## **This document assumes OpenVPN Server is already installed and configured**

* If not follow the given link- [How to setup OpenVpn Server?](https://help.ubuntu.com/lts/serverguide/openvpn.html)

## **Step 1: Set Up CA in Windows AD**

* Follow the given link - [Setup CA in Windows AD](https://docs.google.com/a/gslab.com/document/d/1uDO7v5OQEt2HwALDFBoSGDEoV_klfNdNzIk92sp8k9c/edit?usp=sharing)

## **Step 2: Create new Certificate template for VPN connection**

* Follow the given link - [Create new certificate template](https://docs.google.com/a/gslab.com/document/d/1Dyc5FBBWLfAIcz1AfOoGaonx45rPXnD17Vngriyvj1k/edit?usp=sharing)

## **Step 3: Configure User certificate Auto-Enrollment**

* Follow the given link - [User certificate Auto-Enrollment](https://docs.google.com/a/gslab.com/document/d/1_a1NTnGpzUIE10YT8uywGfRbDcLF0ZPfItBICDhZbbQ/edit?usp=sharing)

## **Step 4: Export CA certificate**

* Follow the given link - [Export CA certificate](https://docs.google.com/a/gslab.com/document/d/1ZJmErjn7Prvrcs7L4R36IM5ZcpYh4LIMs5F02zYoz6M/edit?usp=sharing)

## **Step 5: Export User certificate**

* Follow the given link - [Export User certificate](https://docs.google.com/a/gslab.com/document/d/1G-XWNgMhWqVn3ggOXIhEIZi448zKqHZ8bDnS19wgsPo/edit?usp=sharing)

## 

## 

## **Step 6: Modify OpenVpn to use AD CA certificates.**

* Copy windows AD ca certificate which we exported in step 5 in /etc/openvpn directory.
* Export administrator or any other user certificate and key, by following step 6 and then copy the same in /etc/openvpn directory.
* Edit /etc/openvpn/server.conf file to change following -

ca RootCA.crt #Windows AD CA certificate

cert administrator.crt #Windows AD administrator certificate

key administrator.key #Windows AD administrator key

## **Step 7: User authentication and certification validation.**

* **Username and Password authentication**

/etc/openvpn/server.conf

username-as-common-name  
 script-security 3  
 auth-user-pass-verify /etc/openvpn/scripts/auth.sh via-env

* **Certificate verification (Script to ensure users using only his/her creds and cert to access openvpn and user creds validation)**

[/etc/openvpn/scripts/auth.sh](https://drive.google.com/a/gslab.com/file/d/0BwEsFoHX046Vb3hTYVA0SFN1VlE/view?usp=sharing)

#!/bin/bash

dn="cn=users,dc=vpn,dc=local" #Change dc depends upon your AD domain

ad\_host="10.136.60.58" #Windows AD IP

ad\_domain="vpn.local" #Windows AD domain

if [ "${username,,}" != "${common\_name,,}" ]; then

echo "$(date) | $username : DENIED username [$username] and cert [$common\_name] does not matched" >> /etc/openvpn/access.log

exit 1

fi

user=`ldapsearch -x -h $ad\_host -b $dn -D "$username@$ad\_domain" -w $password -s sub \

-b $dn "(&(objectCategory=person)(objectClass=user)(sAMAccountName=$username))" "dn" | grep 'numEntries:'`

if [ -z "$user" ]

then

echo "$(date) | $username : Invalid password " >> /etc/openvpn/access.log

exit 1

fi

echo "$(date) | $username : connected" >> /etc/openvpn/access.log

exit 0

## **Step 8: Setup OpenVpn server in HA (Active-Passive mode)**

Assuming you have two OpenVpn servers already configured-

* Follow the given link - [Configure HA Virtual IP](https://docs.google.com/a/gslab.com/document/d/10iPQ2P7cYndU3jxPbRceIl6FHGZq5YIFQ673IZlwof0/edit?usp=sharing)
* Change in /etc/openvpn/server.conf -

local <your Virtual HA ip> #Change it with your HA Virtual IP

* Restart OpenVpn Server-

$ service openvpn@server restart

## **Step 9: Change client ovpn file**

* remote <your Virtual HA ip> 1194
* Add **auth-user-pass**
* Use AD certificates

ca RootCA.crt #Windows AD CA certificate

cert administrator.crt #Windows AD User certificate

key administrator.key #Windows AD User key

* Comment ns-cert-type server

#ns-cert-type server

## **Step 10: Ensure User will get same IP from both OpenVpn servers**

* Follow the given link - [Setup External Storage](https://docs.google.com/a/gslab.com/document/d/1vb6XaP4zubcbmuV7zcrMkn5Bscq3wbaue8TpWsjwImM/edit?usp=sharing)

## **Step 11: Restart the OpenVpn server**

$ service openvpn@server restart