Table of Contents

VMware Components Used

Validated with below versions, but it should be compatible with higher versions as well.

1. vCenter 6.7
2. ESXI 6.7

Prepare vCenter environment for deployment

Pre – Requisite

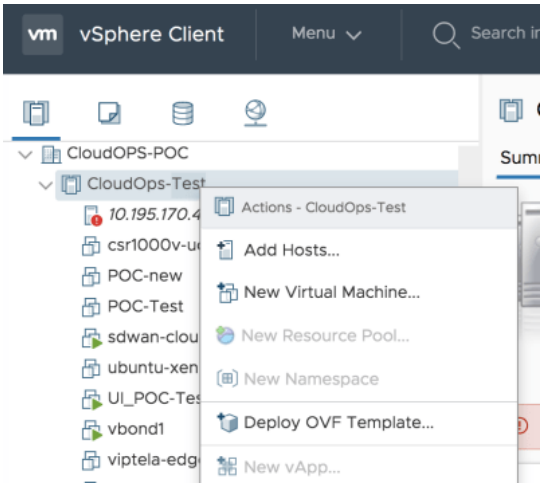
Create "**vmnet-1**", "**vmnet-2**", "**vmnet-3**" networks, if not created.

Create "**VM Network**", public network, if not created.

Create "**vmnet-4**" private network, if not created.

Deploy OVA using vSphere

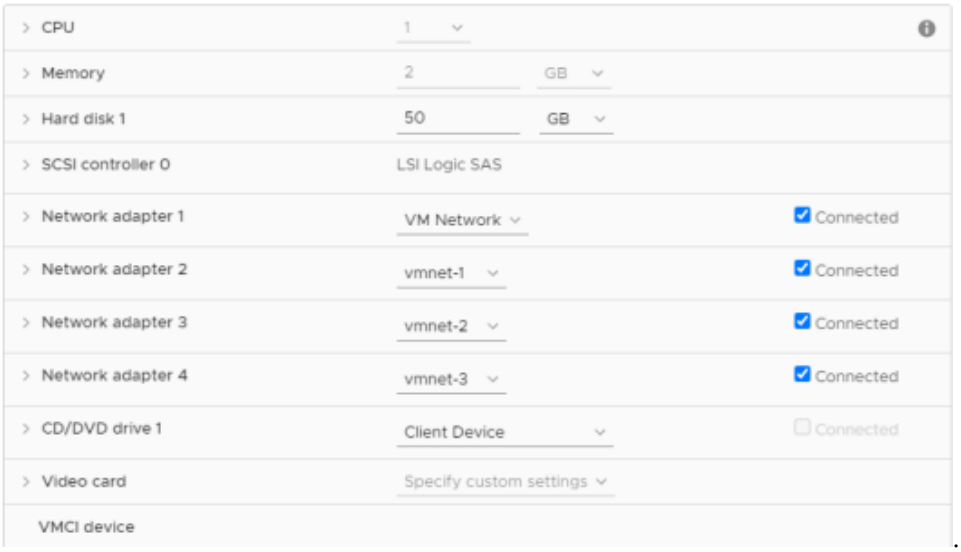
1. Deploy the OVA (SDWAN-vPrem-v2.x.ova), by selecting "Deploy OVF Template" Option.



2. Select Network adpter1 to the public facing port group, Interface1 will go to the public network. VM network should map to the public network port group.

3. vmnet-1 (10.0.1.x), vmnet-2 (10.0.99.x) and vmnet-3 (10.0.100.x) do not serve any purpose but are needed for the vPrem OVA private addressing.

4. Map your private subnet portgroup to vmnet-1, vmnet-2, vmnet-3.



5. Boot up the deployed VM. Once the image comes up, in the console do the following steps:

    1. Open the console of new VM (**username – tester, password – p0ct00l@2**).
    2. Run command – ***sudo vi /etc/netplan/00-installer-config.yaml***
    3. Update the highlighted values as per your subnet.
        1. **addresses** – VM public IP (VM Network - reachable from cisco network/VPN). Change to an IPv4 address you will be assigning to the VM. It should be reachable from your workstation (cisco network/VPN).
        2. **via** – replace it with the gateway of your VM Network subnet.
        3. **from** – this should be same as the addresses in point 1 above.
        4. **gateway4** - replace it with the gateway of your VM Network subnet.

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens160:
      addresses:
          - 10.194.228.60/24
      routes:
          - to: 0.0.0.0/0
            via: 10.194.228.1
            metric: 40
            table: 101
      routing-policy:
          - from: 10.194.228.60/24
            table: 101
      gateway4: 10.194.228.1
      nameservers:
          search: []
          addresses:
              - 171.70.168.183
    ens192:
      addresses:
          - 10.0.1.1/24
      routes:
          - to: 0.0.0.0/0
            via: 10.0.1.1
            metric: 40
```

4. Execute command – ***sudo netplan apply***
5. Now the new VM should be accessible via the new IP assigned in the above steps.
6. Once interface IP is ping-able, then you can ssh from your mac/laptop.
7. Verify the SDWAN vPrem services are running by executing below commands.
   1. ***ps -ef | grep rest***
   2. ***ps -ef | grep POC***
   3. ***sudo systemctl status poc-service***

```
tester@tester:~$ ps -ef | grep rest
root         932       1  0 May06 ?        00:00:40 python3 -u /home/tester/sdwan-devops/restapi.py
tester    137077  136630  0 00:34 pts/0    00:00:00 grep --color=auto rest
tester@tester:~$ ps -ef | grep POC
root        1313       1  0 May06 ?        00:00:00 /usr/bin/node /usr/local/lib/node_modules/forever/bin/monitor /home/tester/sdwan-devops/POC_tool_UI/server.js
root        1326    1313  0 May06 ?        00:00:12 /usr/bin/node /home/tester/sdwan-devops/POC_tool_UI/server.js
tester    137084  136630  0 00:34 pts/0    00:00:00 grep --color=auto POC
tester@tester:~$
tester@tester:~$ sudo systemctl status poc-service
[sudo] password for tester:
● poc-service.service - Sevice to start poc-tool
     Loaded: loaded (/etc/systemd/system/poc-service.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-05-06 01:14:53 UTC; 2 days ago
      Tasks: 19 (limit: 9443)
     Memory: 230.3M
     CGroup: /system.slice/poc-service.service
             ├─ 932 python3 -u /home/tester/sdwan-devops/restapi.py
             ├─1313 /usr/bin/node /usr/local/lib/node_modules/forever/bin/monitor /home/tester/sdwan-devops/POC_tool_UI/server.js
             └─1326 /usr/bin/node /home/tester/sdwan-devops/POC_tool_UI/server.js

May 08 21:52:11 tester sudo[122099]: pam_unix(sudo:session): session closed for user root
May 08 22:05:25 tester sudo[125903]:     root : TTY=unknown ; PWD=/home/tester/sdwan-devops ; USER=root ; COMMAND=/usr/sbin/iptables -t nat -v -L PREROUTING -n --line-number
May 08 22:05:25 tester sudo[125903]: pam_unix(sudo:session): session opened for user root by (uid=0)
May 08 22:05:25 tester sudo[125903]: pam_unix(sudo:session): session closed for user root
May 08 22:50:05 tester sudo[129921]:     root : TTY=unknown ; PWD=/home/tester/sdwan-devops ; USER=root ; COMMAND=/usr/sbin/iptables -t nat -v -L PREROUTING -n --line-number
May 08 22:50:05 tester sudo[129921]: pam_unix(sudo:session): session opened for user root by (uid=0)
May 08 22:50:05 tester sudo[129921]: pam_unix(sudo:session): session closed for user root
May 08 22:55:35 tester sudo[130978]:     root : TTY=unknown ; PWD=/home/tester/sdwan-devops ; USER=root ; COMMAND=/usr/sbin/iptables -t nat -v -L PREROUTING -n --line-number
May 08 22:55:35 tester sudo[130978]: pam_unix(sudo:session): session opened for user root by (uid=0)
May 08 22:55:35 tester sudo[130978]: pam_unix(sudo:session): session closed for user root
tester@tester:~$
```

8. If you notice any of the above services not running, then execute the below command.
   # sudo systemctl restart poc-service

9. Open the below file and do the modification in proxy parameters as suggested.
 # vi /home/tester/sdwan-devops/env.list

Update the two proxy parameters "HTTP_PROXY" and "HTTP_PROXY" as per below suggestion.

- If you are on Cisco network and VMs require the proxy to reach internet, then use these parameters as it is as it has been provided in the original file.
- If you are in some other network where some other proxy is required, then please provide the same for both parameters.
- If the VM can reach the internet without any proxy, then remove these 2 parameters completely from the file.

Note – In order to make the setup work it is mandatory that VM should reach the internet to validate and deploy setup so please make sure that above steps are applied carefully.

Access vPrem UI and Configure UI parameter

1. Launch SDWAN vPrem UI from browser with http://vPremPublicIP:3001
2. Initially, you see Default Configuration, below fields are pre-filled

VMWARE CONFIGURATIONS

SDWAN version = 20.3.3 → **Viptela version**
Folder = viptela_2 → **This folder value should be unique. If you have used this value earlier, then make sure to change it to unique value.**

VMWARE TEMPLATES

cEdge Template = csr1000v-ucmk9.16.12.05 → **Default CRS Template, change it if you are going to deploy different version of cEdge.**

NETWORK CONFIGURATIONS

Transport Portgroup = vmnet-2 → **Port group private network**
Management Posrtgroup = vmnet-3 → **Port group private network**
Public Portgroup = VM Network → **Port group private network**
Private Portgroup = vmnet-4 → **Port group private network**
Service VPN Portgroup = vmnet-1 → **Port group Service VPN**

VMANAGE CREDENTIALS

vMANAGE_ORG = POC - 123456 → **Default org name that comes with vPrem tool**

3. To edit configurations, click "**EDIT CONFIGURATIONS**" button.

VMWARE CREDENTIALS

First you have to enter vSphere ip, user, password and hit submit, only then it will pull the Datacenter, Cluster, Datastore info.

vSphere User = administrator@sdwan-cloudops.cisco.com → **vCenter user login**
vSphere Password = c0p\$A**** → **vCenter password**
vSphere Host = 10.195.170.49 → **vCenter IP**

VMWARE CONFIGURATIONS

Select Datacenter, Cluster, Datastore from the drop-down menu, that is populated after entering vSphere login info

Datacenter = CloudOPS-POC →**Datacenter Name**
Cluster = CloudOps-Test → **Cluster Name**
Datastore = datastore1 → **Datastore Name**
SDWAN version → **Viptela version**
Folder → **A unique value. This folder will be created in vCenter for deployment**

ESXI CREDENTIALS

ESXi Host = 10.195.170.43 → **Esxi IP**
ESXi User = root → **Esxi user**
ESXi Password = xxxx → **Esxi Password**

VM TEMPLATES

cEdge Template = csr1000v-ucmk9.16.12.05 → **cEdge template needed for cEdge deployment**

NETWORK CONFIGURATIONS

Transport Portgroup = vmnet-2 → **Port group private network**
Management Posrtgroup = vmnet-3 → **Port group private network**

Public Portgroup = VM Network → **Port group private network**
Private Portgroup = vmnet-4 → **Port group private network**
Service VPN Portgroup = vmnet-1 → **Port group Service VPN**

VMANAGE CREDENTIALS

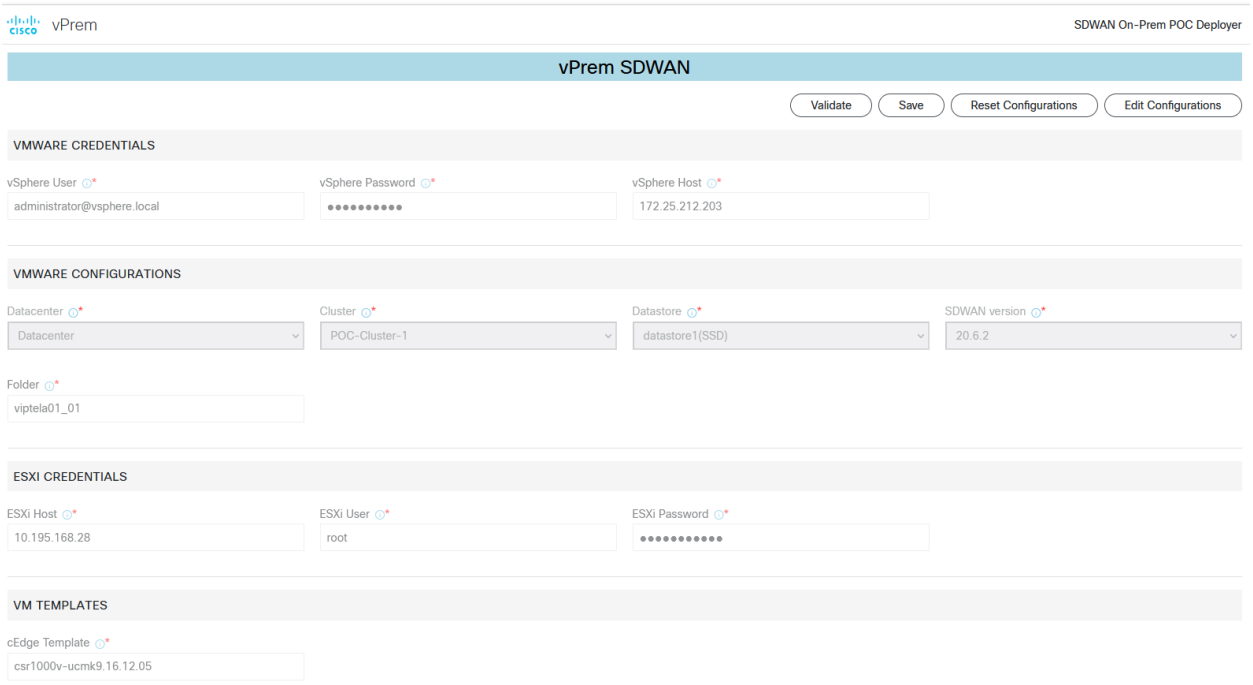
vMANAGE_ORG = 'POC-123456'. -> **Default org name that comes with vPrem tool**

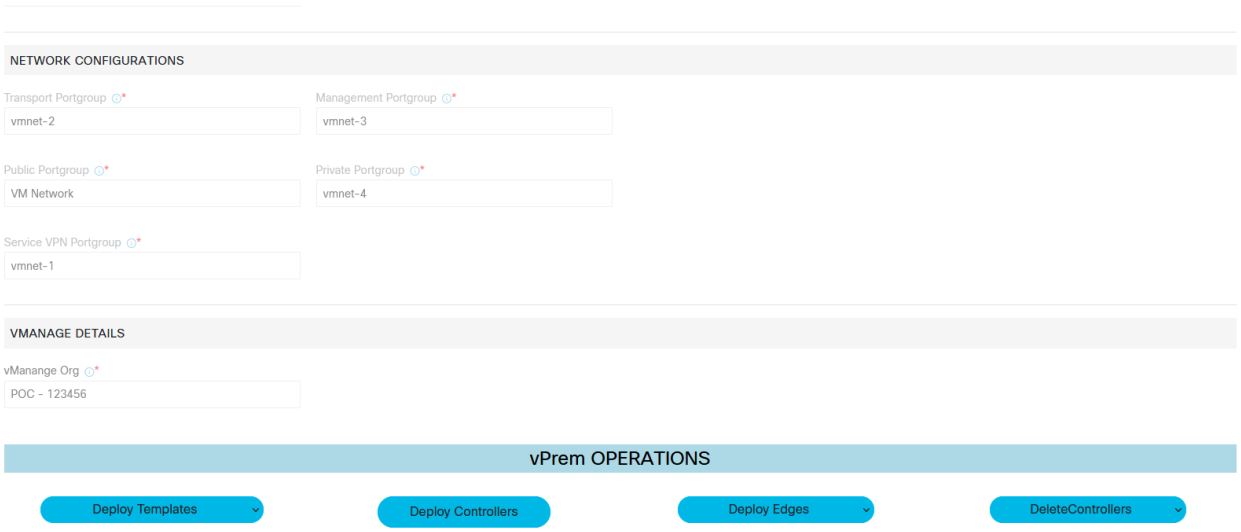
Note: By default, vPrem tool has ORG name with serial file installed with 2 vEdges and 2 cEdges. If you would like to have your own ORG name, please copy the serial file under vPrem ubuntu VM: /home/tester/sdwan-devops/licenses. And update the UI with correct ORG name.

tester@tester:~/sdwan-devops/licenses$ ls -ltr

total 4

-rw-rw-r-- 1 tester tester 2037 Apr 18 11:42 serialFile.viptela





4. To Reset Configuration to default, click "**RESET CONFIGURATIONS**", you will enter edit mode. To come out of Edit mode, use "**CANCEL**" button
5. After filling all the MANDATORY FIELDS (*), you can use "**VALIDATE**" button, to validate Network Configurations.
6. Once all the Mandatory Fields are done, then only "**SAVE**" button will be enabled.
7. Once the configuration is saved, then only below buttons will be enabled

DEPLOY TEMPLATES

DEPLOY vBOND TEMPLATE
DEPLOY vSMART TEMPLATE
DEPLOY vMANGE TEMPLATE

DEPLOY CONTROLLERS

DEPLOY EDGES

DEPLOY cEDGE
DEPLOY vEDGE

DELETE

DELETE CONTROLLERS
DELETE cEDGE
DELETE vEDGE

Creating the SD-WAN VM templates

vManage, vSmart and vEdge

In the vCenter UI, create the Viptela VM Templates:

1. Deploy the Viptela OVA for vManage, vEdge and vSmart -

   Templates Deployment can be done via vPrem Gui or OVF tool commands or vCenter UI.

   vPrem Gui :
   ** For Deploying the templates via Gui-
   Deploy Templates button is available, under which we have options for Deploying Template for 1: vSmart 2: vManage 3: vBond
   It will create the templates as per given viptela version. It will not overwrite the existing Templates on vCenter if they already exist.

   Note: OVA Files for vSmart, vManage, and vEdge should be available on vPrem machine at /home/tester location.

   Ovftool Commands:

   ** Below ovftool command can be used to deploy these templates
   sudo ovftool --noSSLVerify --net:'VM Network'='{Public network}' --datastore='datastore1' --name=viptela-vmanage-19.2.3-genericx86-64 --diskMode=thin /home/tester/viptela-vmanage-genericx86-64.ova vi://{esxi_username}:{esxi_password}@{esxi_ip}/

   If using OVF Tool command, all three ova (vManage/vSmart/vBond) should be present on vPrem machine at /home/tester.
   viptela-smart-genericx86-64.ova / viptela-smart-{SDWAN version}-genericx86-64.ova
   viptela-vmanage-genericx86-64.ova / viptela-vmanage-{SDWAN version}-genericx86-64.ova
   viptela-edge-genericx86-64.ova / viptela-edge-{SDWAN version}-genericx86-64.ova

   Check on vsphere templates should be created as below for 19.2.3 viptela version:
   viptela-vmanage-19.2.3-genericx86-64
   viptela-edge-19.2.3-genericx86-64
   viptela-smart-19.2.3-genericx86-64

   vCenter UI:

This is required when you deploy all 3 ova from vsphere itself (using Deploy OVF Template). In the "Select storage" section, set the virtual disk format to "Thin provisioned" to make more efficient use of the datastore disk space.

2. Next step is needed only for OVAs of version 19.x. It is automatically taken care of for OVAs of version 20.x.

3. Once all 3 OVAs of version 19.x have been deployed, edit the settings of each Viptela VM template:

    1. Add a "SCSI Controller" of type "LSI Logic Parallel".
    2. Change "Hard disk 1" "Virtual Device Node" setting from "IDE 0" to "New SCSI controller".
    3. Click OK.
    4. The VM is now ready to use as a template for use with terraform.

    Note: Do not add a second disk to the vManage template. Terraform will do this dynamically.

CSR1000v

In the vCenter UI, create the VM template for CSR1000v w/SD-WAN (aka cEdge):

1. Deploy the OVF. (csr1000v-ucmk9.16.12.1e.ova or similar)
2. In the "Select storage" section, set the virtual disk format to "Thin provisioned" to make more efficient use of the datastore disk space.
3. In the "Customize template" section, just leave the values blank and click "Next". Terraform will set these properties when it clones the VM.
4. After the OVF is successfully deployed, go to the "Configure" section and select "vApp Options" from the menu on the left. Click "Edit..." and unselect the "Enable vApp options" checkbox at the top. Say "Yes" to the dialog box, then click "OK".
5. Power on the VM and watch the console.
6. Power off the VM immediately after the first reboot. (If you miss this and power it off after it is fully up, delete the VM and repeat this process.)
7. The VM is now ready to use as a template for use with terraform.

Deploy Controllers and Edges

Deploy Controllers

1. Click on "DEPLOY_CONTROLLER" to deploy the sdwan controllers.

   Note: It performs few validations, before it actually deploys controllers. Validation check includes – Check Network configuration entered by user exists or not, vBond/vSmart/vManage template creation on vCenter and template settings on vSphere is correct or not.

   Note: Because of some intermittent connection issues from vPrem VM to vManage, sometimes vManage is not completely up. Check the log /home/tester/sdwan-devops/sdwan.log or console.log under vPrem VM for the failures.

2. Launch vManage UI by launching https://vPremPublicIP:9912/ , make sure vBond ,vSmart are added and shows green on dashboard.
   Credential for vManage → username – admin, password – cisco

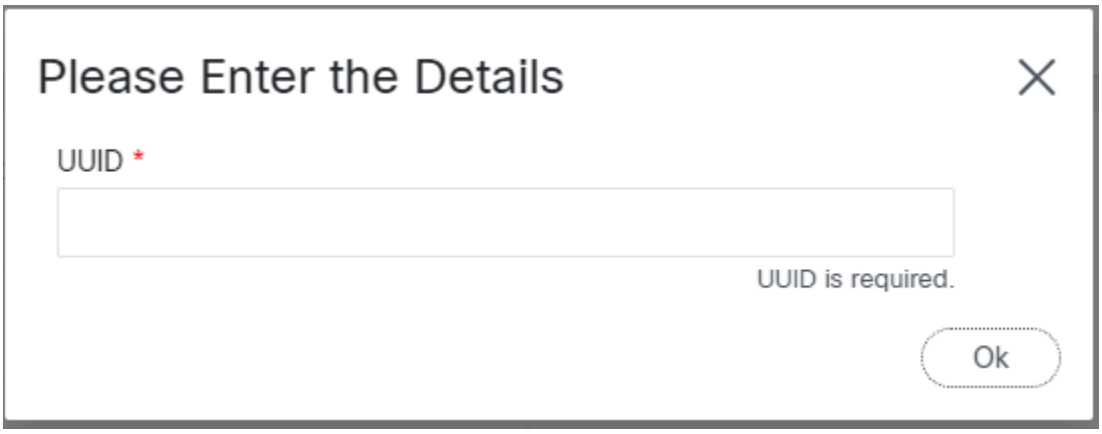
   Note: For Viptela versions 20.5 and above, there is a bug because of which the deployment of edges fails if we try to deploy directly after the deployment of controller. The workaround for this is to reboot the vManage once after the successful deployment of all the controllers. vPrem Tool takes care of this issue. Tool automatically reboot the vManage once the controllers are deployed successfully. All we have to do is wait for the vManage UI to come back after the reboot and then proceed for the further operations.

Deploy Edges

Deploy vEdge

Click on "DEPLOY-vEDGE" to deploy the edge devices and enter the valid vEDGE UUID via which you want to make the device up.

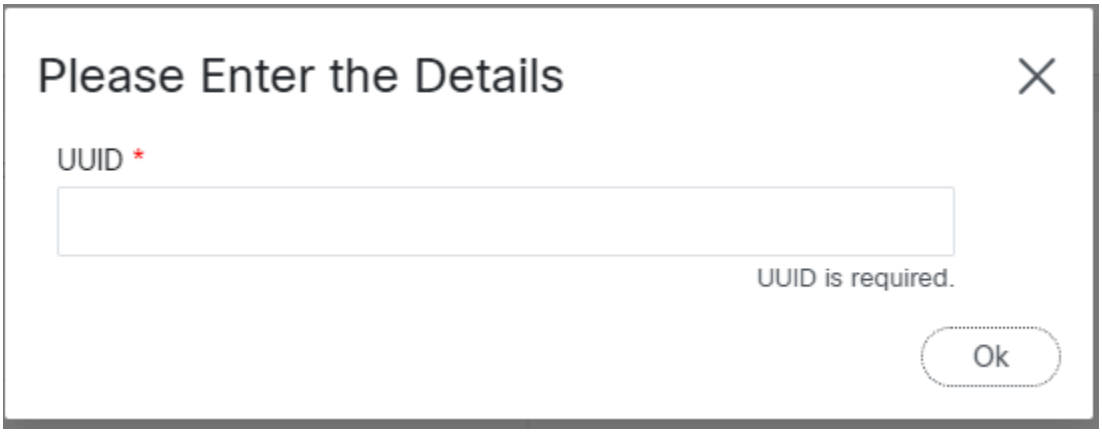
Note: Login to vManage and get the vEdge UUID from the registered devices list.



Deploy cEdge

3. Click on "DEPLOY-cEDGE" to deploy the edge devices and enter the valid cEDGE UUID via which you want to make the device up.

   Note: Login to vManage and get the cEdge UUID from the registered devices list



Delete Edges and Controllers

1. To remove any vEDGE and cEDGE device, please enter the corresponding UUID.
2. After deleting vEDGE and cEDGE, you can delete the Controllers.

Caveats

1. vCenter user that used for deployment should have the admin permissions to create required VM resources.
2. vEdge not coming online while deploying, workaround is to reboot the VM and bring it online.