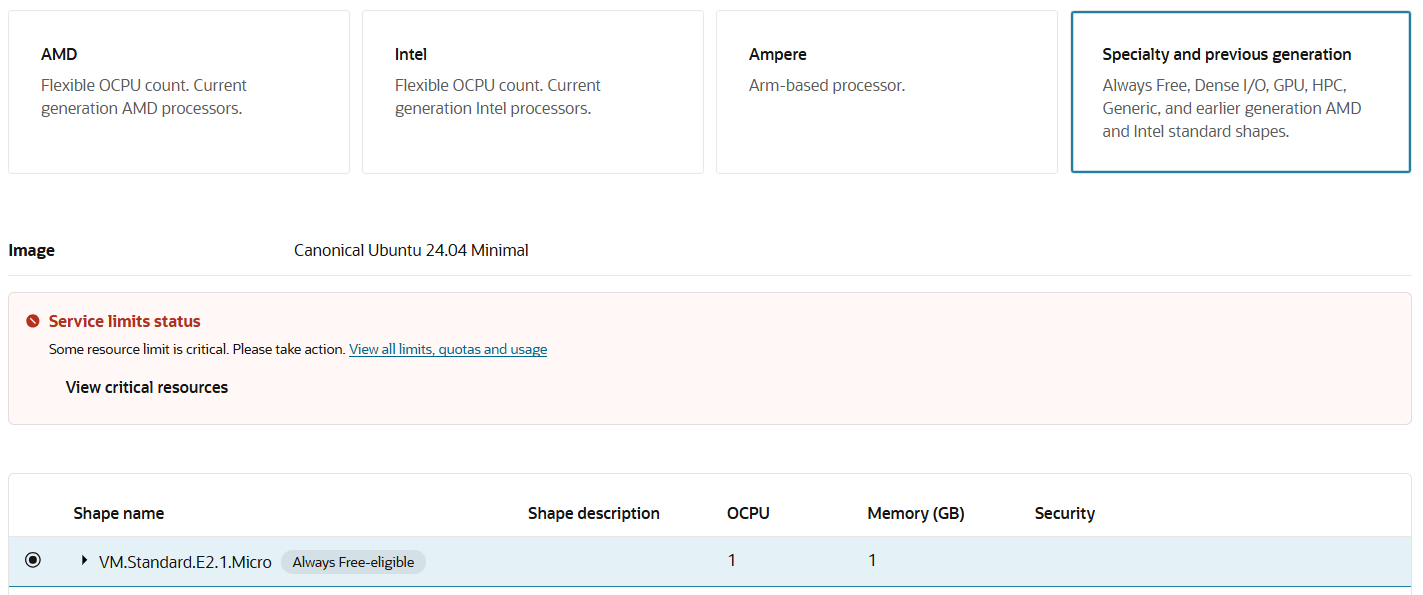
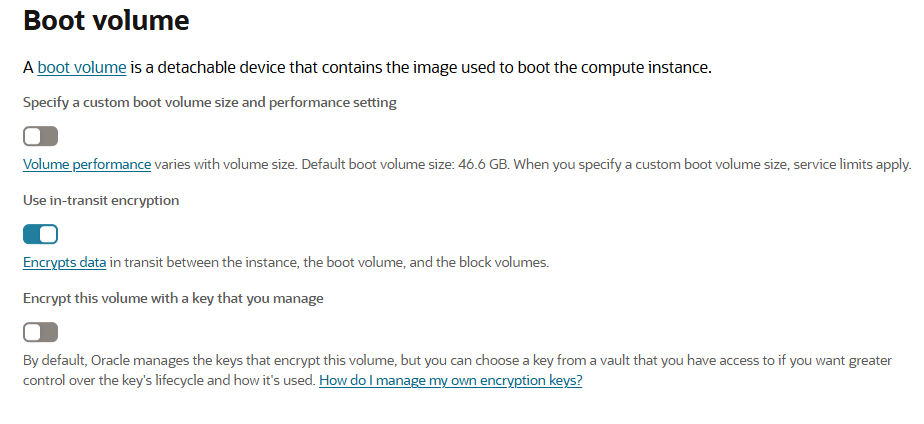
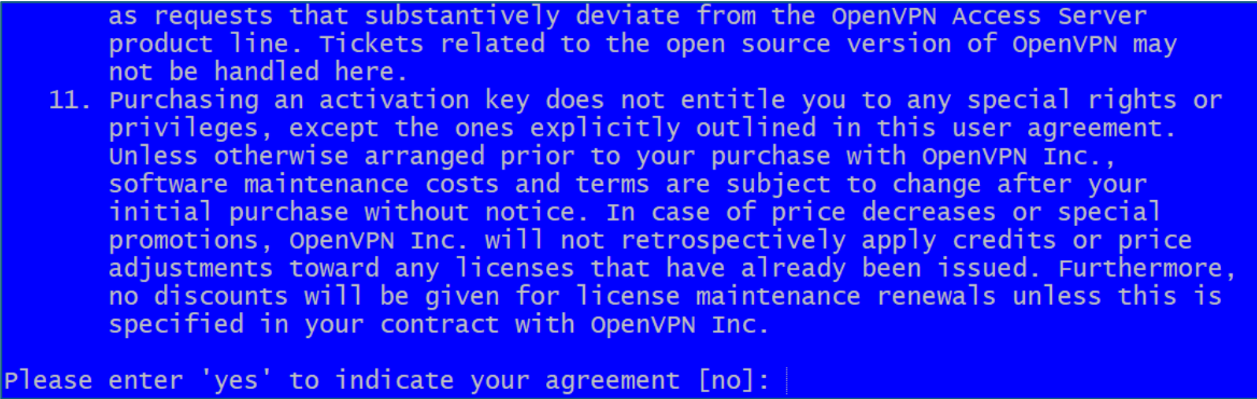
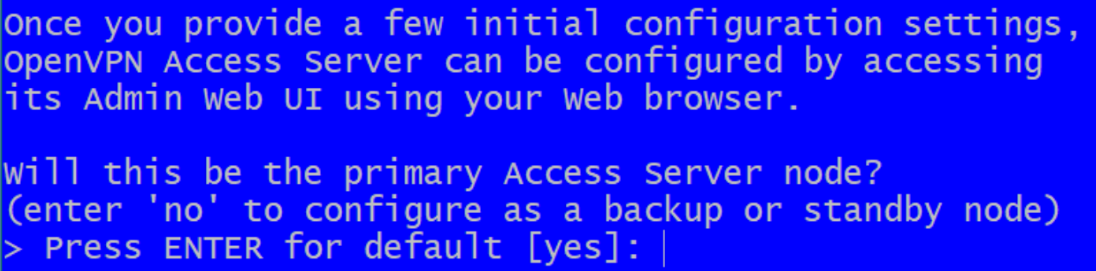
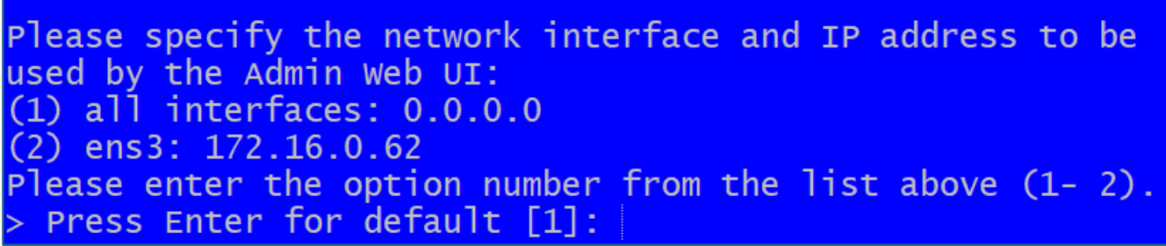
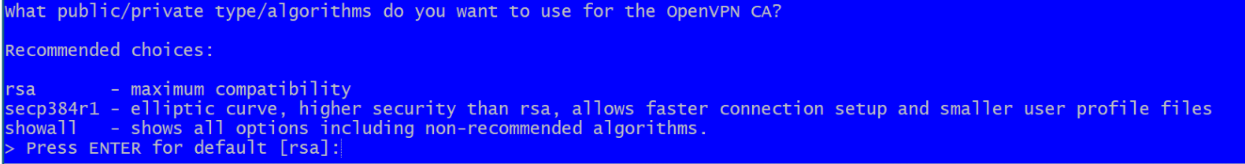
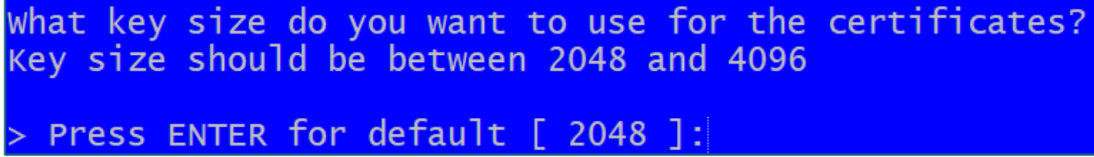
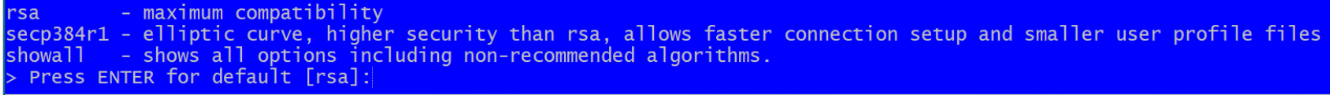
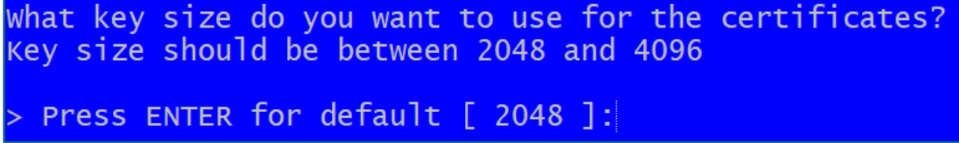
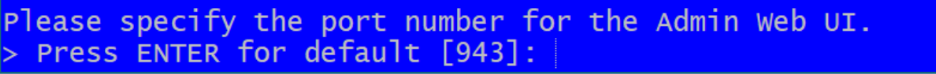
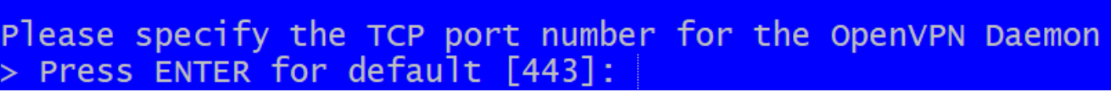
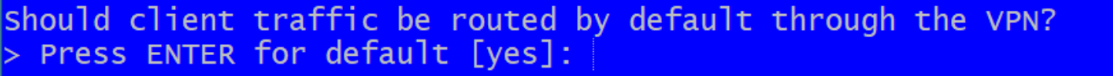
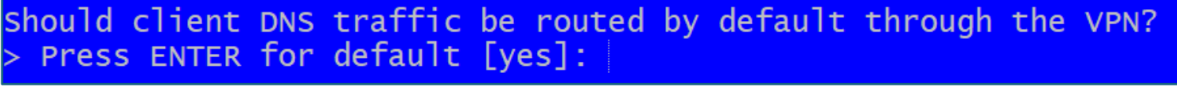
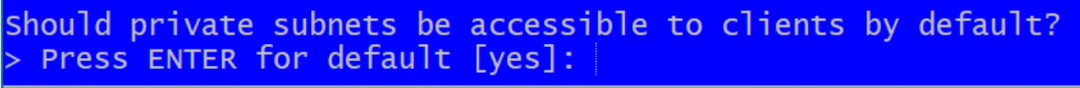
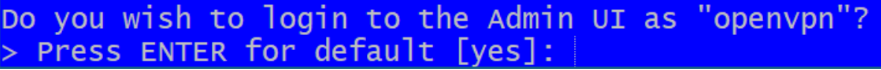
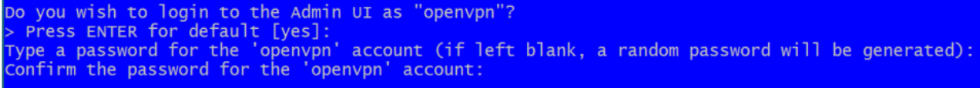
1. Login to OCI Tenancy.
2. Go to marketplace and type OpenVPN.
3. Click on that OpenVPN Access Server BYOL.
4. Select compartment and launch instance.
5. Give name for instance and select shape (can be mostly free one)
6. If the limit has exceeded for free VPN then go to specialty and previous generation image section.
7. If this also does not work, then go for VM.Standard.E2.1 (this needs approval).
8. Select existing VCN and subnets.
9. Generate new pair of keys and Download them.
10. Make Sure for boot volume section, the use in-transit encryption is enabled.
11. Create Instance.
12. Create NSG and attach it to the Instance.
    * 1. What is my IP (search on google)
      2. Add Access of GUI console (943 and 443 ports) only to your own public IP.
      3. Add port 1194 (UDP) only for public subnet created in OCI VCN.
      4. Add access of ssh remote (port 22) only to your own IP.

**VPN Configuration**

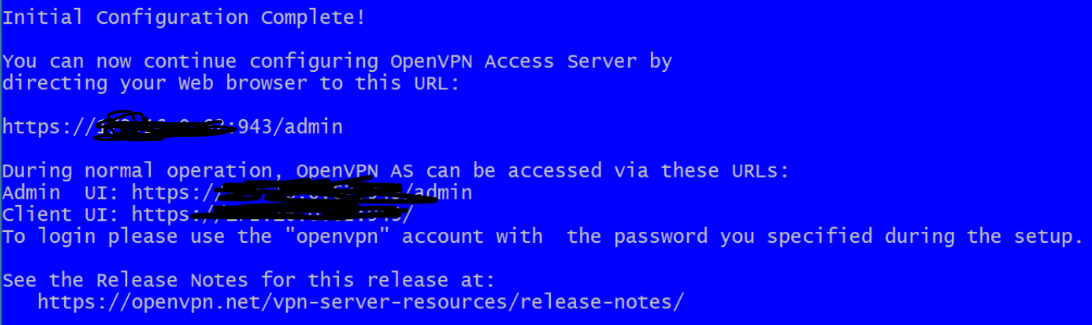
1. Generate .ppk key using PuTTYgen, with help of that downloaded private key.
2. Now open PuTTY and login into instance using public IP and .ppk key, the default user is **openvpnas**.
3. This will automatically initiate the configuration window.

Enter: yes



1. Enter: yes
2. Enter: 1(default)
3. Enter: default(RSA)
4. Enter: default (2048)
5. Enter: default(rsa)
6. Enter: default(2048)
7. Enter: default(943)
8. Enter: default(443)
9. Enter: default(yes)
10. Enter: default(yes)
11. Enter: default(yes)
12. Enter: default(yes)
13. Enter Alphanumeric + special character 8 letter strong password.
14. Enter (specify activation key latter)

This will initiate the Configuration, and you’ll see the message for admin UI



**GUI Configuration**

1. https://<publicIP>/admin

2. Enter your previously set credentials and agree the terms and conditions.

3. Go to Configuration -> network settings

replace the hostname/IP Address with instance’s public IP from private IP.

Save Changes.

4. Go to Configurations -> VPN settings

Check for the routing. The private subnet should be the private subnet created in OCI to access resource.

If VPN is only to access single VM then add only single IP instead of entire subnet.

5. If internet is required, then click on use client’s specific DNS.

Primary: 8.8.8.8 and secondary: 1.1.1.1

6. Save changes.

7. Go to user management -> user permission

Create new user (should not be admin)

Set password which has to be a combination od alphanumeric and special characters.

Save settings.

8. Go to authentication -> settings

Make sure MFA is yes.

9. Share VPN credentials with the user 1:1 along with the document to setup.

10. Ask for public IP of the user allow in NSG attached to VPN instance.

11. Add IP only for 443 port access.

Please note : there will be no port access allowed for 0.0.0.0/0 IP, NSG is must and MFA is also mandatory.

Last step is to add ingress & egress rule as per the instance access requirements in respective NSG.

For example, if access needs to be granted for application access then add into their respective

NSG the ingress rule

IP :- user’s public IPPort :- 22 (whichever are required)

Add egress rule in NSG

direction : egress

Destination type : NSG

Destination : NSG name(app server)

Destination port : which are required from vpn