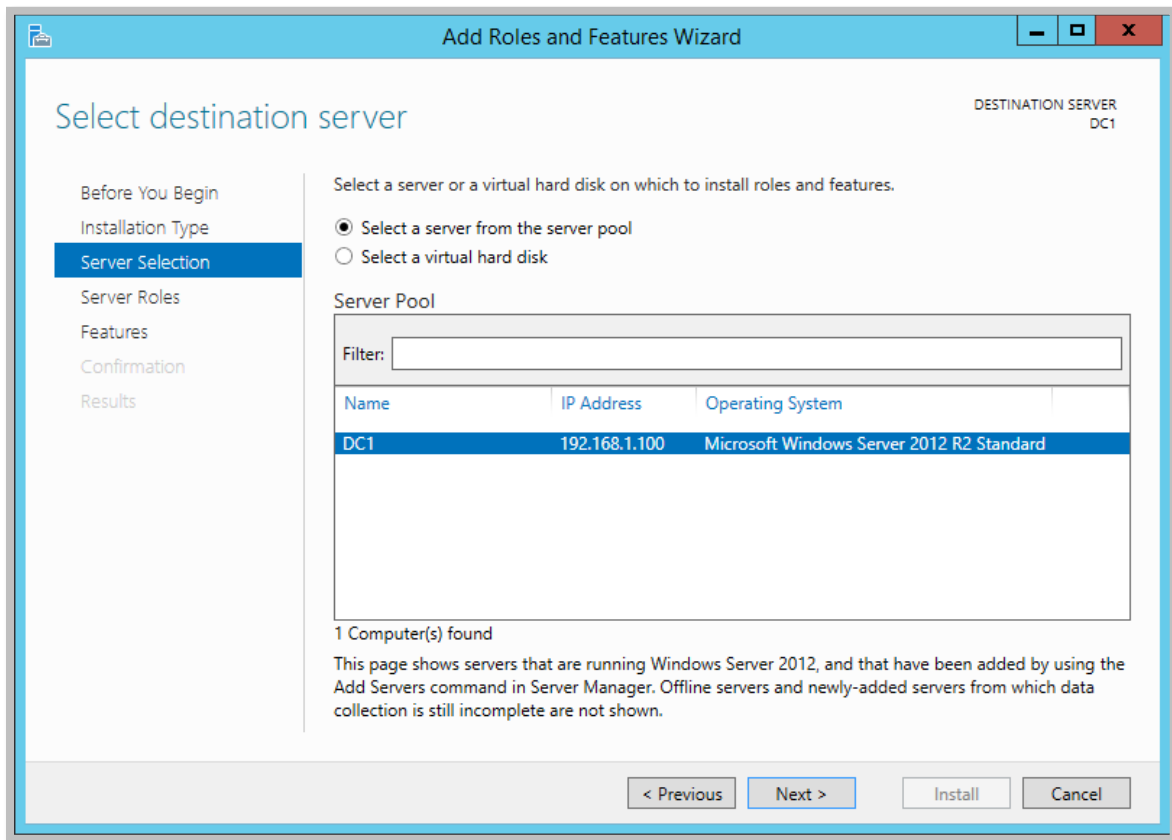
1. On **Server Manager** -> **Dashboard**
2. Select **Add Role and Feature**



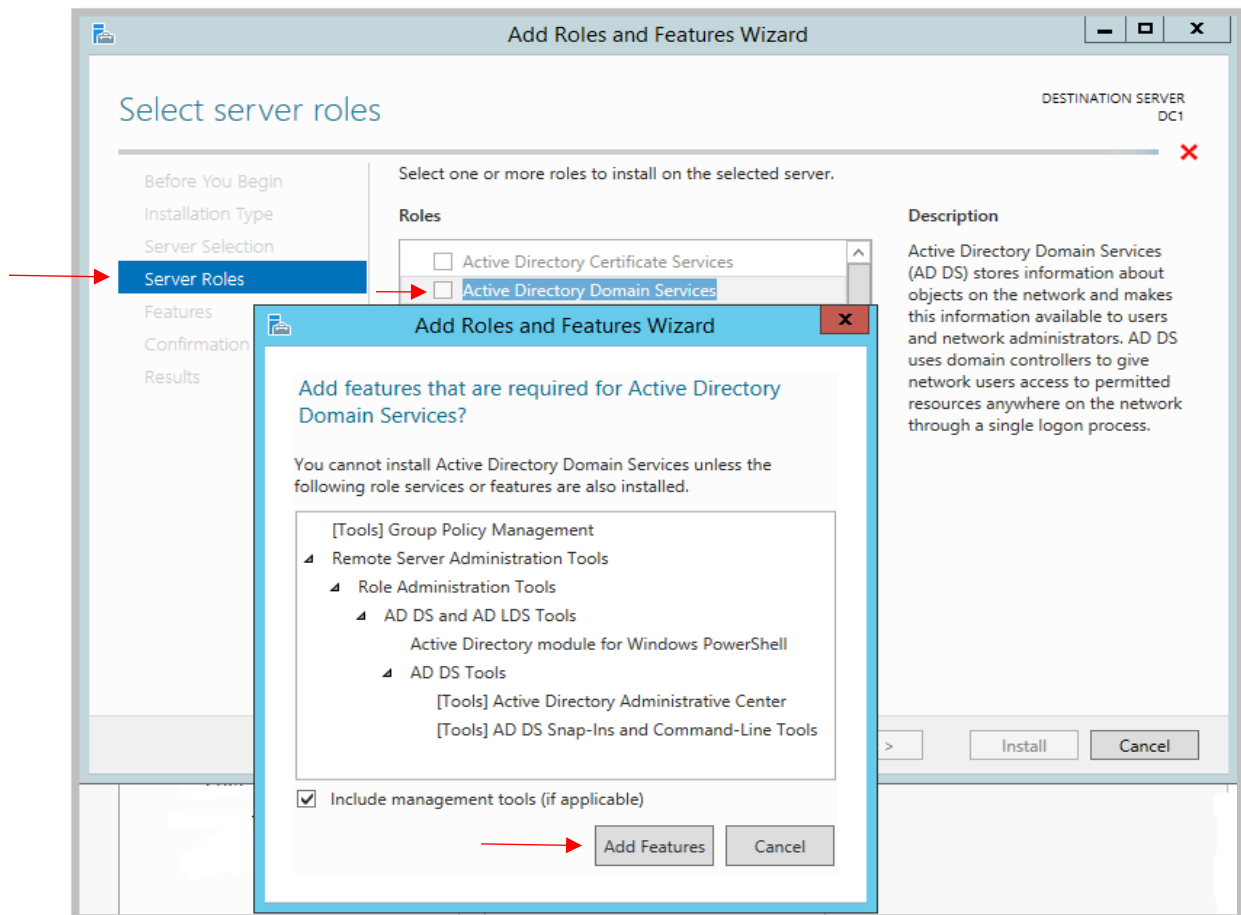
3. On **Before You Begin** Page Select **Next**



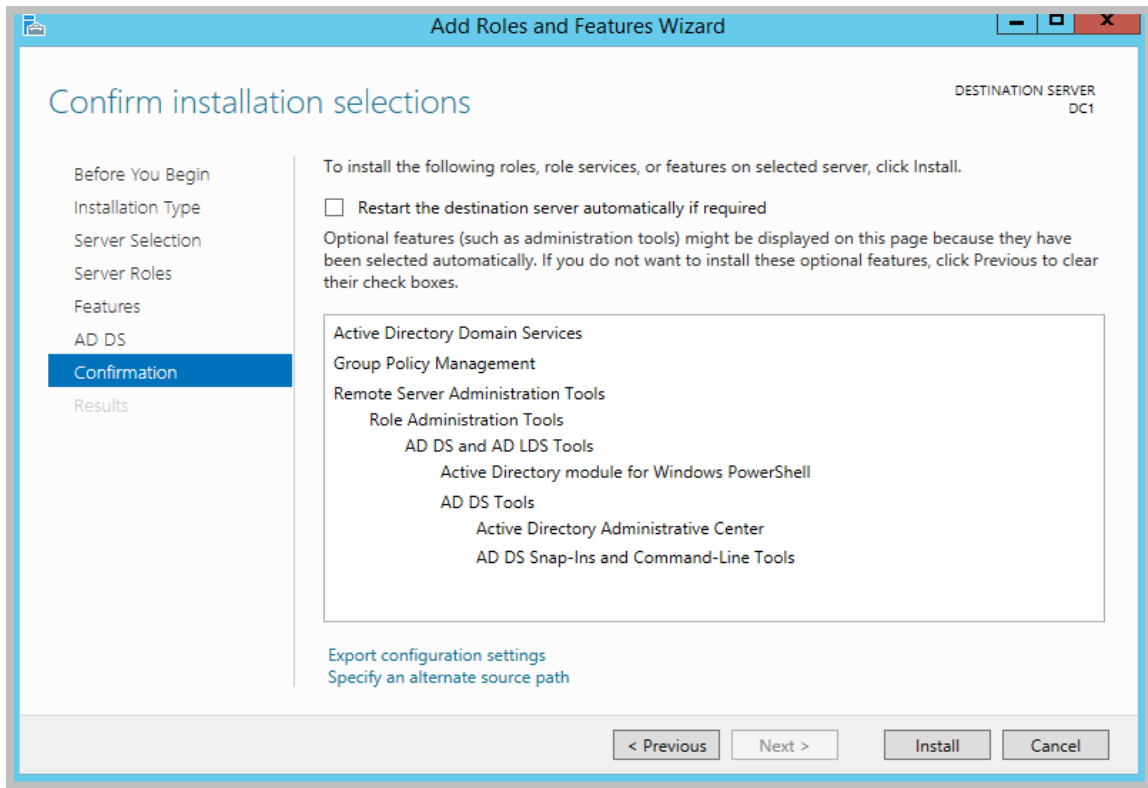
4. On **Installation type** page, select **Role-based or Feature-based Installation** then Select **Next**
5. On **Server selection** page, select **DC1** Server then select **Next**



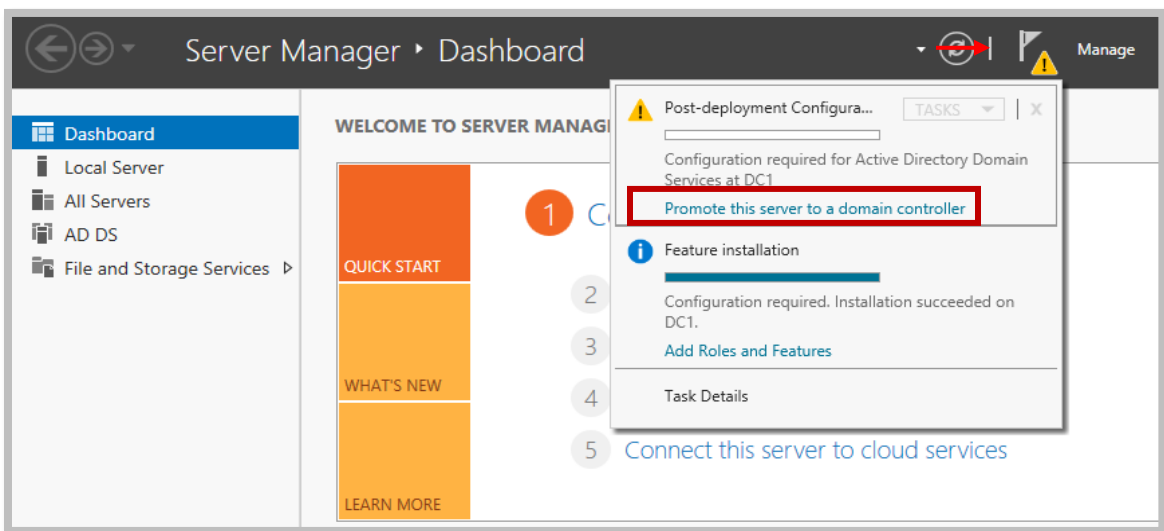
6. on Server Role page, select **Active Directory Domain Services** then click **Add Feature**



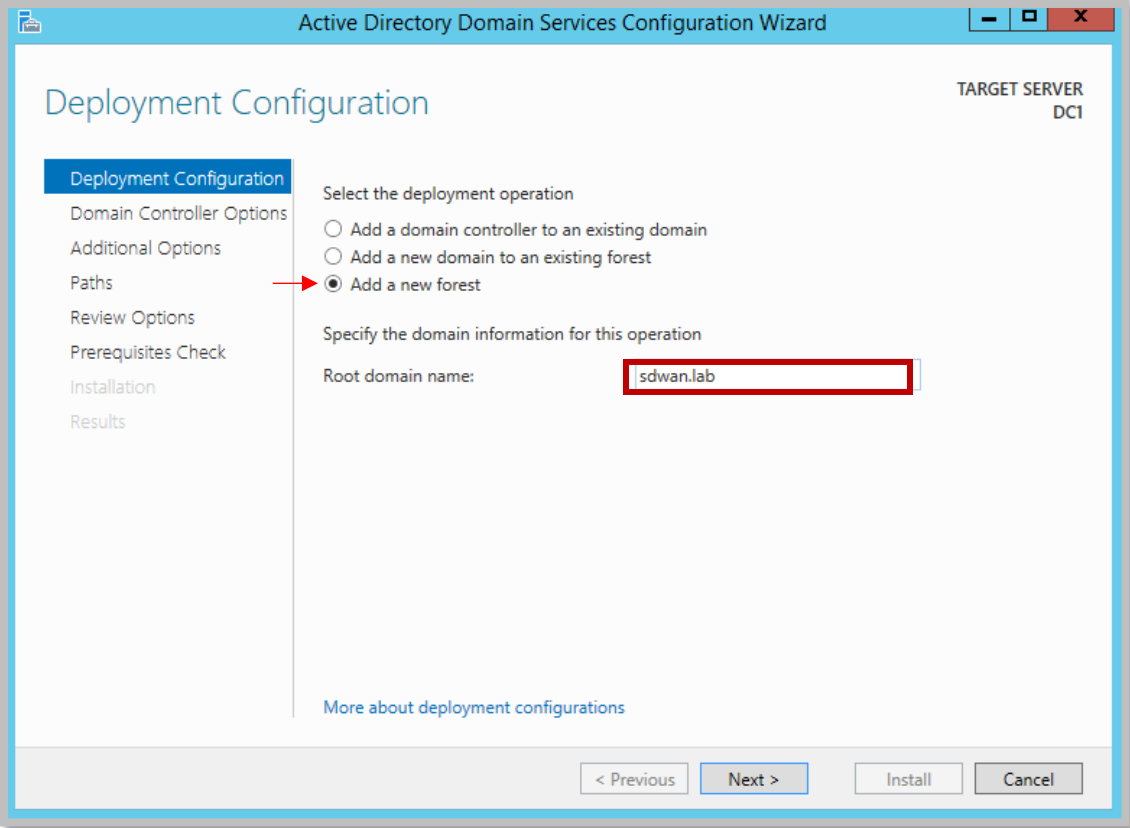
7. Select **Next** on **Features** and **AD DS** page, then click **Install**



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

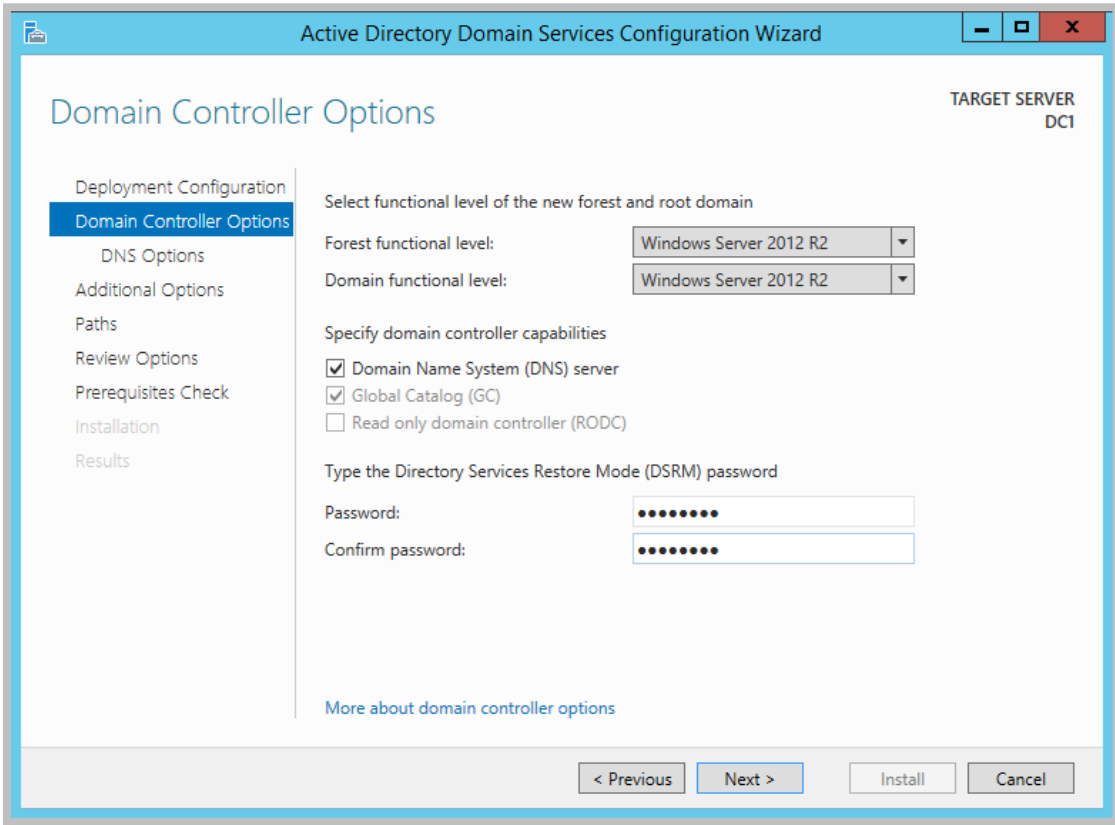


9. Select **Add a new Forest**. Root Domain name: **sdwan.lab**



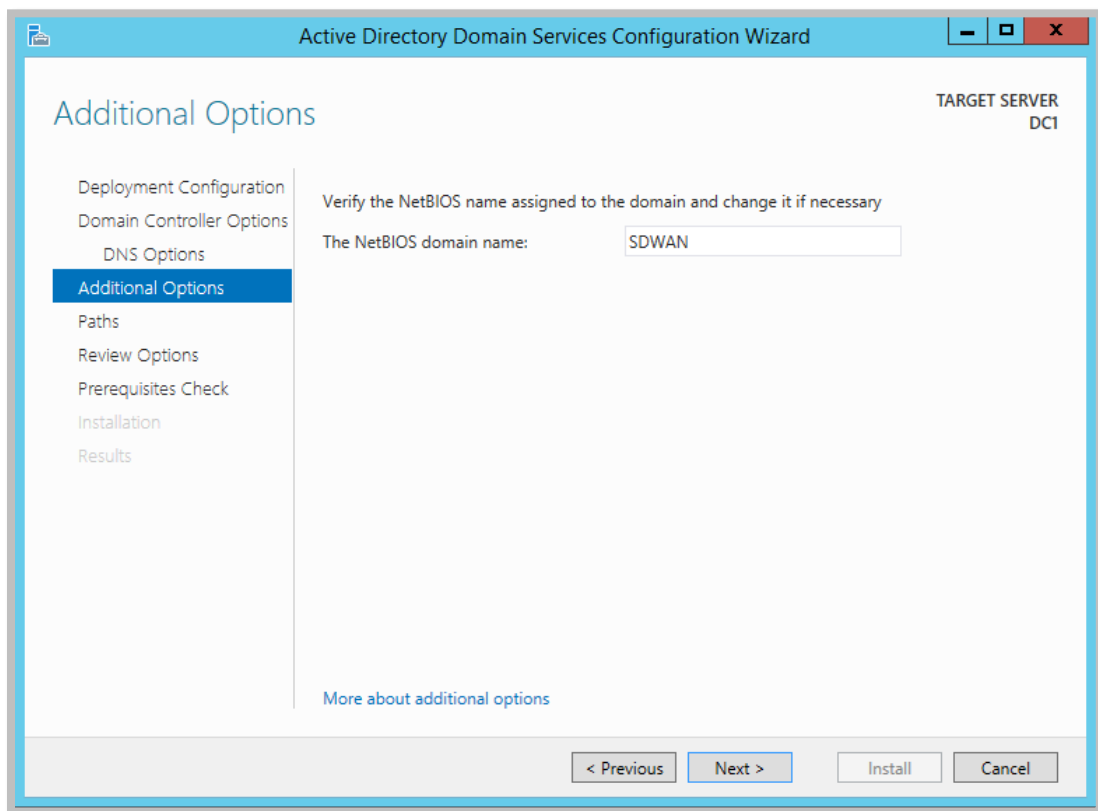
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Deployment Configuration'. On the left, a navigation pane lists steps: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. A red arrow points to the 'Add a new forest' radio button under the heading 'Select the deployment operation'. Below this, under 'Specify the domain information for this operation', the 'Root domain name' is set to 'sdwan.lab' in a text box. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. The top right corner indicates 'TARGET SERVER DC1'.

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

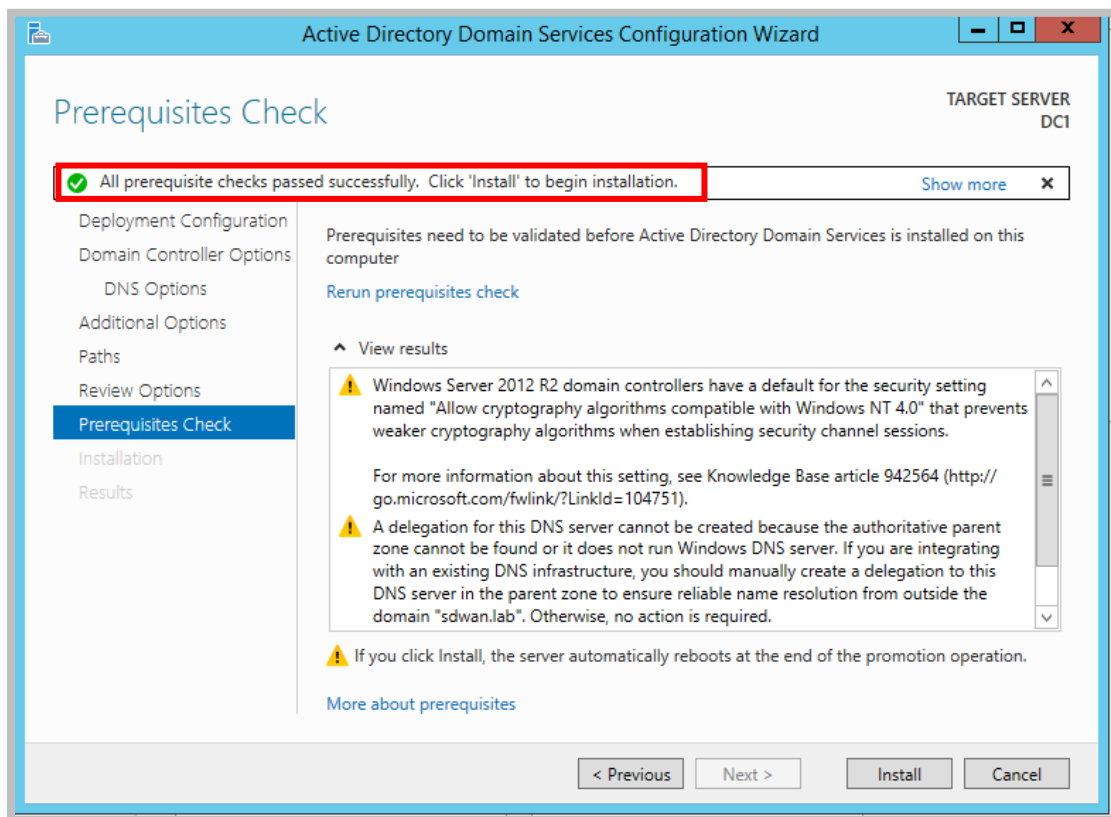


The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window at the 'Domain Controller Options' step. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Domain Controller Options'. On the left, the navigation pane shows 'Domain Controller Options' selected. The main area has the heading 'Select functional level of the new forest and root domain'. Below this, 'Forest functional level' and 'Domain functional level' are both set to 'Windows Server 2012 R2' in dropdown menus. Under 'Specify domain controller capabilities', the checkboxes for 'Domain Name System (DNS) server' and 'Global Catalog (GC)' are checked, while 'Read only domain controller (RODC)' is unchecked. Below this, there is a section 'Type the Directory Services Restore Mode (DSRM) password' with two password fields labeled 'Password:' and 'Confirm password:'. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. The top right corner indicates 'TARGET SERVER DC1'.

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

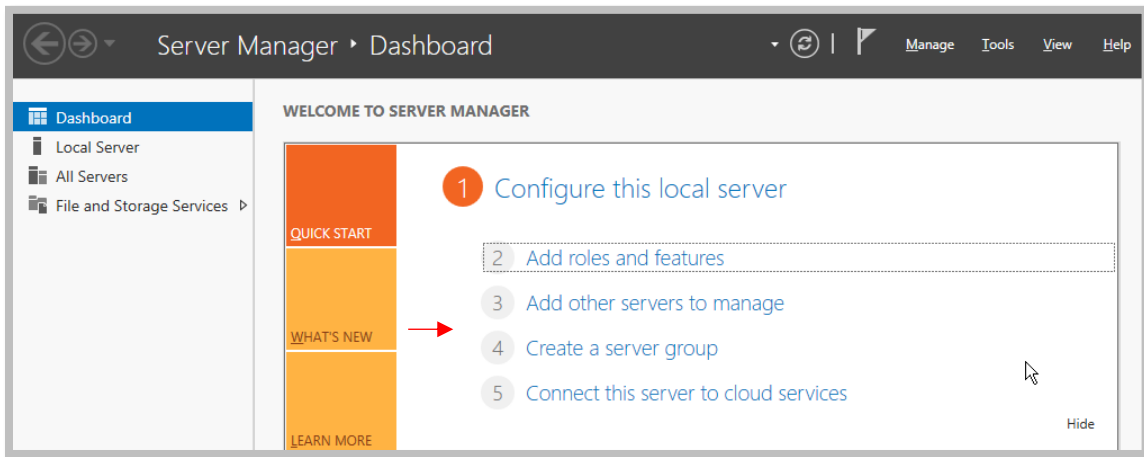


13. On Paths and Review Check page, select **Next**
14. On Prerequisites Check page, if same in the picture, select **Install**

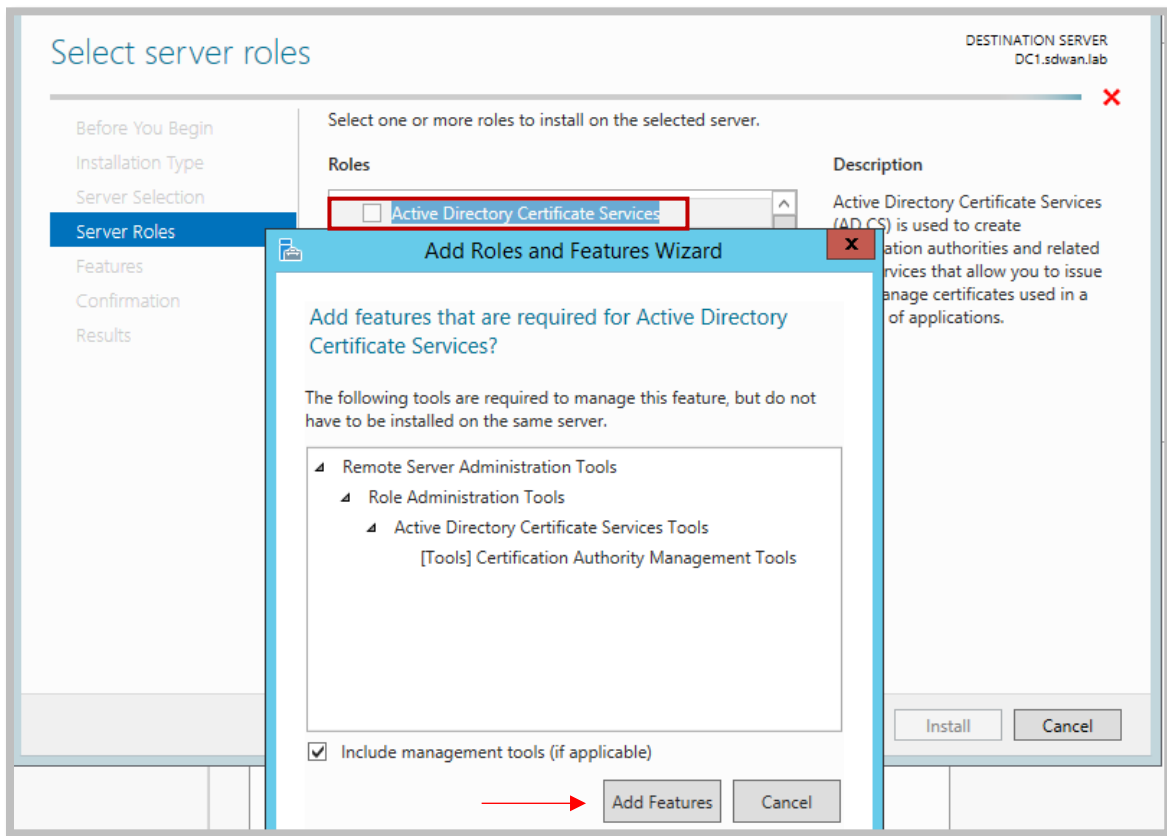


Active Directory Certificate Server Installation

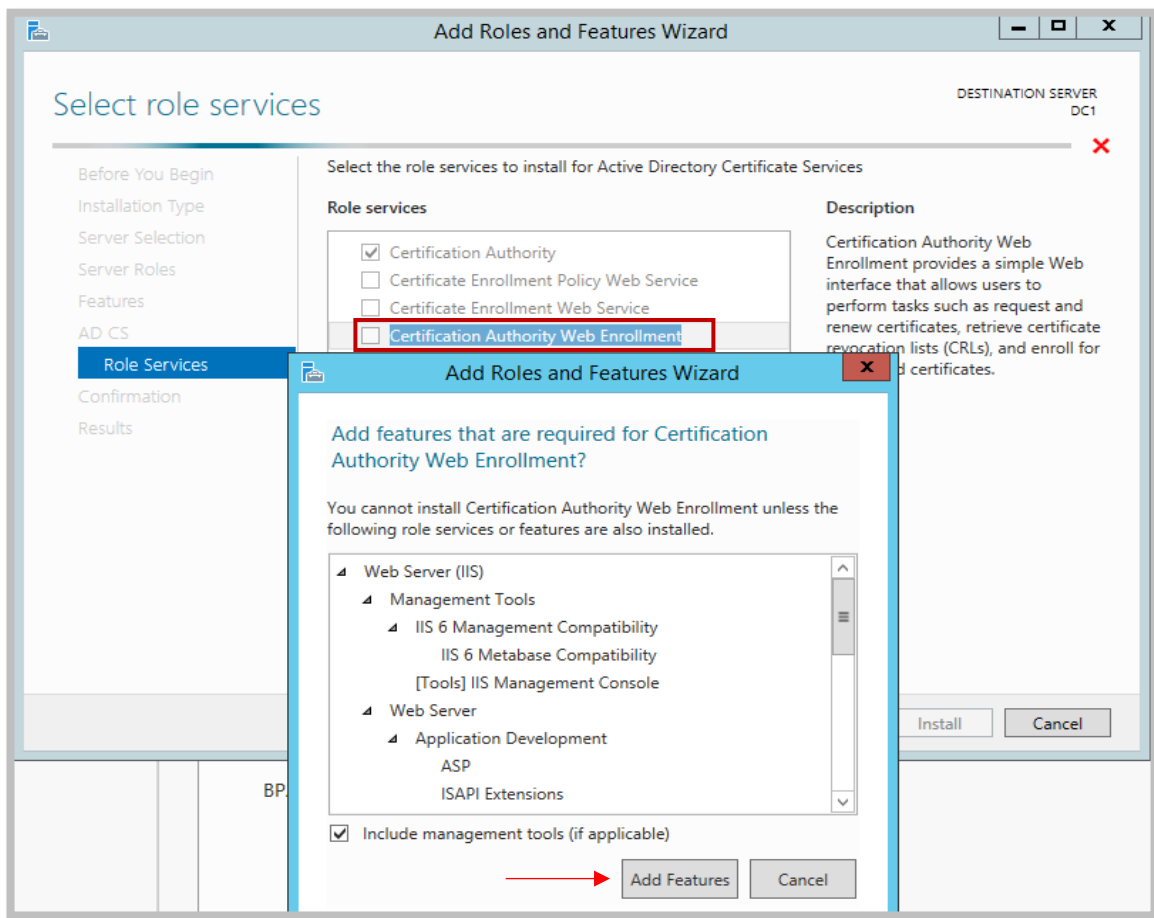
15. Now login to windows server AD Domain
16. On **Server Manager** -> **Dashboard**
17. Select **Add Role and Feature**



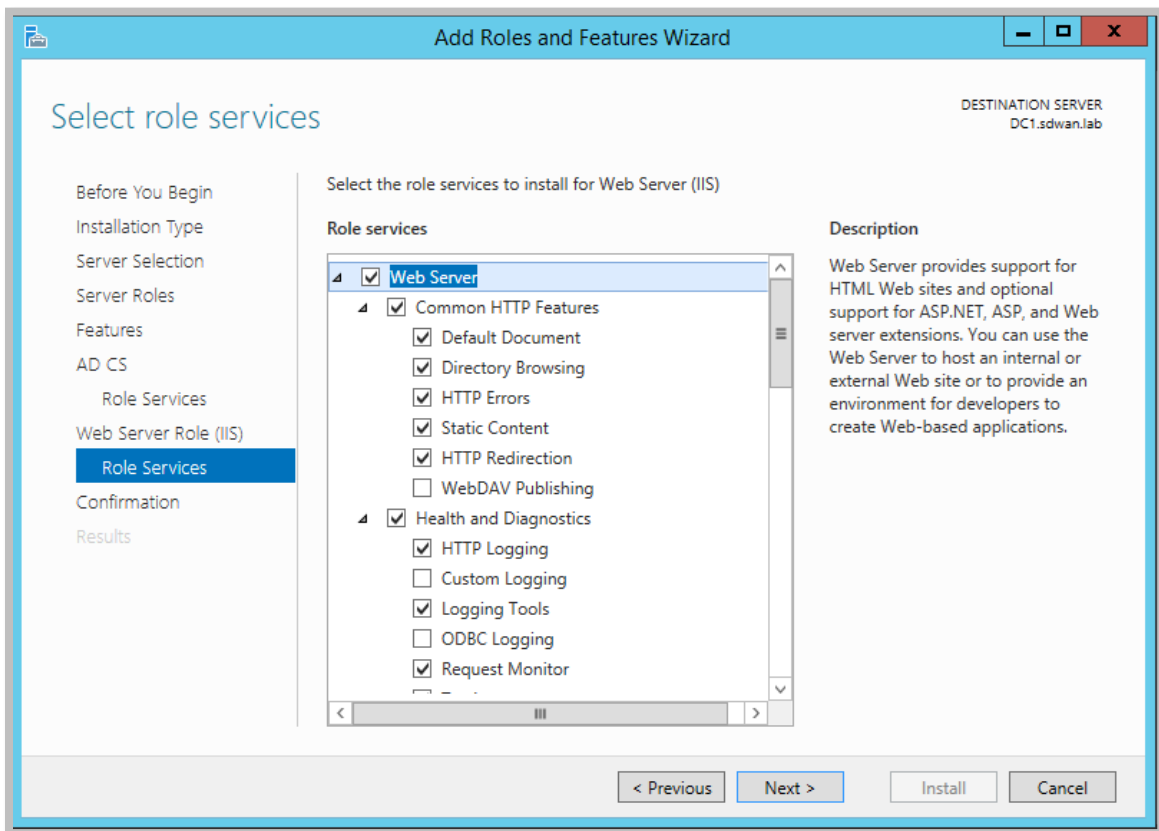
1. Base Steps 9-12 Select **Next**
2. on **Server Roles** page, Select **Active Directory Certificate Server**
3. Then select **Add Features**



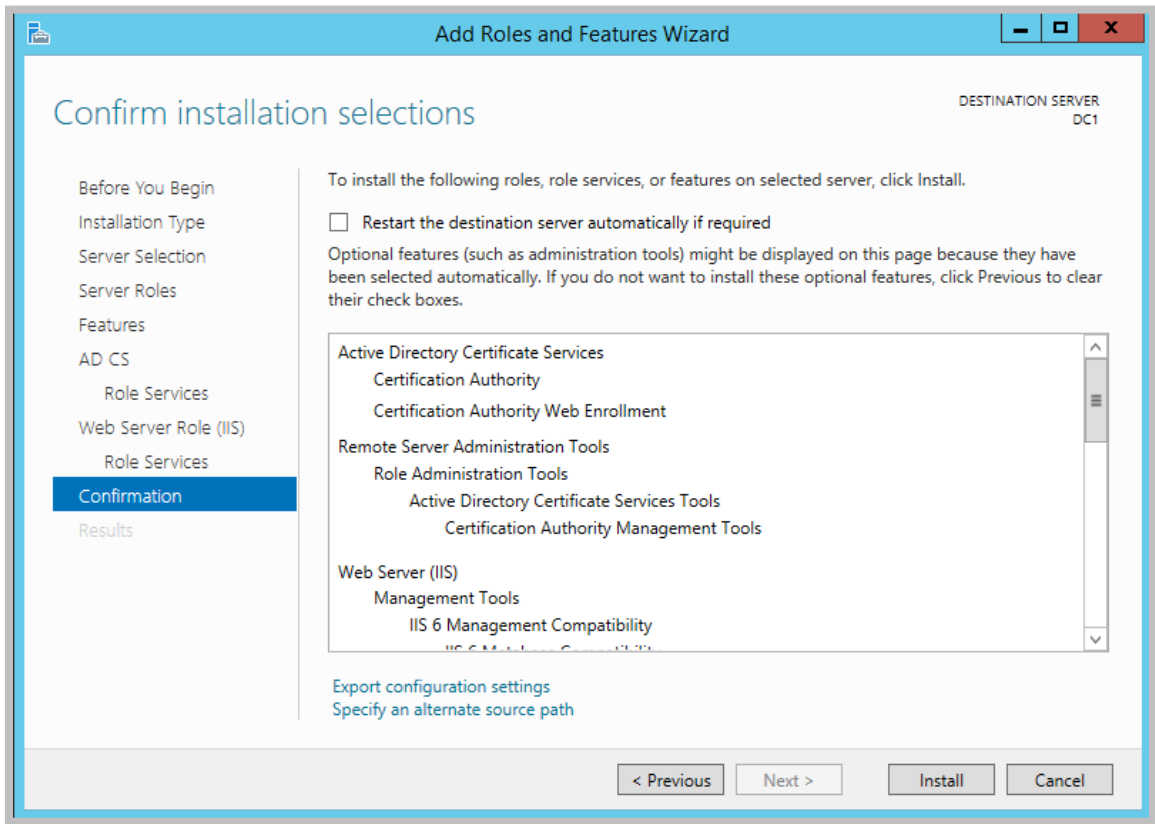
4. Select **Next** on **Features** page
5. On AD CS Role Services page, select **Certificate Authority Web Enrollment**, then select **Add Features**



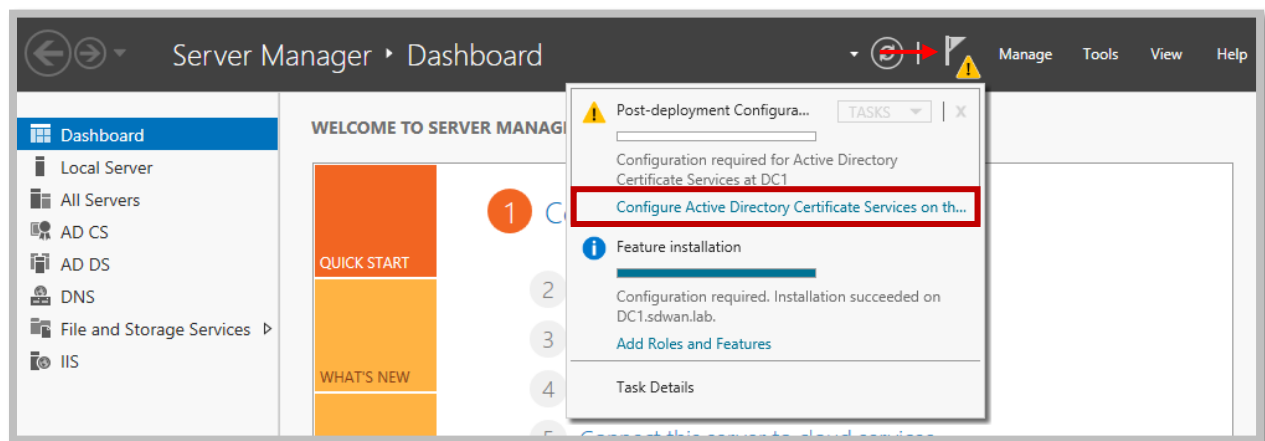
6. Select Next on Web Server Rolle(IIS) and Role Services



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

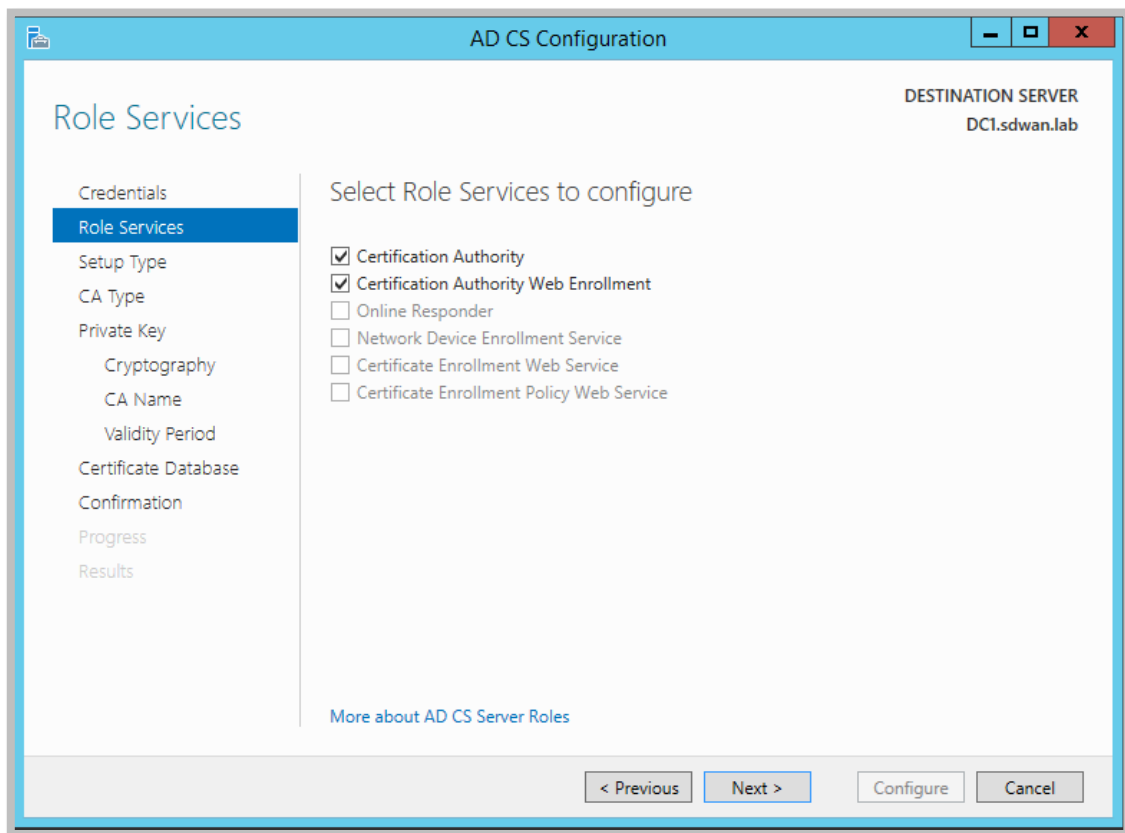


8. Select Notification, then select **Configure Active Directory Certificate Service** on th..

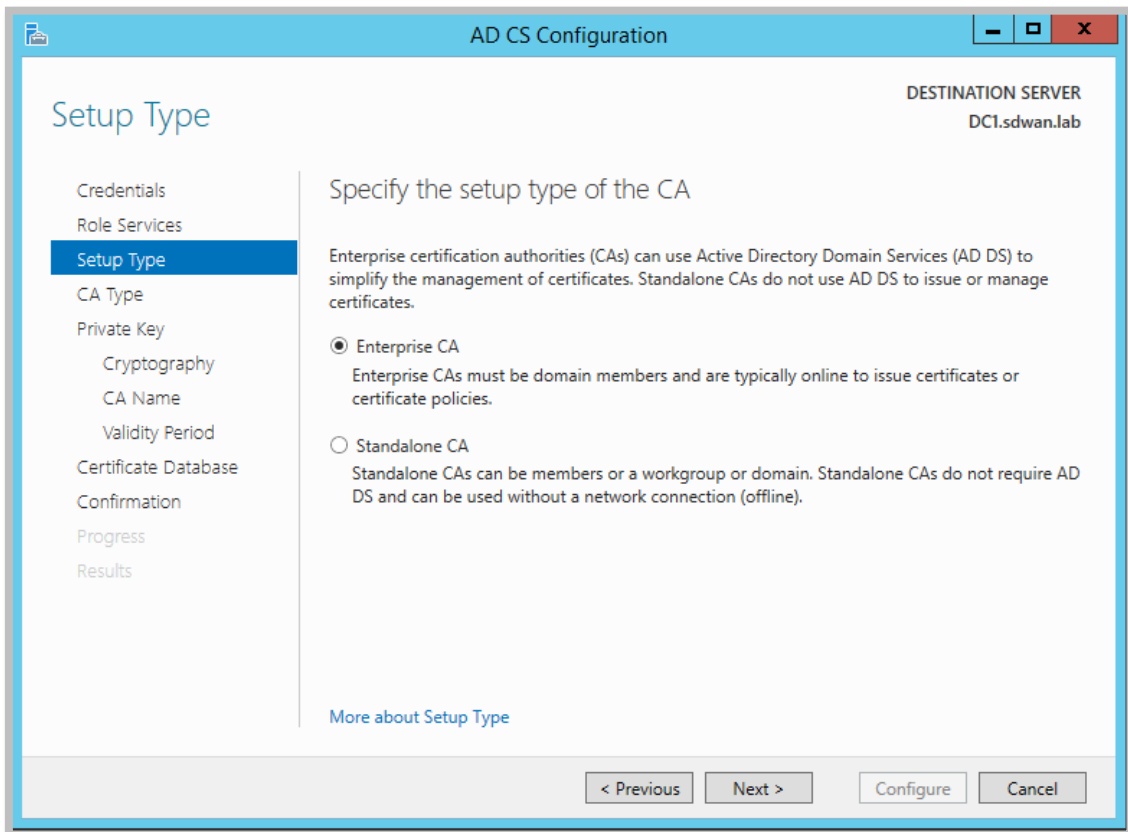


9. On **Credential** page Click **Next**

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**

The screenshot shows the 'AD CS Configuration' window with the 'CA Type' page selected in the left-hand navigation pane. The 'DESTINATION SERVER' is listed as 'DC1.sdwan.lab'. The main content area is titled 'Specify the type of the CA' and includes a descriptive paragraph about PKI hierarchies. Two radio buttons are present: 'Root CA' (which is selected) and 'Subordinate CA'. Below each radio button is a brief explanation of its function. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
DC1.sdwan.lab

CA Type

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ **Root CA**
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ **Subordinate CA**
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

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

The screenshot shows the 'AD CS Configuration' window with the 'Private Key' page selected in the left-hand navigation pane. The 'DESTINATION SERVER' is listed as 'DC1.sdwan.lab'. The main content area is titled 'Specify the type of the private key' and includes a descriptive paragraph about the need for a private key. Three radio buttons are present: 'Create a new private key' (which is selected), 'Use existing private key', and 'Select a certificate and use its associated private key'. Below each radio button is a brief explanation of its function. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
DC1.sdwan.lab

Private Key

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ **Create a new private key**
Use this option if you do not have a private key or want to create a new private key.

☐ **Use existing private key**
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

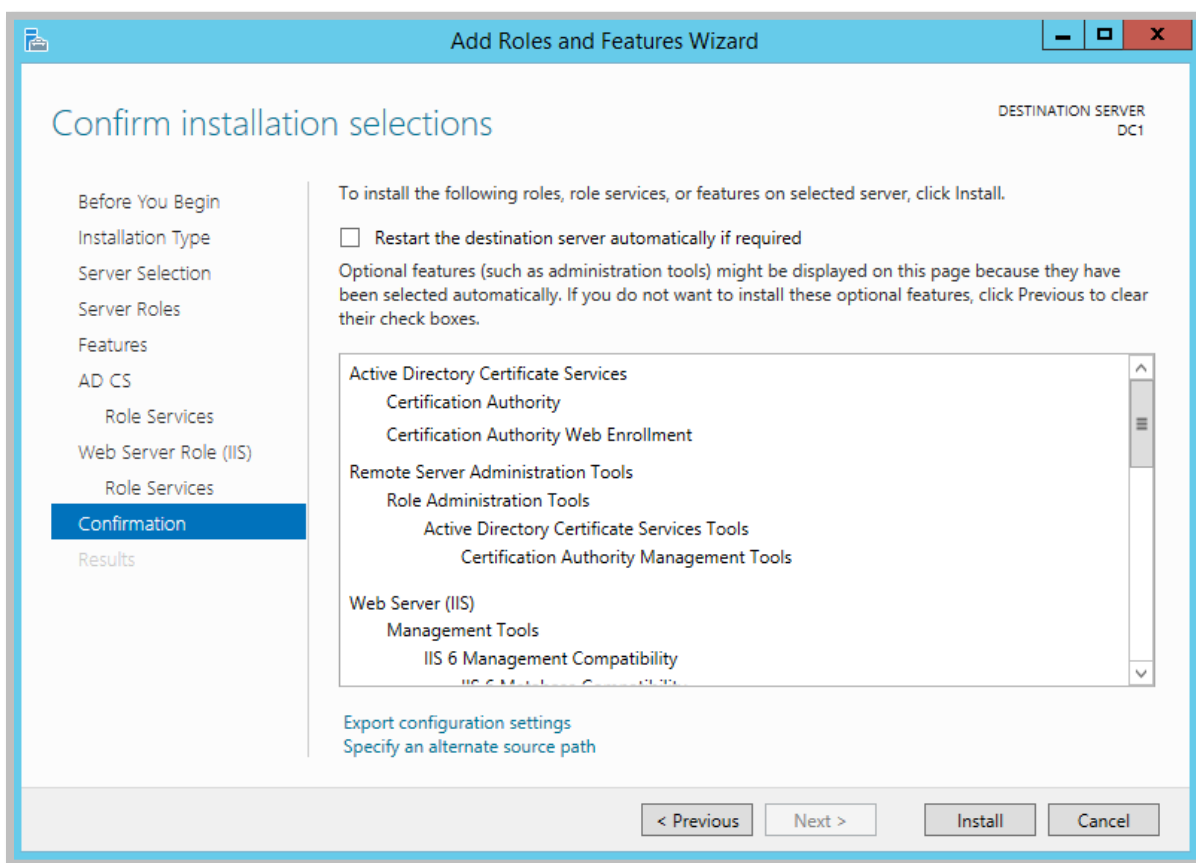
☐ **Select a certificate and use its associated private key**
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ **Select an existing private key on this computer**
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

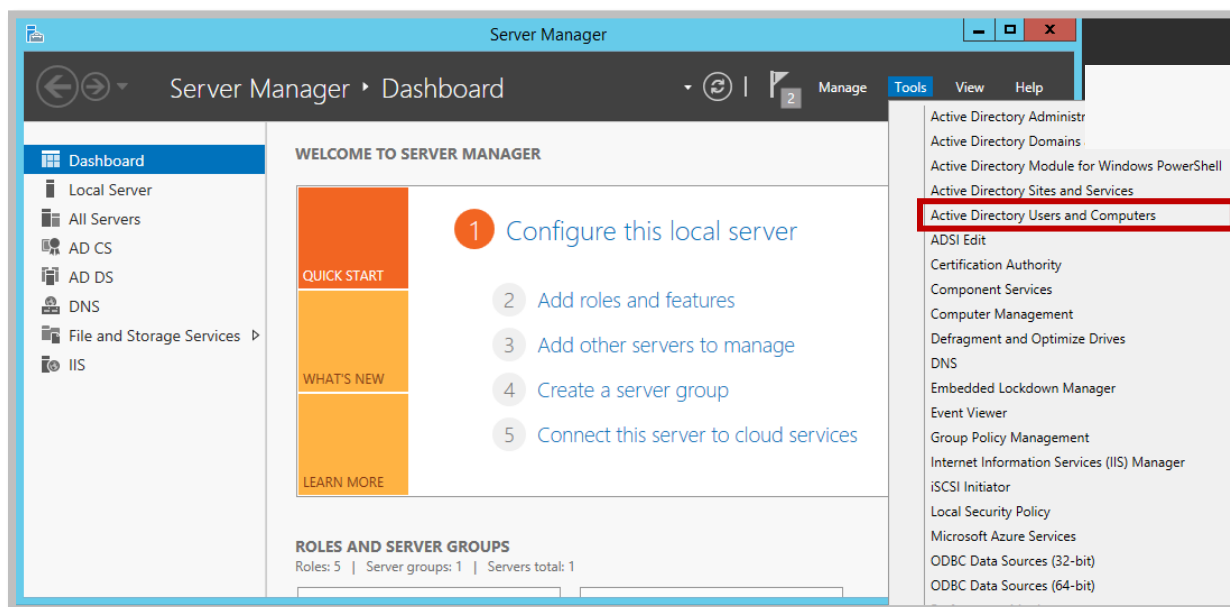
[More about Private Key](#)

< Previous Next > Configure Cancel

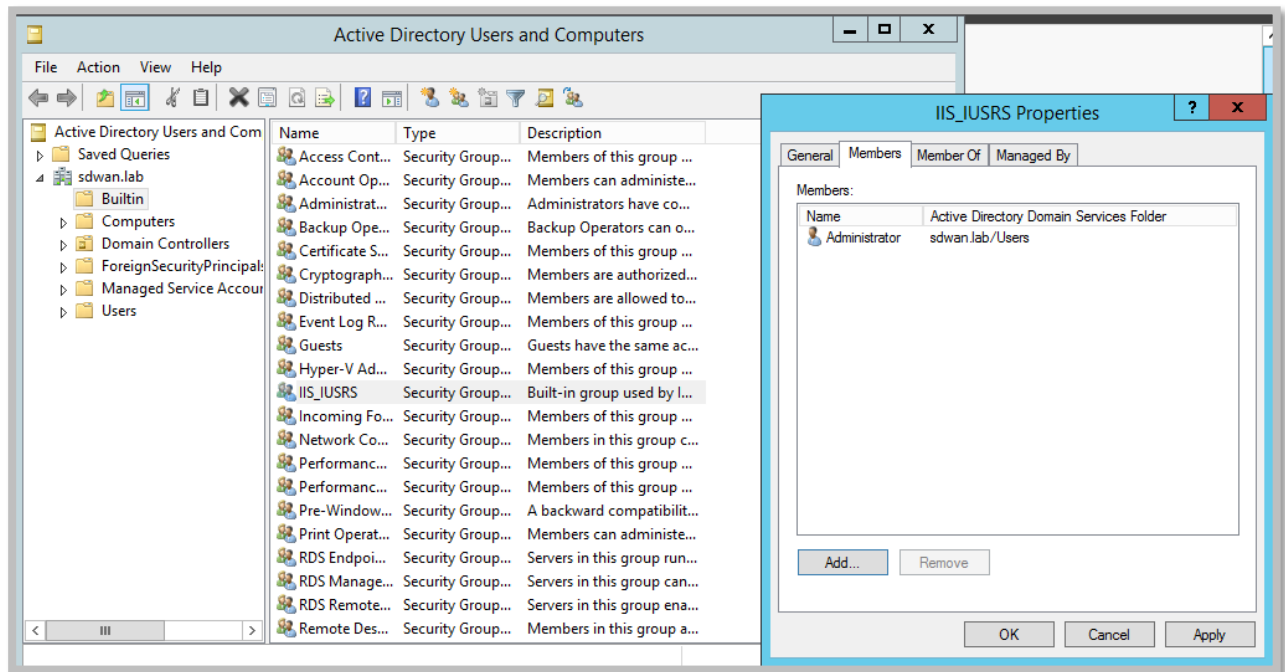
14. On **Cryptography** Select **Next**
15. On **CA name** page, Select **Next (Nothing Change)**
16. On **Validity Period** page select **Next**
17. On **Certificate Database** page select **Next**
18. On **Confirmation** page Click next an **configure**



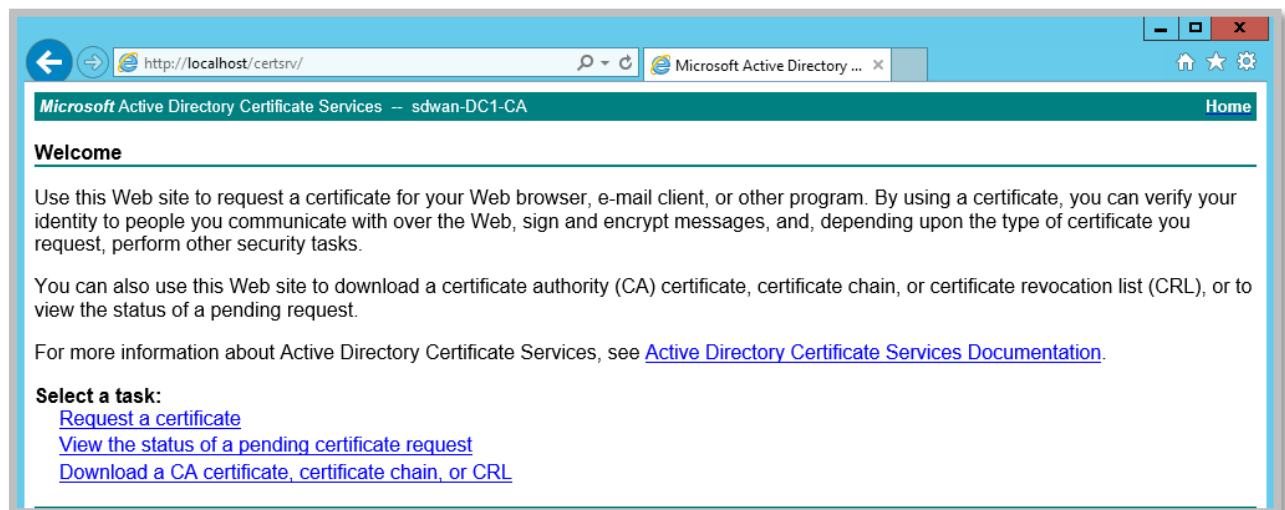
19. Before Get Certificate go to **Active Directory user and Services**



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



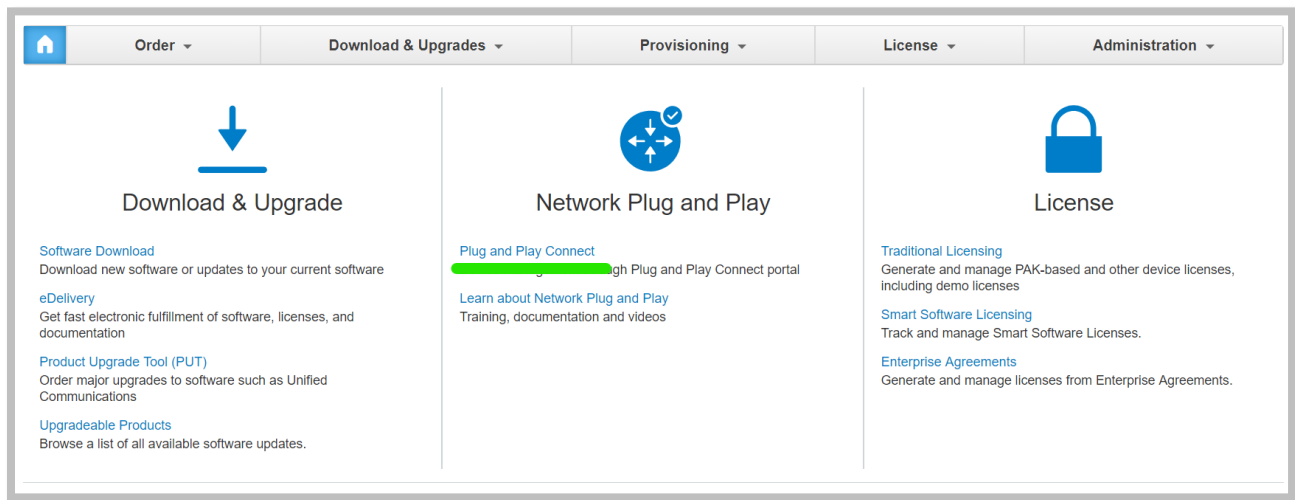
21. Browse URL <http://localhost/certsrv> to check page loaded correctly



Cisco Smart Account

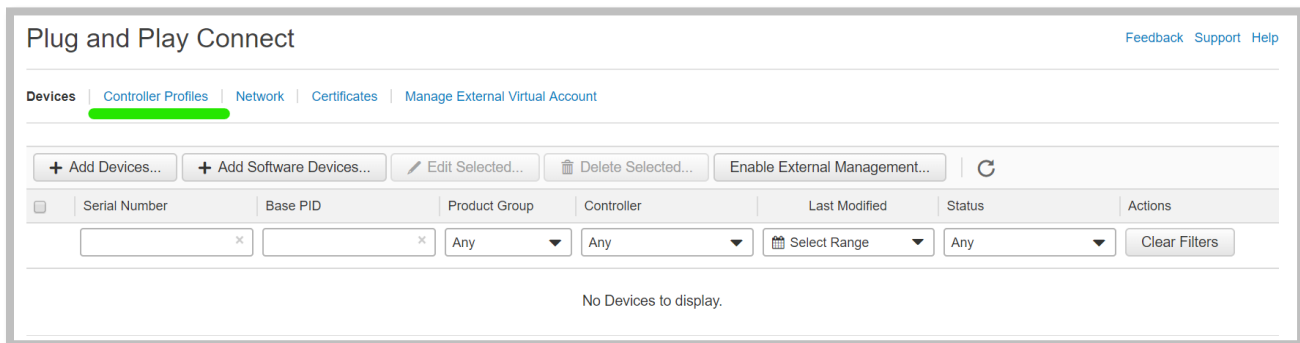
Login Smart Account

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

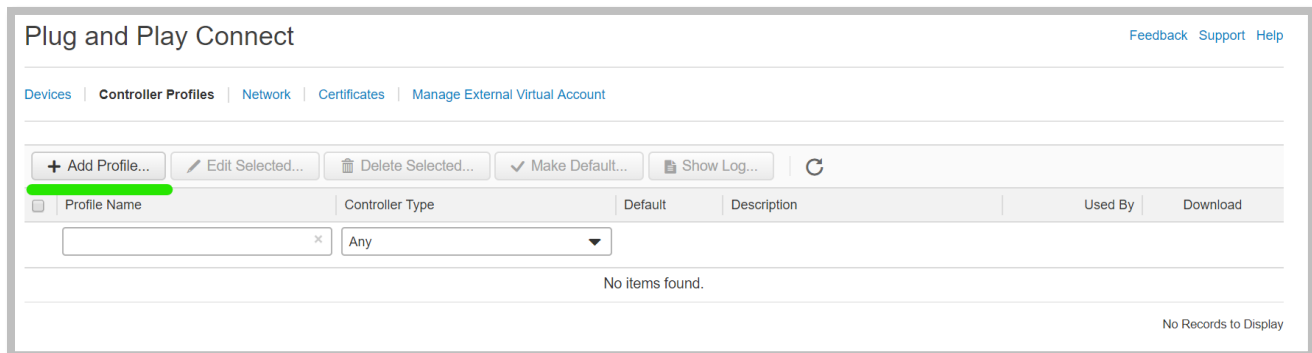


Add Controller Profile

- 4- Select **Controller Profiles**.



- 5- Select **Add Profile**.



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

Add Controller Profile

STEP 1
Profile Type

Conditional Steps

Choose the type of Profile to be created:

* Controller Type: VBOND

Cancel Next

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

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

Add Controller Profile

STEP 1 ✓
Profile Type

STEP 2
Profile Settings

STEP 3
Review

STEP 4
Confirmation

Profile Settings:

* Profile Name: SDWAN-LAB

Description: SD-WAN Training LAB in EVE-NG

Default Profile: Yes

Multi-Tenancy: No

* Organization Name: sdwanlab-webinar

* Primary Controller:

IPv4 DTLS:// 192.168.100.12 12346

Server Root CA: Max file size up to 1 MB or max characters not to exceed 1048576 Browse

Cancel Back Next

3- Select **Submit**.

Add Controller Profile

STEP 1 ✓
Profile Type

STEP 2 ✓
Profile Settings

STEP 3
Review

STEP 4
Confirmation

Review the following options to make sure they are correct before you Submit the changes.

Profile Type:

Controller Type: VBOND

Profile Settings:

Profile Name: SDWAN-LAB

Description: SD-WAN Training LAB in EVE-NG

Primary IPv4 Address: 192.168.100.12

Primary Protocol: dtls

Primary Port: 12346

Organization Name: sdwanlab-webinar

SP Organization Name:

Cancel

Back

Submit

4- Select **Done**.

Add Controller Profile

STEP 1 ✓
Profile Type

STEP 2 ✓
Profile Settings

STEP 3 ✓
Review

STEP 4
Confirmation

✓

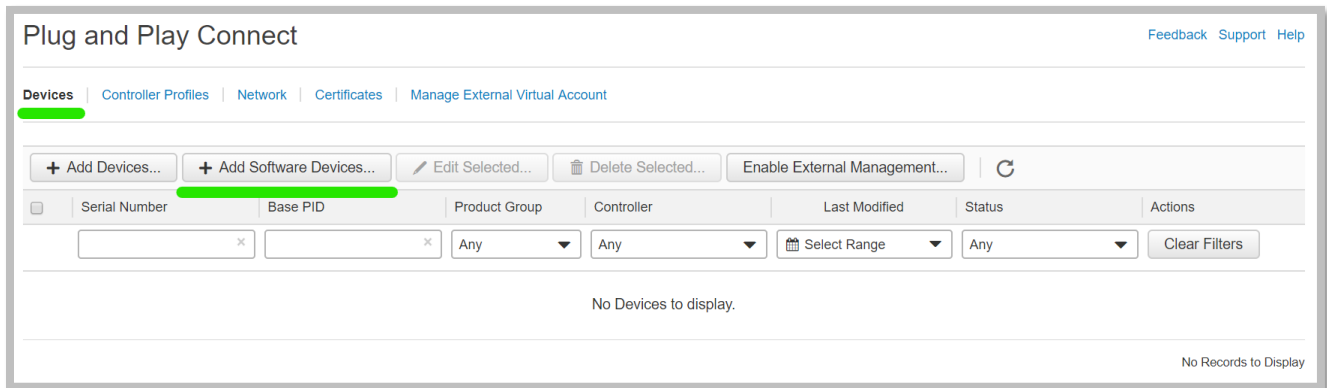
The controller profile "SDWAN-LAB" was successfully created.

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**.



Plug and Play Connect

Feedback Support Help

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account

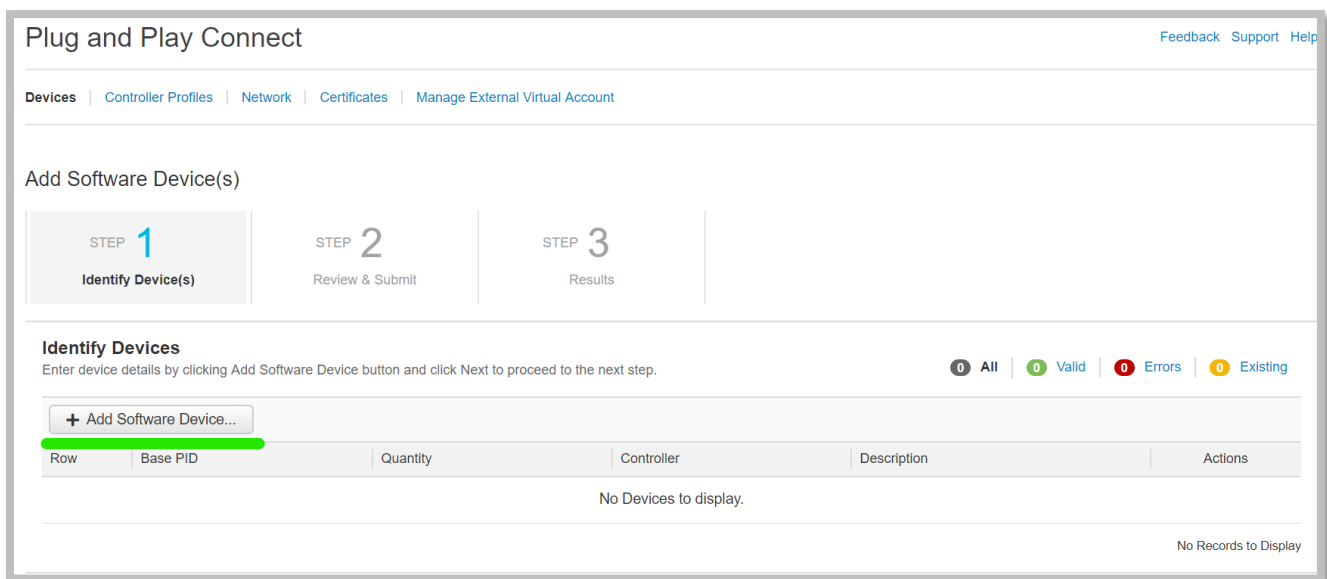
+ Add Devices... + Add Software Devices... Edit Selected... Delete Selected... Enable External Management... Refresh

Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
		Any	Any	Select Range	Any	Clear Filters

No Devices to display.

No Records to Display

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



Plug and Play Connect

Feedback Support Help

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account

Add Software Device(s)

STEP 1 Identify Device(s) | STEP 2 Review & Submit | STEP 3 Results

Identify Devices

Enter device details by clicking Add Software Device button and click Next to proceed to the next step.

All 0 Valid 0 Errors 0 Existing

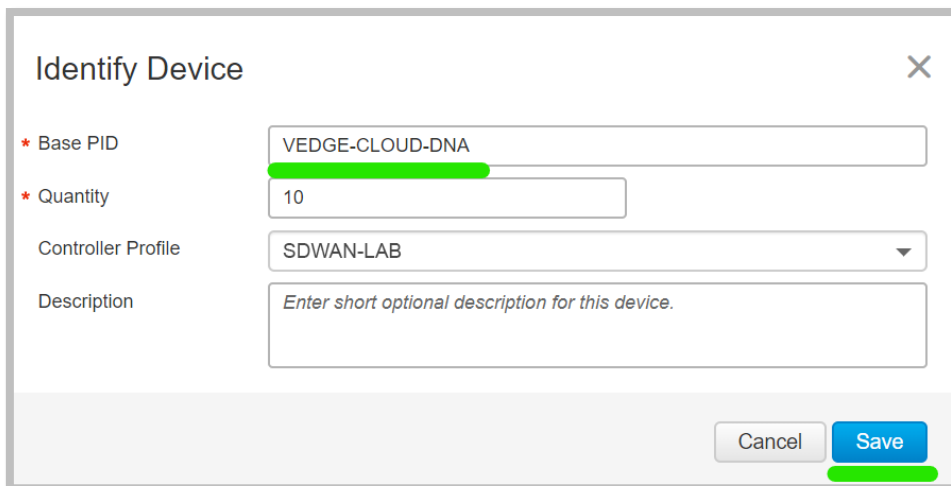
+ Add Software Device...

Row	Base PID	Quantity	Controller	Description	Actions

No Devices to display.

No Records to Display

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



Identify Device

* Base PID VEDGE-CLOUD-DNA

* Quantity 10

Controller Profile SDWAN-LAB

Description Enter short optional description for this device.

Cancel Save

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

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

Identify Device

★ Base PID

CSR1KV

★ Quantity

10

Controller Profile

SDWAN-LAB

Description

Enter short optional description for this device.

Cancel

Save

6- Select **Next**.

Plug and Play Connect

Feedback Support Help

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account

Add Software Device(s)

STEP 1
Identify Device(s)

STEP 2
Review & Submit

STEP 3
Results

Identify Devices

Enter device details by clicking Add Software Device button and click Next to proceed to the next step.

1 All | 1 Valid | 0 Errors | 0 Existing

+ Add Software Device...

Row	Base PID	Quantity	Controller	Description	Actions
1	VEDGE-CLOUD-DNA	10	SDWAN-LAB	--	
2	CSR1KV	10	SDWAN-LAB	--	

Showing 2 Record

Cancel

Next

7- Select **Submit**.

Plug and Play Connect

[Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | [Certificates](#) | [Manage External Virtual Account](#)

Add Software Device(s)

STEP 1 ✓
Identify Device(s)

STEP 2
Review & Submit

STEP 3
Results

Review & Submit
Submit action will submit following 1 newly identified device(s).

Row	Base PID	Quantity	Controller	Description
1	VEDGE-CLOUD-DNA	10	SDWAN-LAB	--
2	CSR1KV	10	SDWAN-LAB	--

Showing 2 Record

Cancel

Back

Submit

8- Select **Done**.

Plug and Play Connect

[Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | [Certificates](#) | [Manage External Virtual Account](#)

Add Software Device(s)

STEP 1 ✓
Identify Device(s)

STEP 2 ✓
Review & Submit

STEP 3
Results

Attempted to add 1 device(s)

i

Add Devices request is recorded!
Your request will be processed in background and an email will be sent to [redacted] once process is completed.

Done

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

Plug and Play Connect

[Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | [Certificates](#) | [Manage External Virtual Account](#)

+ Add Devices...

+ Add Software Devices...

Edit Selected...

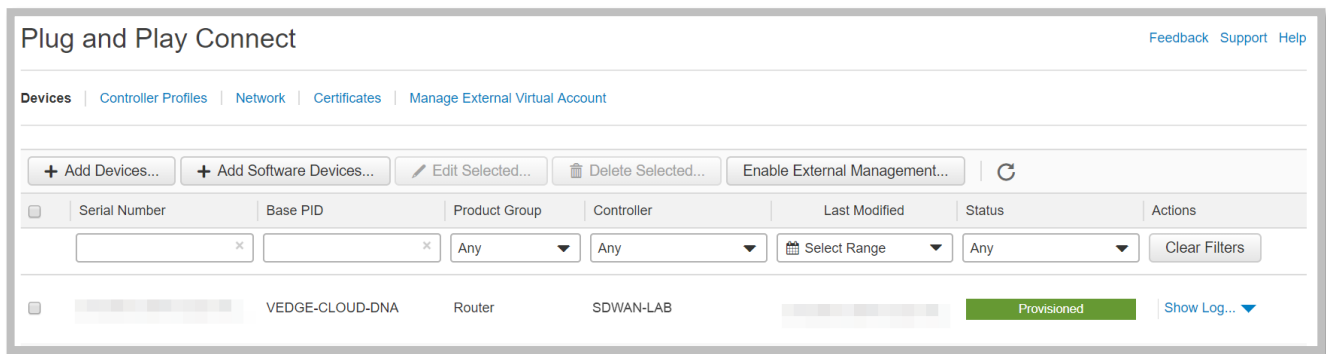
Delete Selected...

Enable External Management...

↺

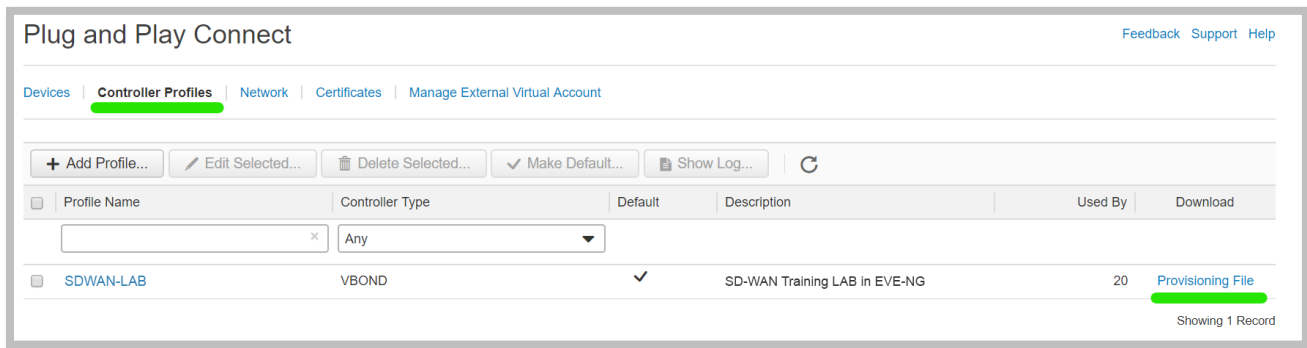
☐	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
☐			Any	Any	Select Range	Any	Clear Filters
☐	CSR1KV	Router	SDWAN-LAB			Pending for publish	Show Log...

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

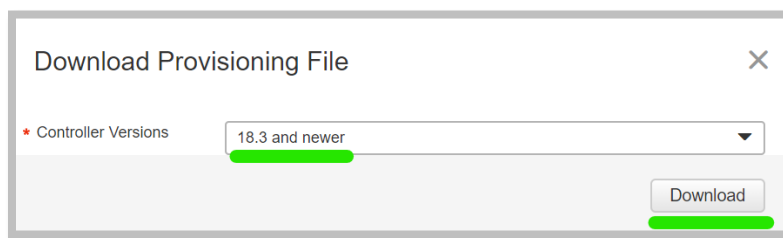


Serial File

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**

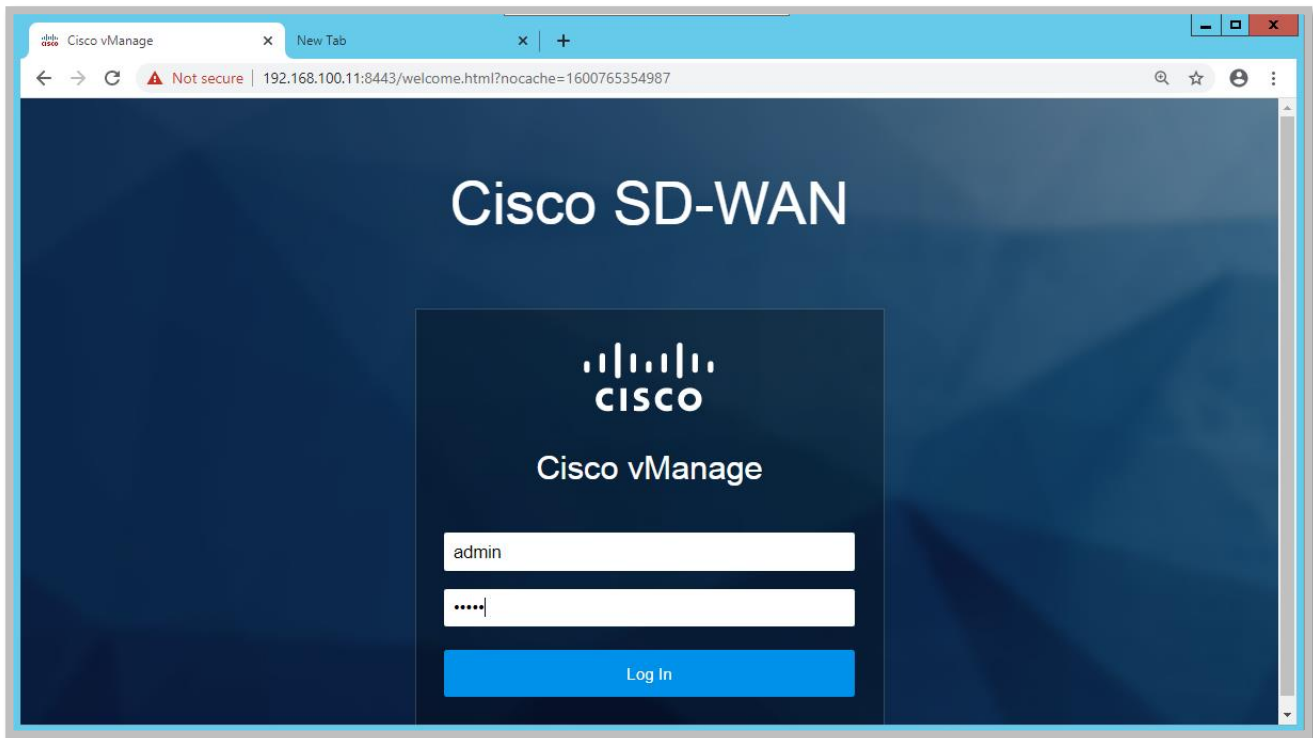
```
vmanage login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
Available storage devices:
hdb 100GB
1) hdb
Select storage device to use: 1
Would you like to format hdb? (y/n): y
```

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

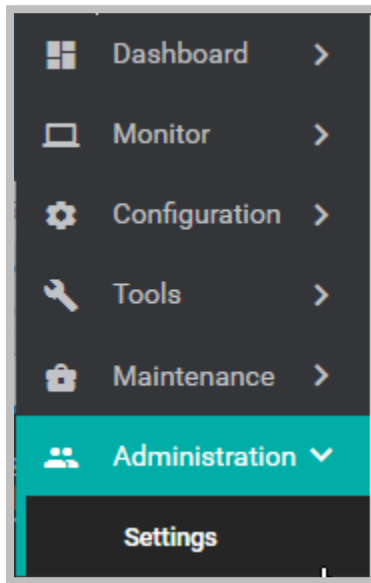
```
config
system
system-ip 100.1.1.11
site-id 100
organization-name "sdwanlab-webinar"
clock timezone Asia/Tehran
vbond 192.168.100.12
!
ntp
server 172.16.32.10
version 4
prefer
exit

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



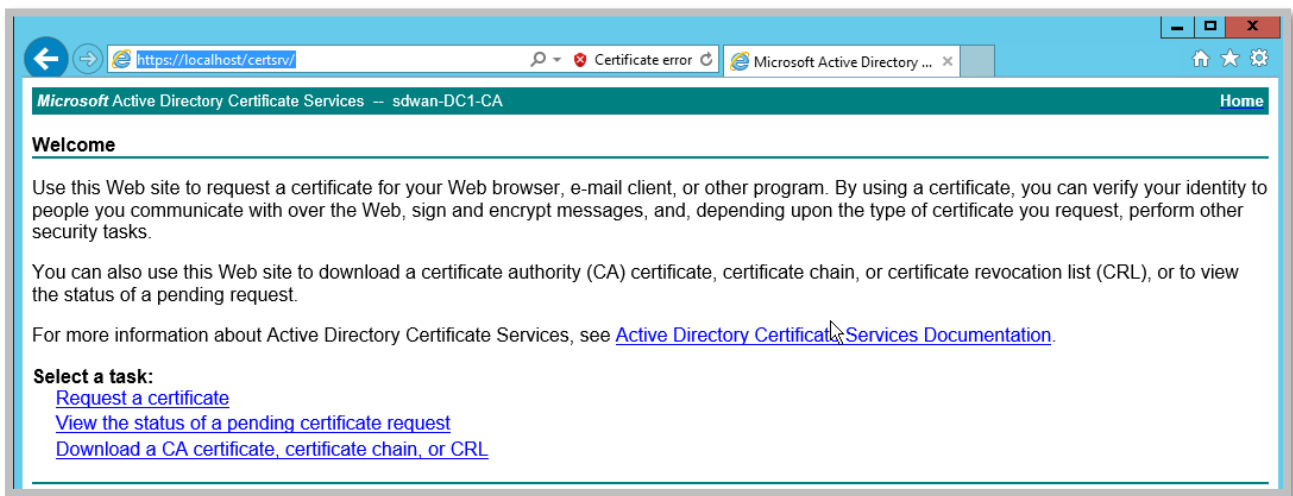
- 6- Go to **Administration/Setting** in vManage menu



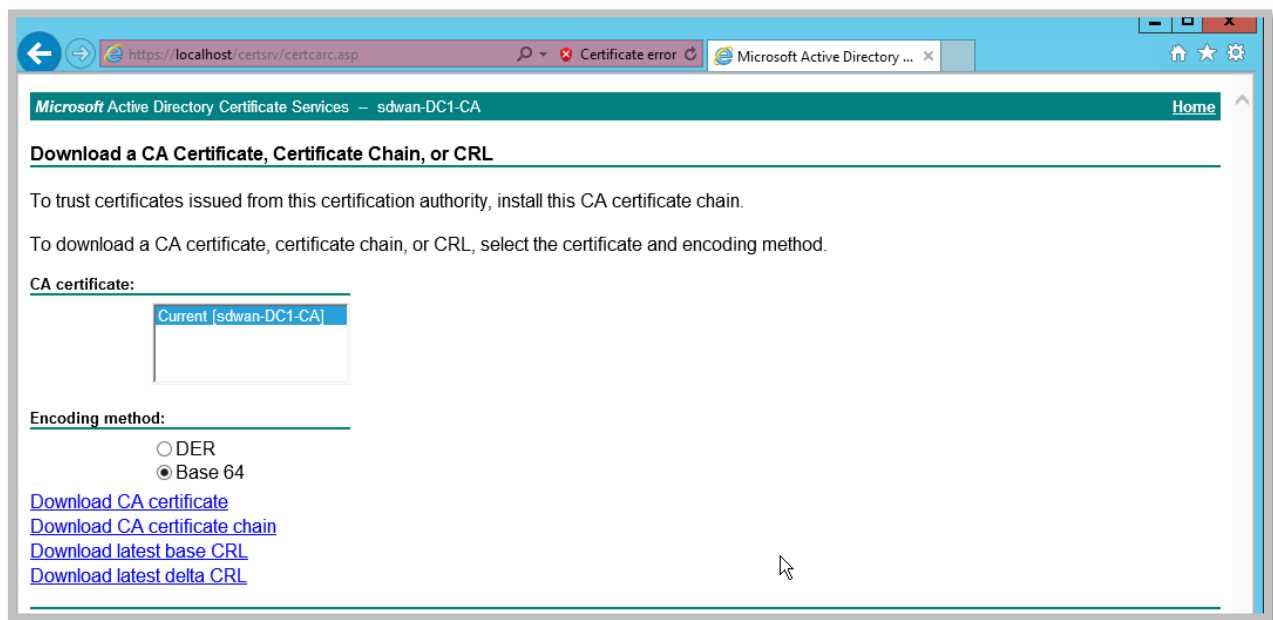
- 7- Change **Organization name and vBond IP address**

Organization Name	sdwanlab-webinar
vBond	192.168.100.12 : 12346

- 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

Controller Certificate Authorization Enterprise

Certificate Signing by: ☐ Cisco Automated (Recommended) ☐ Symantec Automated ☐ Manual ☒ Enterprise Root Certificate

Certificate Select a file

```
MTRaMEMxExARBgoJkiaJk/IsZAEZFgNsYWwxFtATBgoJkiaJk/IsZAEZFgVzZhdh
bJEVMBMGAT1UEAxMMc2R3YW4tREMxLUNBMiBjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBKgKCAQEAwTQn0SC2YtYowTFWBjkdZUwj+cXepIK+tpamIKeChRsYjHGdY1xR
mVmnwnt6PNZgLoL+FTbLz3G0c8DHPmGsn7WGGX0ascYnjdKzmjw2SeNYXNedf
PBWOCe6ZoxI2/VqwgGqGh7h47eQG3XNqF8JGMXzdV5VBwq8MaWVINpsg05xF3
Hq5PolpLc6pduTsVcW6SjZkMZojZQZ9ZIRHugBvsTuPiZU1gTJz5dE4MCW
FpHa96faDLws3WF1004LgLFxYzm1CHII/EFKneVc3Dg0TVI9CeaHPmQBnZVqF5Nr
aN4fwXt+UcBxUZUx6/GxMUcJCC2ryIMbEwIDAQABo1EwTzALBgnVNHQ8EBAMCAYYw
DwYDR0TAQH/BALUwAwEB/zAdBgNVHQ4EFgQUj7Dy+cUPUVzr1/D63NIK2/frelgw
EAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQADggEAL63PqRmQmxd3PXy
wY1syTmwAHV85QX6KcdNI9oZ5g8BJuFn7n/cTcoVd+dkghbCl2IGuVlPYQNd1S
wJKz17mAUFBW/Ko+JaDlyRurmXJKHEz3uYgvFU/6SITnaOejXnpY94tZ+EMHqHT
PV5L7IAzoBCvpjCHwLhtniCK3aVsgvCE043FW+u3egol2uZs3H7pBVx/Indee0o
FuL+fasxXA8ERAQniPygZM+yy5xriZWikupEGDUHdS1B5wOL98HgFu5Dwt+ENqr
9fNbpL7QJxnsTasqE7cEX1WyxQIFPIm9V+3/q8PGU+aaB9C5055MzTrQCGeJOG
3YyWxDbg=
-----END CERTIFICATE-----
```

☒ Set CSR Properties

Domain Name

Activate Windows
Go to System in Control Panel to activate Windows.

16- Mark **Set CSR properties**

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

☒ Set CSR Properties

Domain Name

sdwan.lab

Organizational Unit

sdwanlab-webinar

Secondary Organizational Unit

sdwanlab-webinar

Organization

vIPtela Inc

City

Org City

State

Org State

Email

m.rafati@sdwan.lab

2-Letter Country Code

US

Validity

1 Year

Exact Text Match

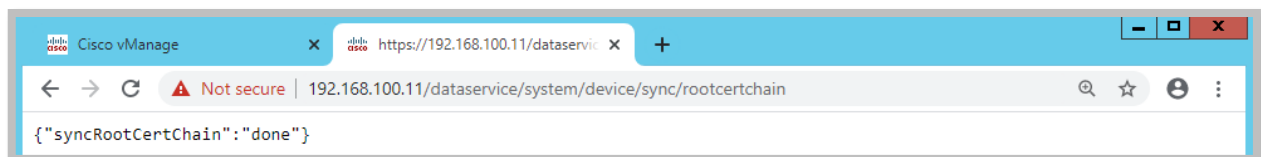
Base Your Organization

Import & Save Cancel

18- Click **import and Save**

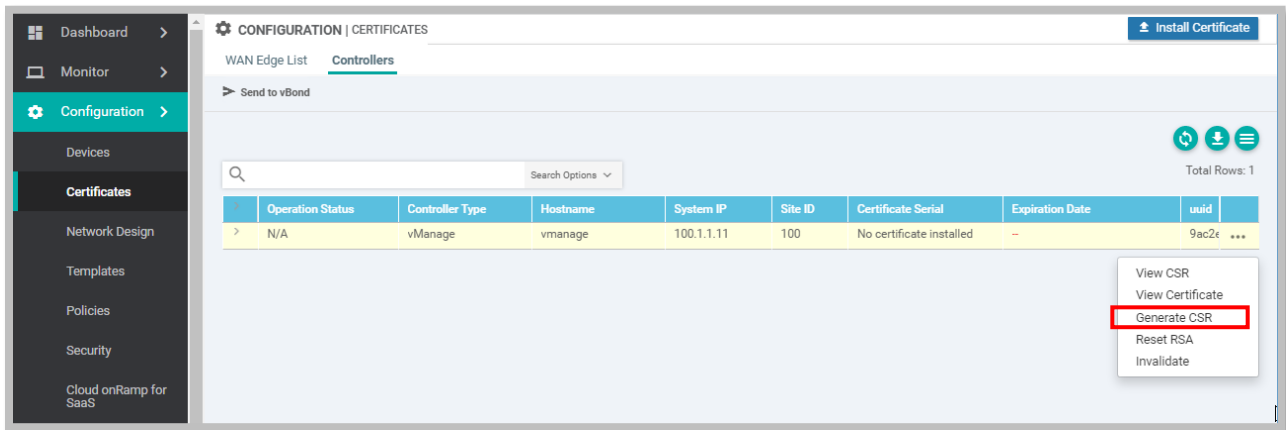
19- Open new browser tab, then enter

<https://192.168.100.11/dataservice/system/device/sync/rootcertchain>

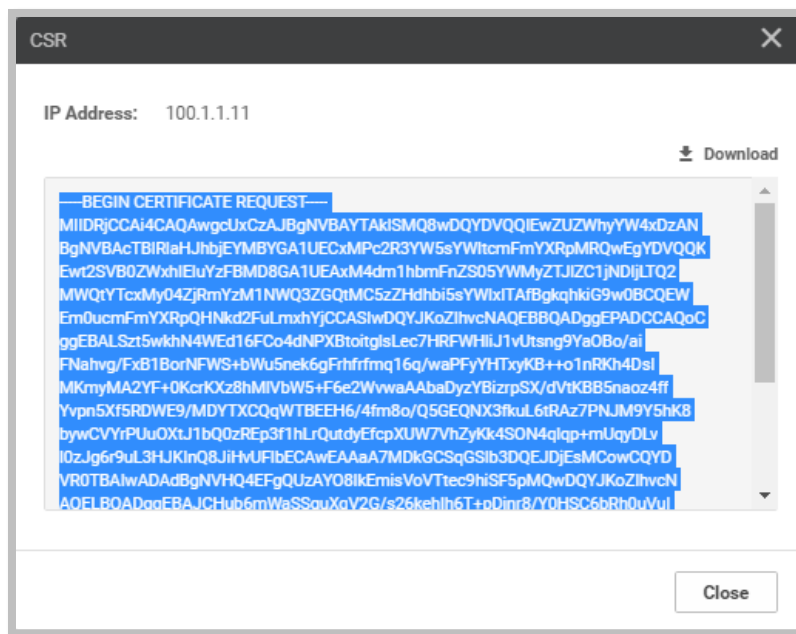


20- on vManage, select menu **Configuration->Certificate->Controllers**

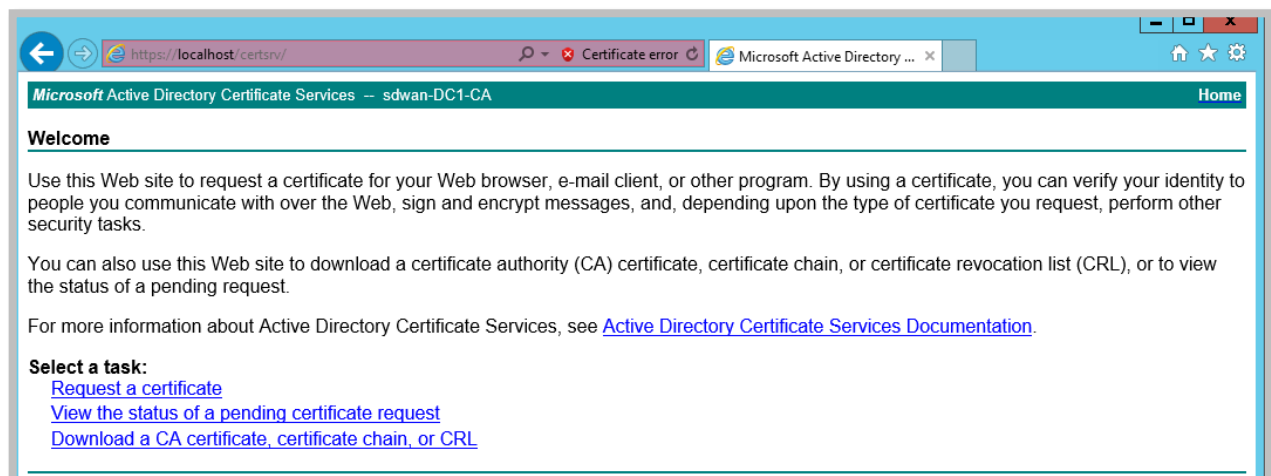
21- Click ... then select **generate CSR**



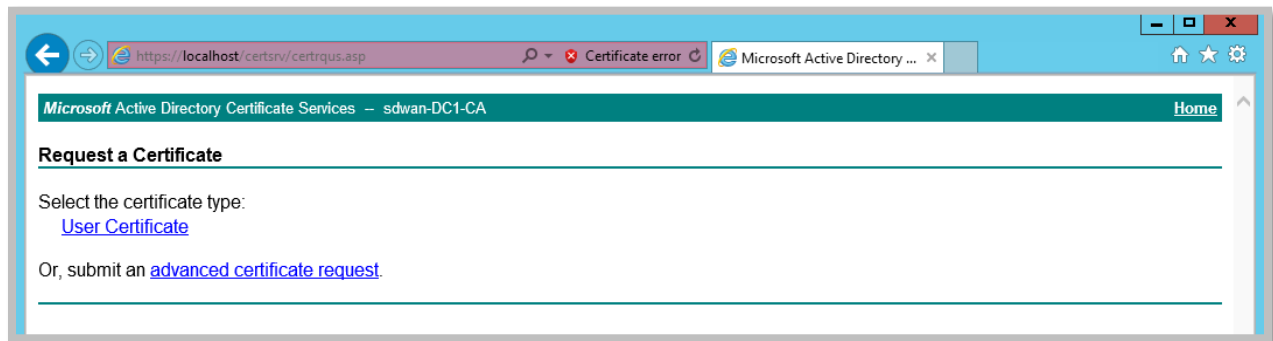
22- Copy PEM format of Certificate



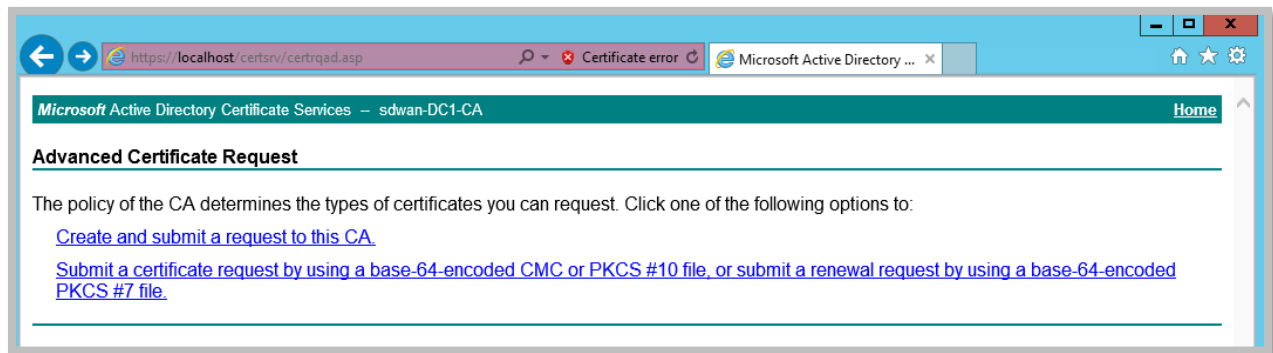
23- Open Certificate Authority web enrollment URL <http://localhost/certsrv>



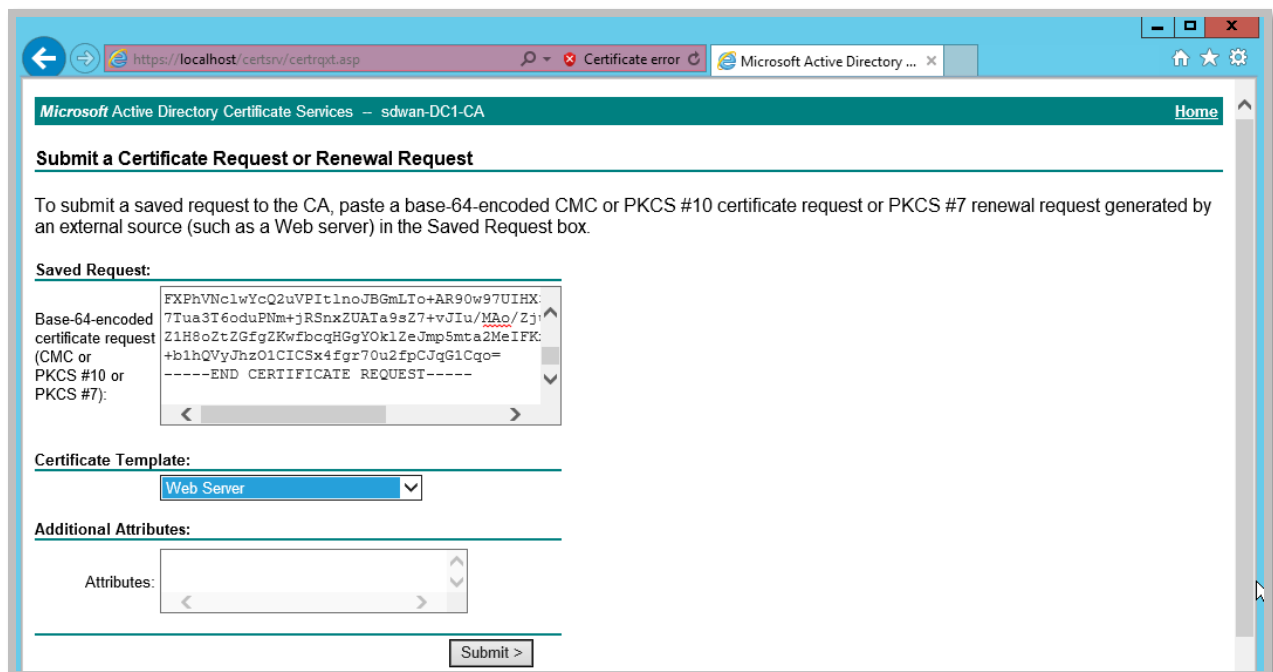
- 24- Click on **request a certificate**
- 25- Click **advance certificate request**



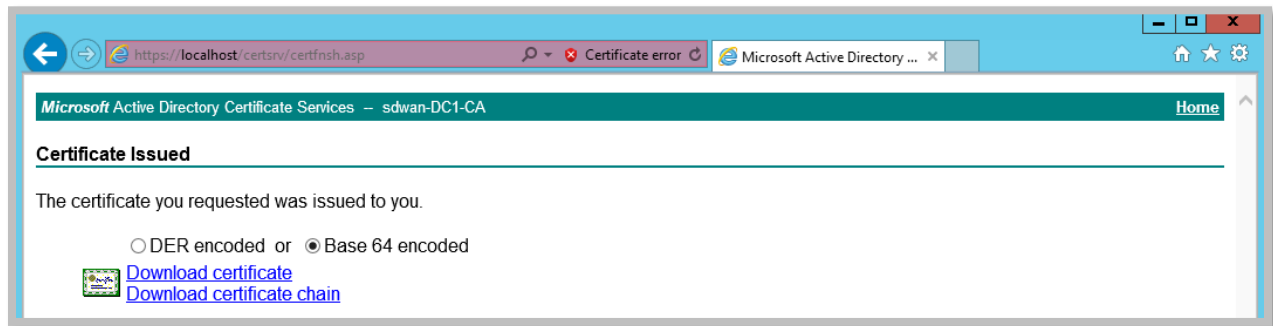
- 26- Select **submit a certificate request by**



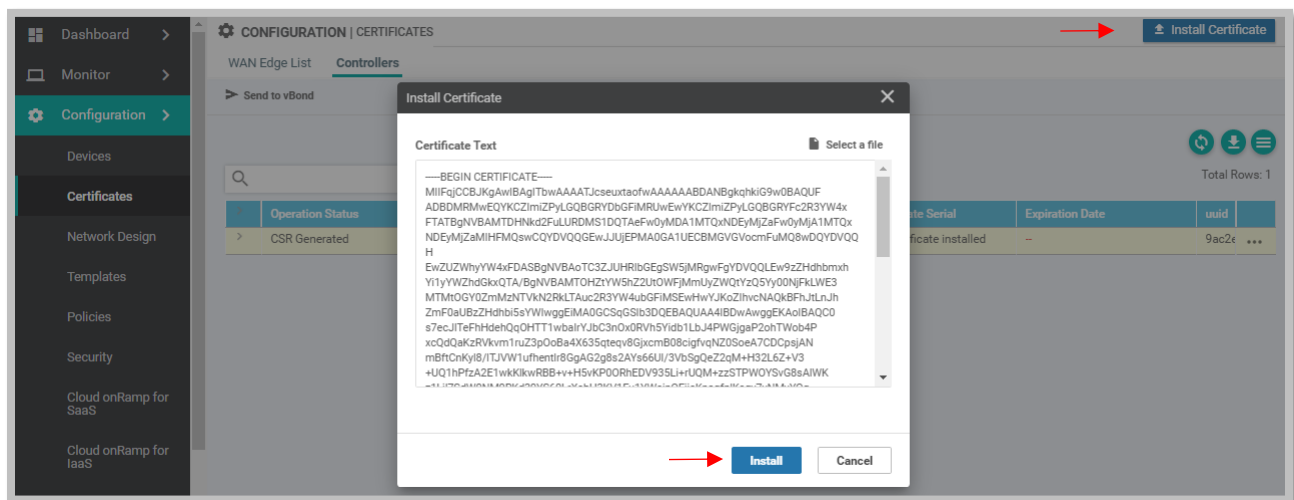
- 27- Paste CSR and select **certificate Template** Web Server the click **Submit**



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

	Status	Message	Device Type	Device ID	System IP	vManage IP
>	Success	Successfully synced vEdge l...	vManage	9ac2e2ed-c49c-461d-a713-...	100.1.1.11	100.1.1.11

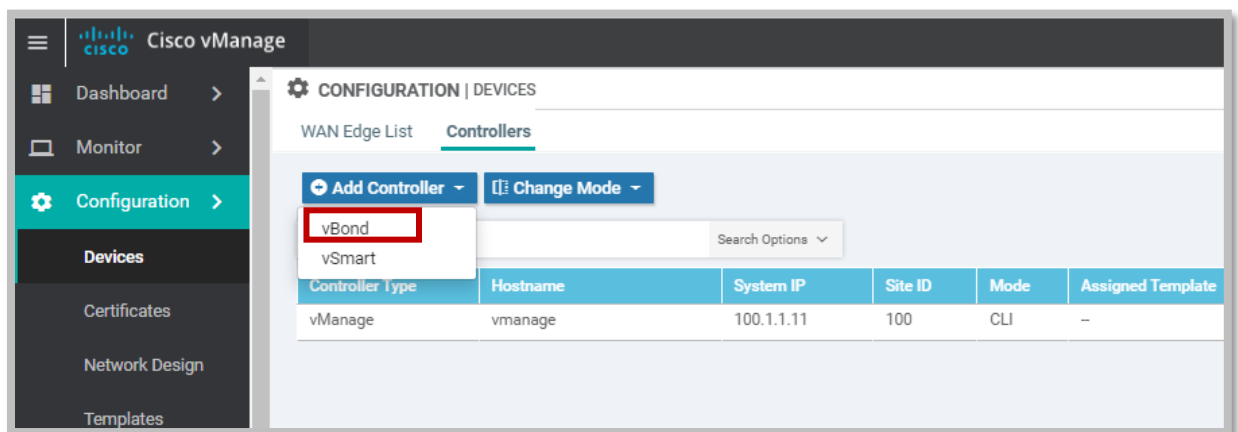
vBond

- 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**.

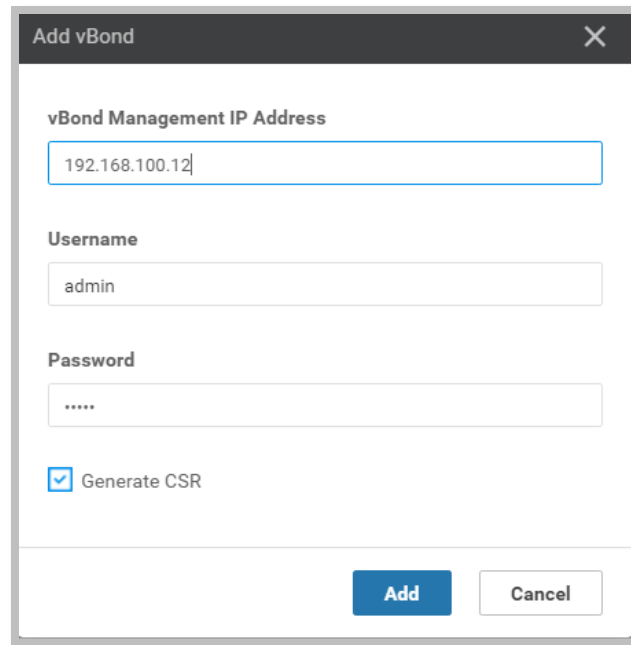
```
config
system
  system-ip 100.1.1.12
  site-id 100
  organization-name "sdwanlab-webinar"
  clock timezone Asia/Tehran
  vbond 192.168.100.12 local
!
ntp
  server 172.16.32.10
  version 4
  prefer
  exit

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



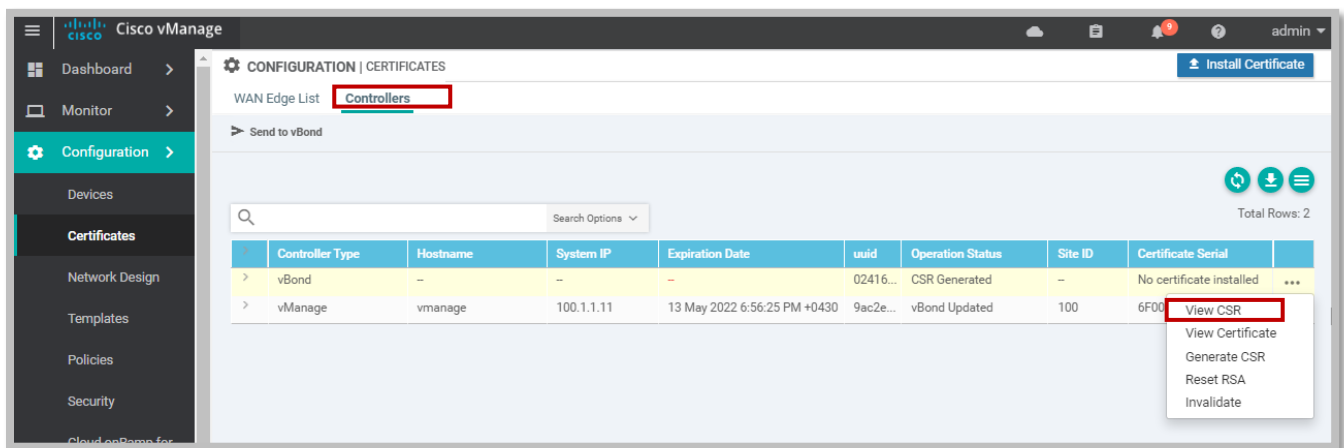
- 4- Enter the **vBond details** add click **Add**.



The 'Add vBond' dialog box contains the following fields and options:

- vBond Management IP Address:** 192.168.100.12
- Username:** admin
- Password:** (masked with dots)
- ☒ **Generate CSR**
- Buttons:** Add, Cancel

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



The screenshot shows the 'CONFIGURATION | CERTIFICATES' page in Cisco vManage. The 'Controllers' tab is selected. A table lists the vBond and vManage controllers. The vBond row shows 'CSR Generated' status. A context menu is open for the vBond row, with 'View CSR' highlighted.

	Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate Serial	
>	vBond	--	--	--	02416...	CSR Generated	--	No certificate installed	...
>	vManage	vmanage	100.1.1.11	13 May 2022 6:56:25 PM +0430	9ac2e...	vBond Updated	100	6F0...	View CSR View Certificate Generate CSR Reset RSA Invalidate

- 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

	Status	Message	Device Type	Device ID	System IP	vManage IP
>	Success	Successfully synced vEdge l...	vBond	02416bb3-45a2-4d5b-88a5-...	--	100.1.1.11

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

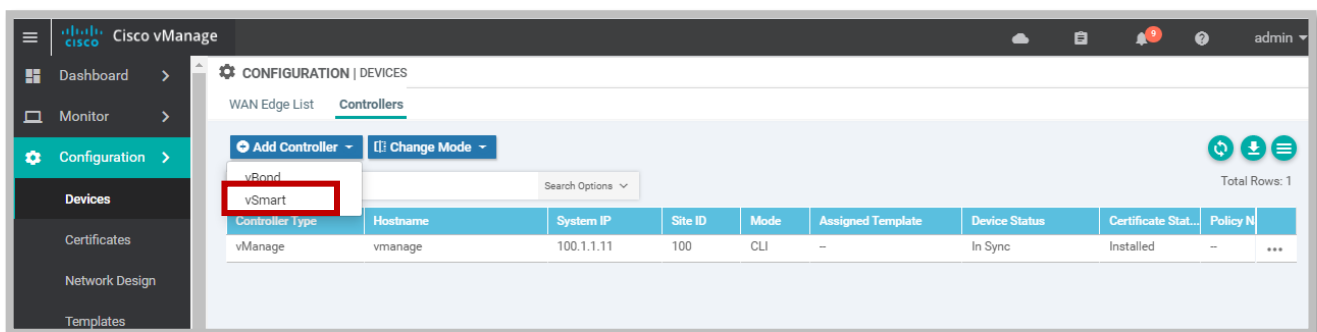
- 1- Once you see the message **System Ready** login with the **username/password admin** and apply the following **bootstrap config**.

```
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

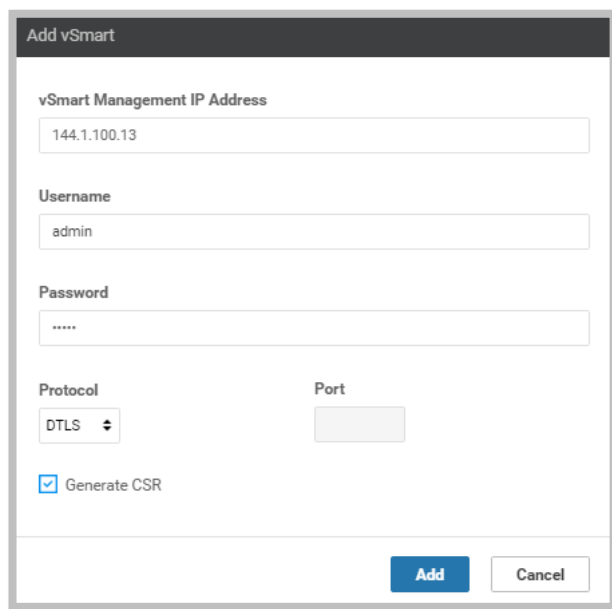
vpn 0
ip route 0.0.0.0/0 192.168.100.1
interface eth0
  no shut
  ip address 192.168.100.13/24

!
```

- 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.

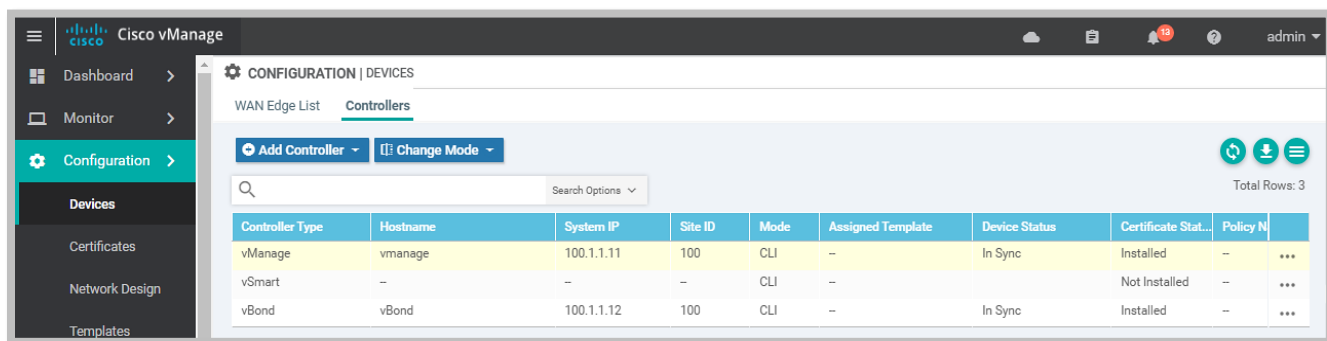


The 'Add vSmart' dialog box contains the following fields and options:

- vSmart Management IP Address:** 144.1.100.13
- Username:** admin
- Password:** (masked with dots)
- Protocol:** DTLS (dropdown menu)
- Port:** (empty text box)
- Generate CSR:** ☒
- Buttons:** Add, Cancel

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

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



The screenshot shows the 'CONFIGURATION | DEVICES' page in Cisco vManage. The 'Controllers' tab is selected, displaying a table of controllers.

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Certificate Stat...	Policy N
vManage	vmanage	100.1.1.11	100	CLI	--	In Sync	Installed	--
vSmart	--	--	--	CLI	--		Not Installed	--
vBond	vBond	100.1.1.12	100	CLI	--	In Sync	Installed	--

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



Status	Message	Device Type	Device ID	System IP	vManage IP
Success	Successfully synced vEdge l...	vSmart	688d430f-1792-48df-8c04-6...	--	100.1.1.11

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
```

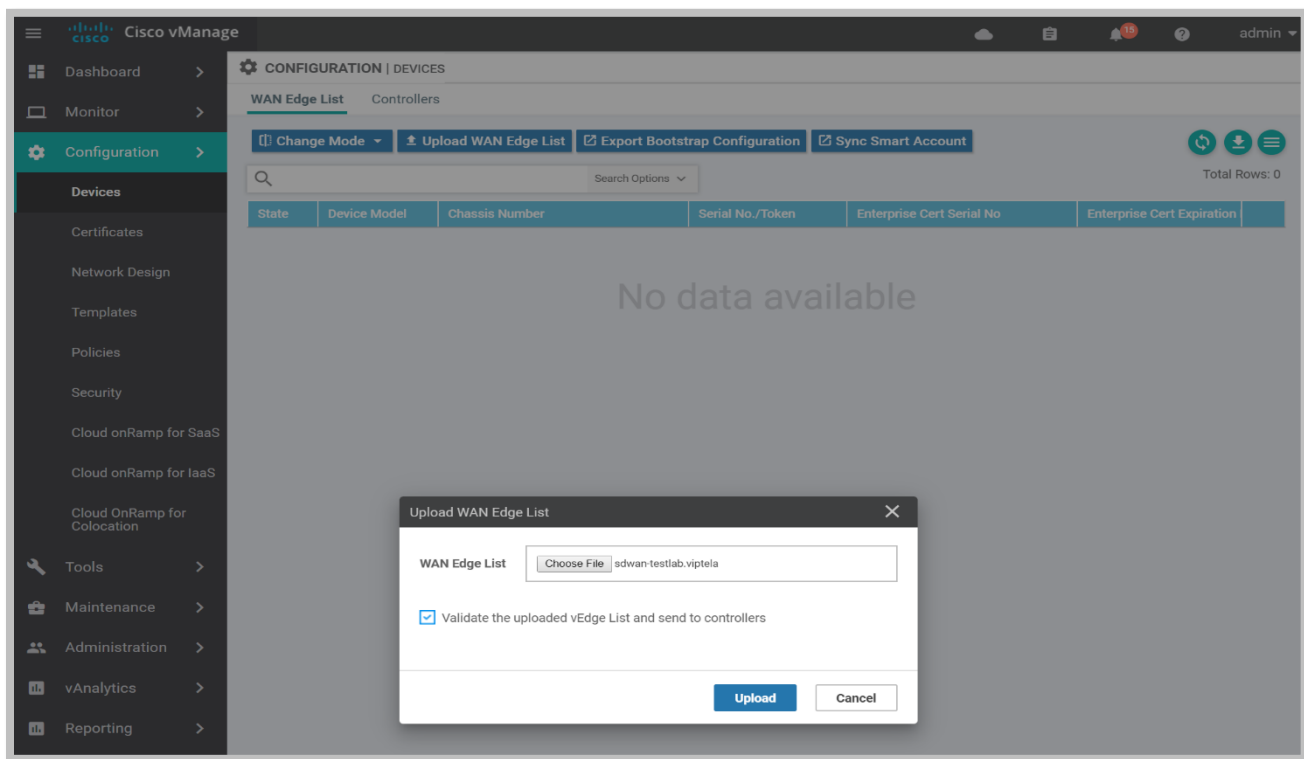
11- show connection in vSmart show control connections

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

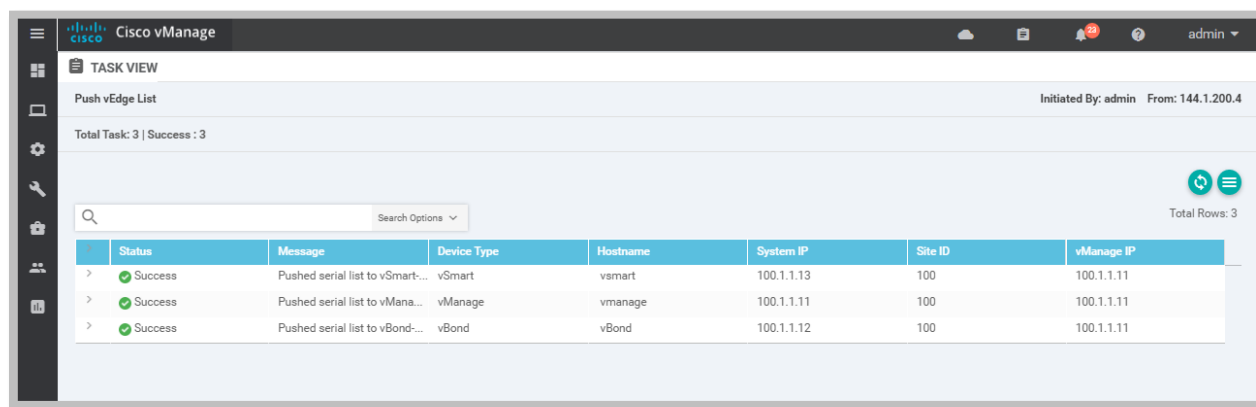
SD-WAN WAN Edges Configuration on EVE-NG

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



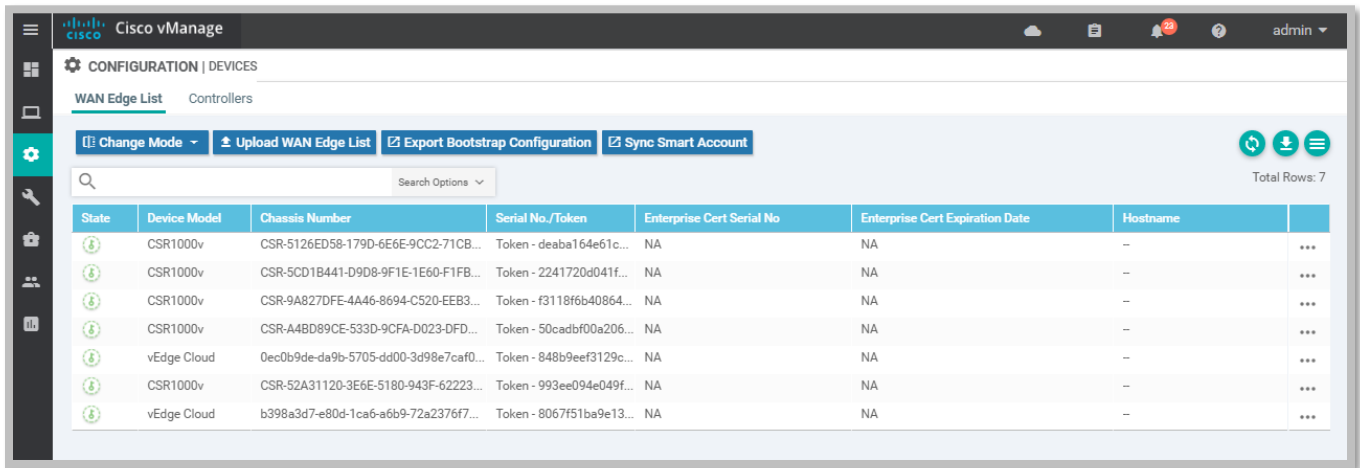
2- A success message looks similar to the below



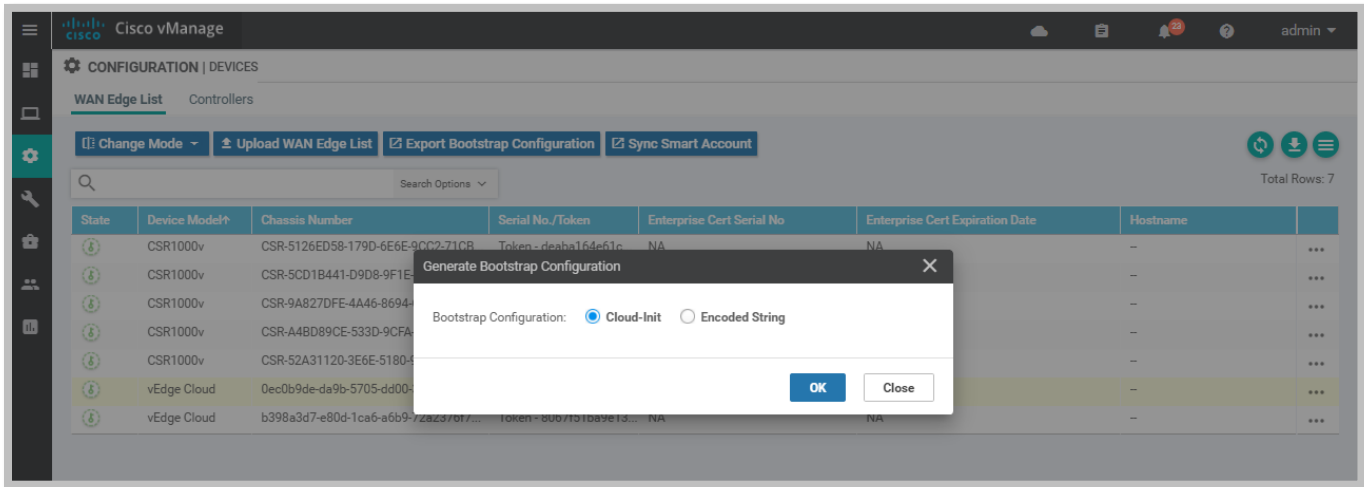
vEdge Cloud

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

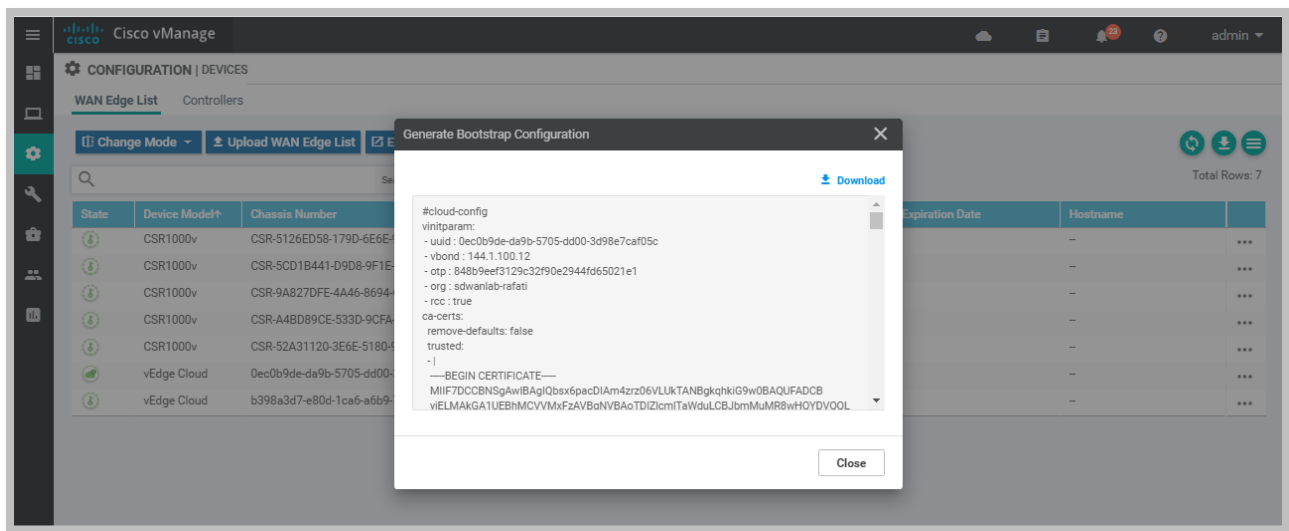
- 1- Configuration--> Devices--> WAN Edge List--> A vEdge Cloud--> ... --> Generate Bootstrap Configuration



- 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 [Filezilla](#) 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			SITE		DOMAIN		PEER		PEER		CONTROLLER			
TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	LOCAL	COLOR	PROXY	STATE	UPTIME	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

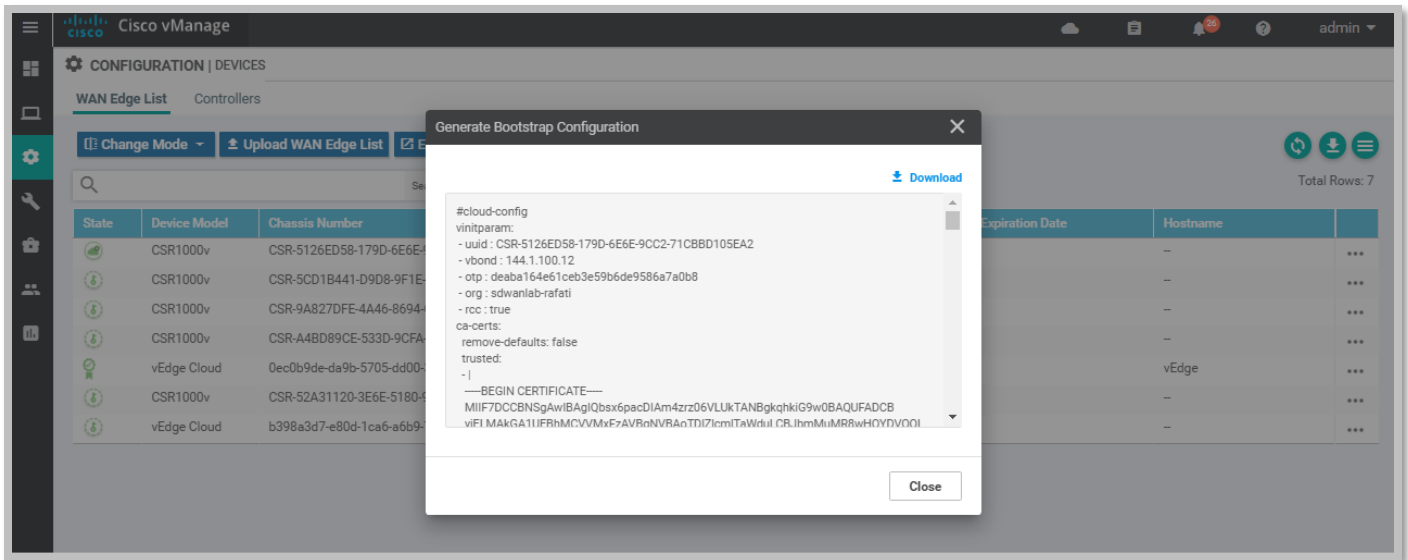
The screenshot shows the Cisco vManage interface for the WAN Edge List. The top navigation bar includes 'Cisco vManage' and 'admin'. The main header is 'CONFIGURATION | DEVICES'. Below this, there are tabs for 'WAN Edge List' and 'Controllers'. A toolbar contains buttons for 'Change Mode', 'Upload WAN Edge List', 'Export Bootstrap Configuration', and 'Sync Smart Account'. A search bar is present with 'Search Options' and 'Total Rows: 7'. The table lists devices with columns: State, Device Model, Chassis Number, Serial No./Token, Enterprise Cert Serial No, Enterprise Cert Expiration Date, and Hostname. A context menu is open over the table, showing options: Running Configuration, Local Configuration, Delete WAN Edge, Generate Bootstrap Configuration, Template Log, and Device Bring Up.

State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Enterprise Cert Expiration Date	Hostname
...	CSR1000v	CSR-5126ED58-179D-6E6E-9CC2-71CB...	Token - deaba164e61c...	NA	NA	...
...	CSR1000v	CSR-5CD1B441-D9D8-9F1E-1E60-F1FB...	Token - 2241720d041f...	NA	NA	...
...	CSR1000v	CSR-9A827DFE-4A46-8694-C520-EEB3...	Token - f3118f6b40864...	NA	NA	...
...	CSR1000v	CSR-A4BD89CE-533D-9CFA-D023-DFD...	Token - 50cadbf00a206...	NA	NA	...
...	vEdge Cloud	0ec0b9de-da9b-5705-dd00-3d98e7caf0...	F522BC3C	NA	NA	...
...	CSR1000v	CSR-52A31120-3E6E-5180-943F-62223...	Token - 993ee094e049f...	NA	NA	...
...	vEdge Cloud	b398a3d7-e80d-1ca6-a6b9-72a2376f7...	Token - 8067f51ba9e13...	NA	NA	...

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

The screenshot shows the same Cisco vManage interface as before, but with a 'Generate Bootstrap Configuration' dialog box open. The dialog box has a title bar with a close button. It contains the text 'Bootstrap Configuration:' followed by two radio buttons: 'Cloud-Init' (which is selected) and 'Encoded String'. At the bottom of the dialog are 'OK' and 'Close' buttons.

- 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.

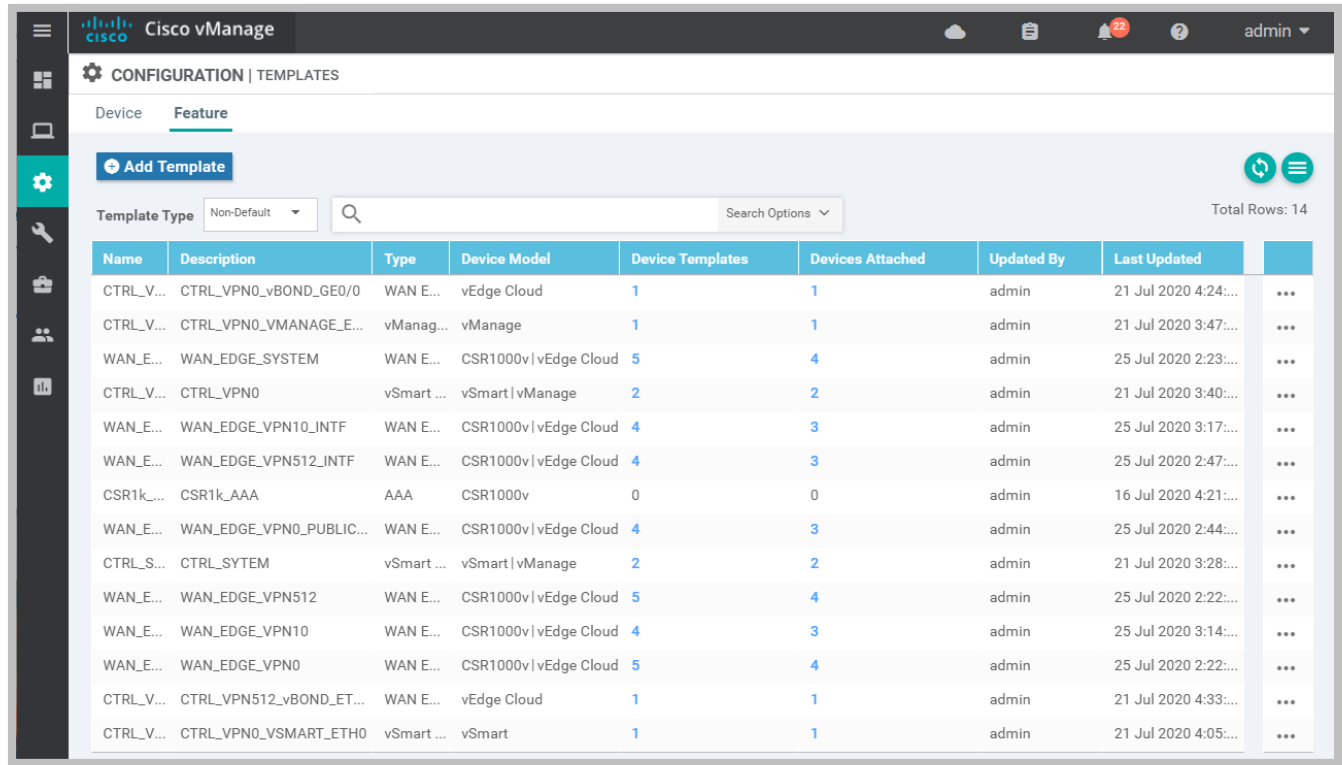
show control connections

					PEER		PEER							CONTROLLER	
PEER	PEER	PEER	SITE	DOMAIN	PEER	PRIV	PEER	PUB							GROUP
TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	LOCAL	COLOR	PROXY	STATE	UPTIME	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



Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
CTRL_V...	CTRL_VPN0_vBOND_GE0/0	WAN E...	vEdge Cloud	1	1	admin	21 Jul 2020 4:24:...
CTRL_V...	CTRL_VPN0_VMANAGE_E...	vManag...	vManage	1	1	admin	21 Jul 2020 3:47:...
WAN_E...	WAN_EDGE_SYSTEM	WAN E...	CSR1000v vEdge Cloud	5	4	admin	25 Jul 2020 2:23:...
CTRL_V...	CTRL_VPN0	vSmart ...	vSmart vManage	2	2	admin	21 Jul 2020 3:40:...
WAN_E...	WAN_EDGE_VPN10_INTF	WAN E...	CSR1000v vEdge Cloud	4	3	admin	25 Jul 2020 3:17:...
WAN_E...	WAN_EDGE_VPN512_INTF	WAN E...	CSR1000v vEdge Cloud	4	3	admin	25 Jul 2020 2:47:...
CSR1k...	CSR1k_AAA	AAA	CSR1000v	0	0	admin	16 Jul 2020 4:21:...
WAN_E...	WAN_EDGE_VPN0_PUBLIC...	WAN E...	CSR1000v vEdge Cloud	4	3	admin	25 Jul 2020 2:44:...
CTRL_S...	CTRL_SYTEM	vSmart ...	vSmart vManage	2	2	admin	21 Jul 2020 3:28:...
WAN_E...	WAN_EDGE_VPN512	WAN E...	CSR1000v vEdge Cloud	5	4	admin	25 Jul 2020 2:22:...
WAN_E...	WAN_EDGE_VPN10	WAN E...	CSR1000v vEdge Cloud	4	3	admin	25 Jul 2020 3:14:...
WAN_E...	WAN_EDGE_VPN0	WAN E...	CSR1000v vEdge Cloud	5	4	admin	25 Jul 2020 2:22:...
CTRL_V...	CTRL_VPN512_vBOND_ET...	WAN E...	vEdge Cloud	1	1	admin	21 Jul 2020 4:33:...
CTRL_V...	CTRL_VPN0_VSMART_ETH0	vSmart ...	vSmart	1	1	admin	21 Jul 2020 4:05:...

- 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**

CONFIGURATION | TEMPLATES

Basic Information | Transport & Management VPN | Additional Templates

System * LAB_SYSTEM_CTRL

Logging* Factory_Default_Logging_Template

AAA * Factory_Default_AAA_Template

Security * Factory_Default_vSmart_vManage_Security_...

Additional System Templates

- + Archive
- + NTP

Transport & Management VPN

VPN 0 * LAB_VPN0_CTRL

VPN Interface LAB_INT_VMANAGE_ETH0

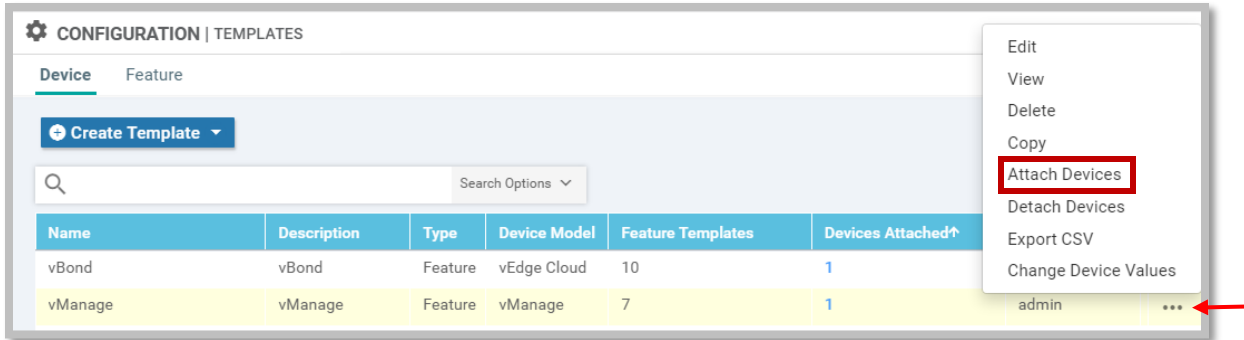
Additional VPN 0 Templates

- + VPN Interface

Create **Cancel**

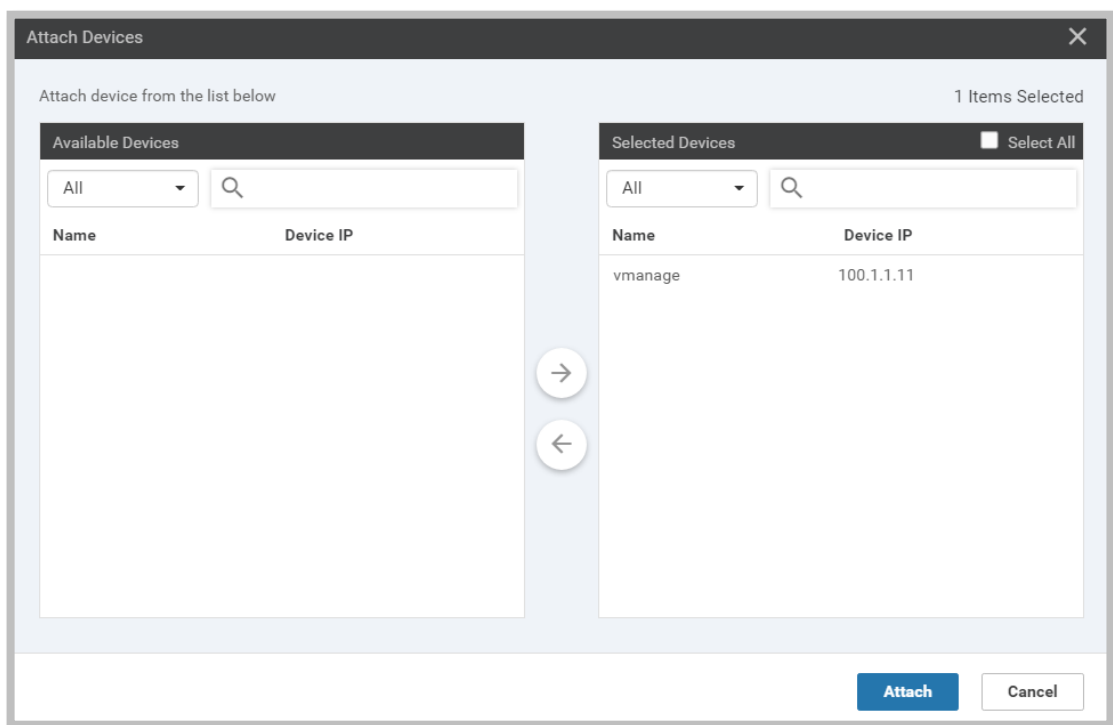
Activate Windows
Go to System in Control Panel to activate Windows.

7- Click on ...



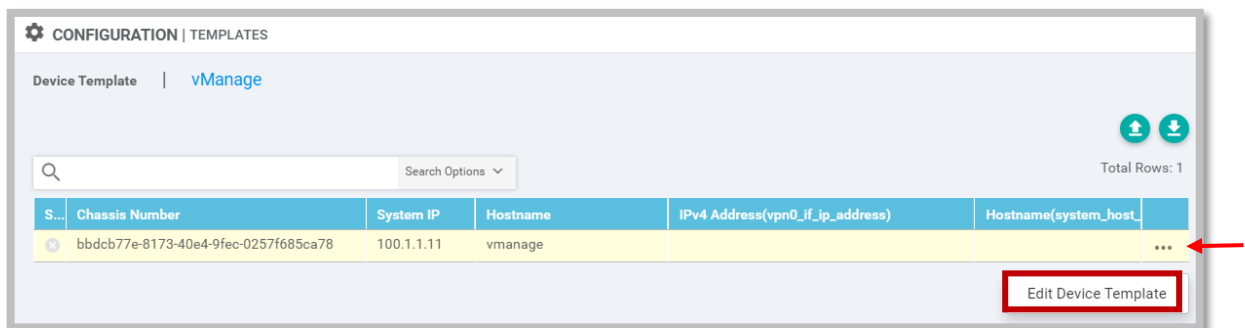
8- Select **Attach Device**

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

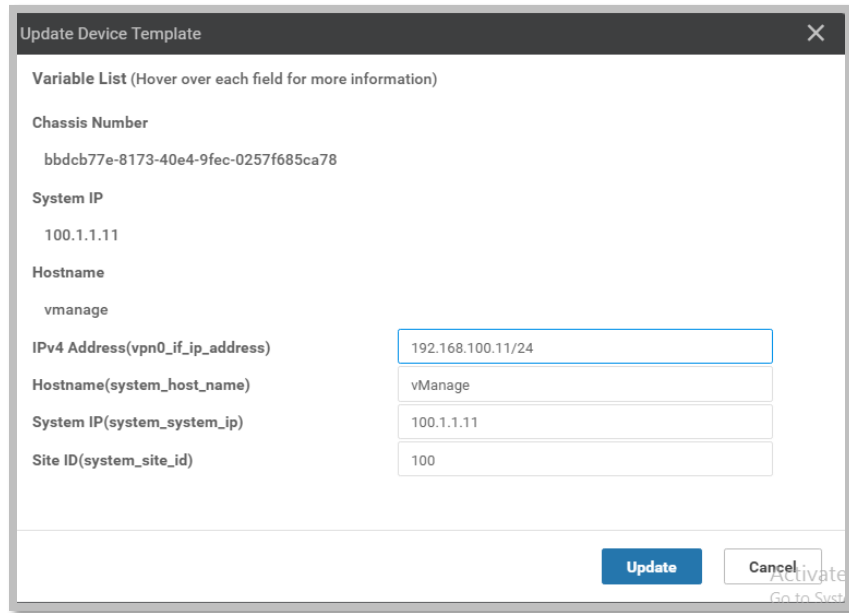


10- Click **Attach**

11- Click on ... then **Edit Device template**



12- Fill require Field then Click Update



Update Device Template

Variable List (Hover over each field for more information)

Chassis Number
bbdcb77e-8173-40e4-9fec-0257f685ca78

System IP
100.1.1.11

Hostname
vmanage

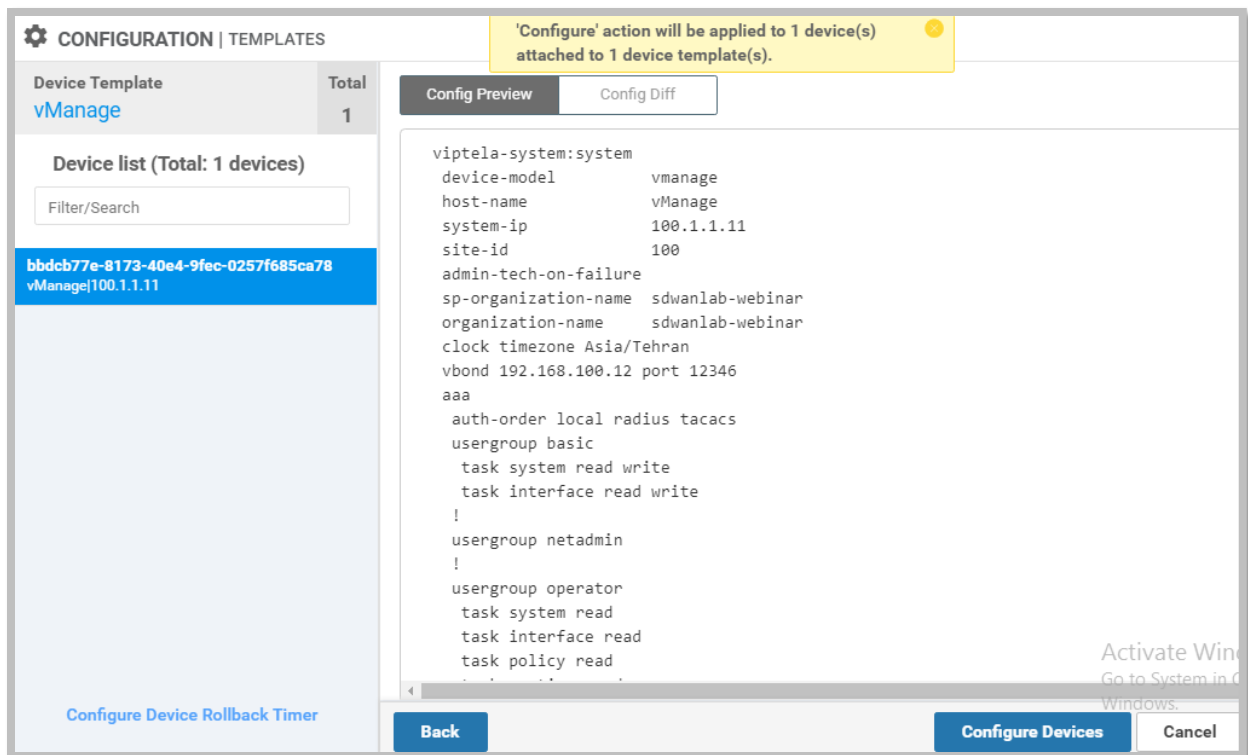
IPv4 Address(vpn0_if_ip_address)

Hostname(system_host_name)

System IP(system_system_ip)

Site ID(system_site_id)

13- Review the Configuration and click Configure Device



CONFIGURATION | TEMPLATES

Device Template: vManage Total: 1

Device list (Total: 1 devices)

Filter/Search

bbdcb77e-8173-40e4-9fec-0257f685ca78 vManage|100.1.1.11

Configure Device Rollback Timer

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

Config Preview Config Diff

```
viptela-system:system
device-model      vmanage
host-name         vManage
system-ip         100.1.1.11
site-id           100
admin-tech-on-failure
sp-organization-name sdwanlab-webinar
organization-name sdwanlab-webinar
clock timezone Asia/Tehran
vbond 192.168.100.12 port 12346
aaa
auth-order local radius tacacs
usergroup basic
task system read write
task interface read write
!
usergroup netadmin
!
usergroup operator
task system read
task interface read
task policy read
```

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**