Configuring Cisco Any Connect Secure Mobility Client

Manual: Configuring Cisco AnyConnect Client in Ubuntu

Platform: Ubuntu

Audience: NIC VPN Users

Date: November 2025

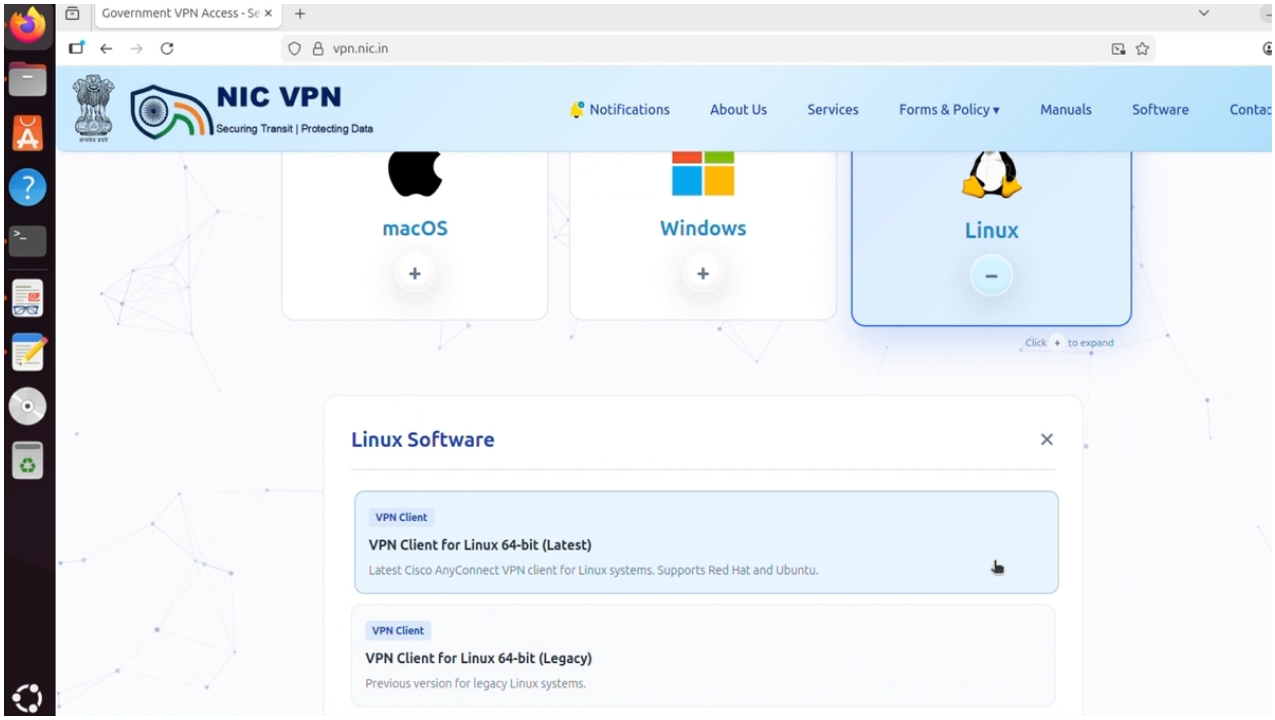
1. Download & Extract

1.
Go to user's home directory

First, open a terminal and navigate to the **user's home directory**.

2.
Download the Cisco AnyConnect Client

Download the **Cisco AnyConnect Client** from the website vpn.nic.in



3.

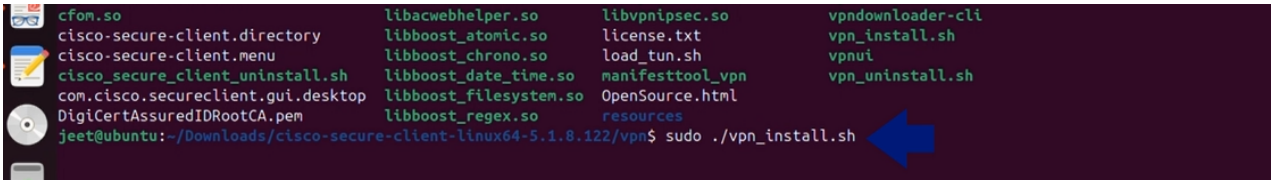
Extract Folder and Install the VPN Client

Install the **VPN Client** by running the following commands.

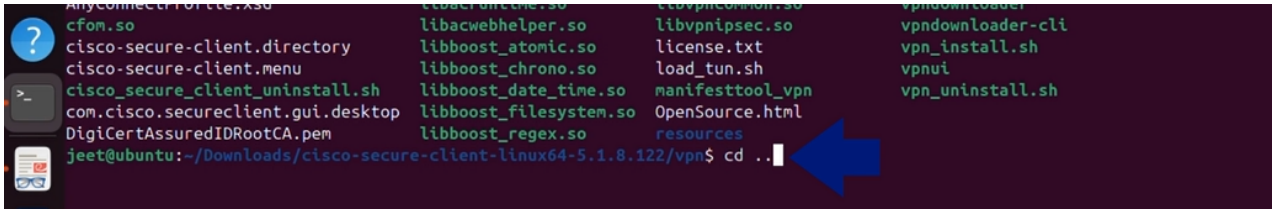
a) tar -xvf anyconnect-linux-64-5.1.8.122-k9.tar.gz

b) cd cisco-secure-client-linux64-5.1.8.122/vpn/

c) ./vpn_install.sh



d) cd ../..



e) systemctl status vpnagentd

2. Tool Installation

1.

Create two folders

To store the **client** and **CA** certificates, create the following directories by running the following **commands**.

a) mkdir -p ~/.cisco/certificates/client ~/.cisco/certificates/ca

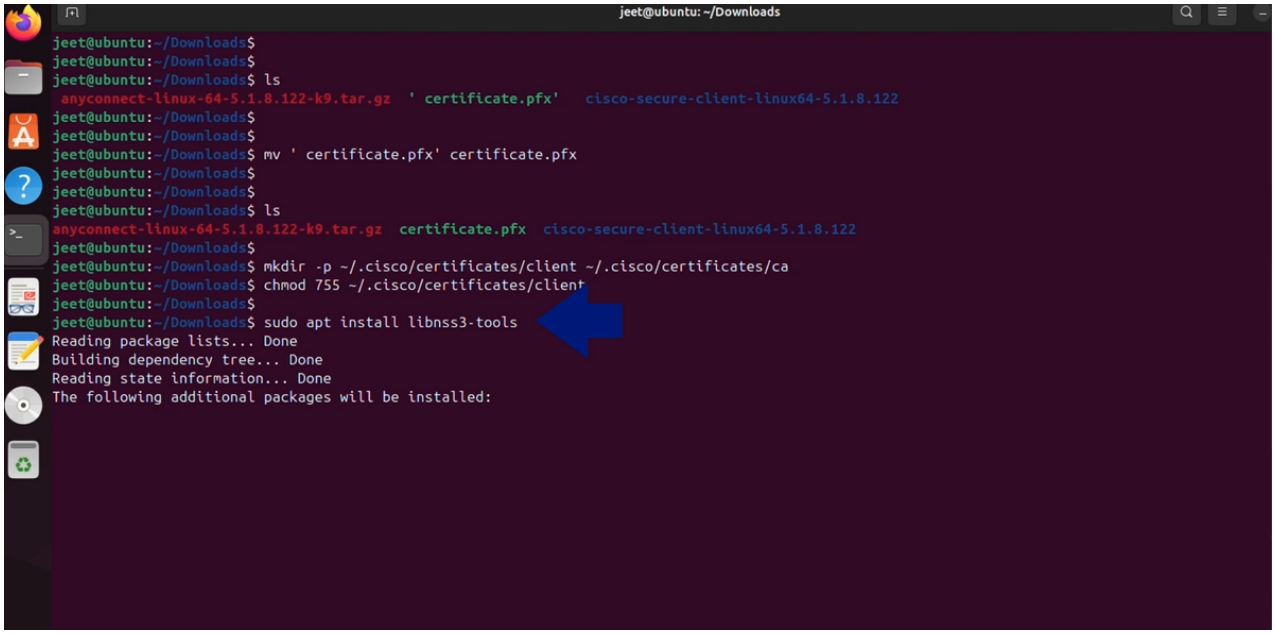
b) chmod 755 ~/.cisco/certificates/client

2.

Install required certificate tools

Install the required **certificate tools** by running the following **commands**.

a) sudo apt install libnss3-tools

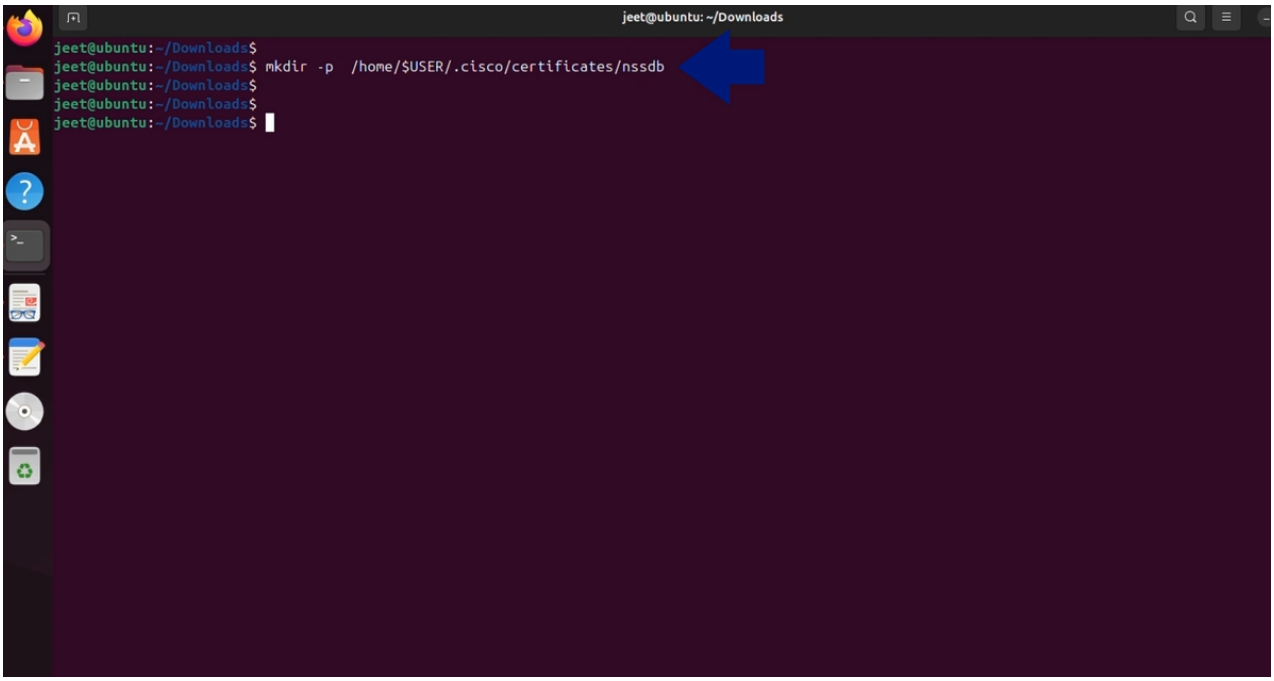


3.

Create a directory

To store the **NSS** database, create the following directory by running the following **command**.

a) mkdir -p /home/$USER/.cisco/certificates/nssdb



3. Import Certificate (DSC)

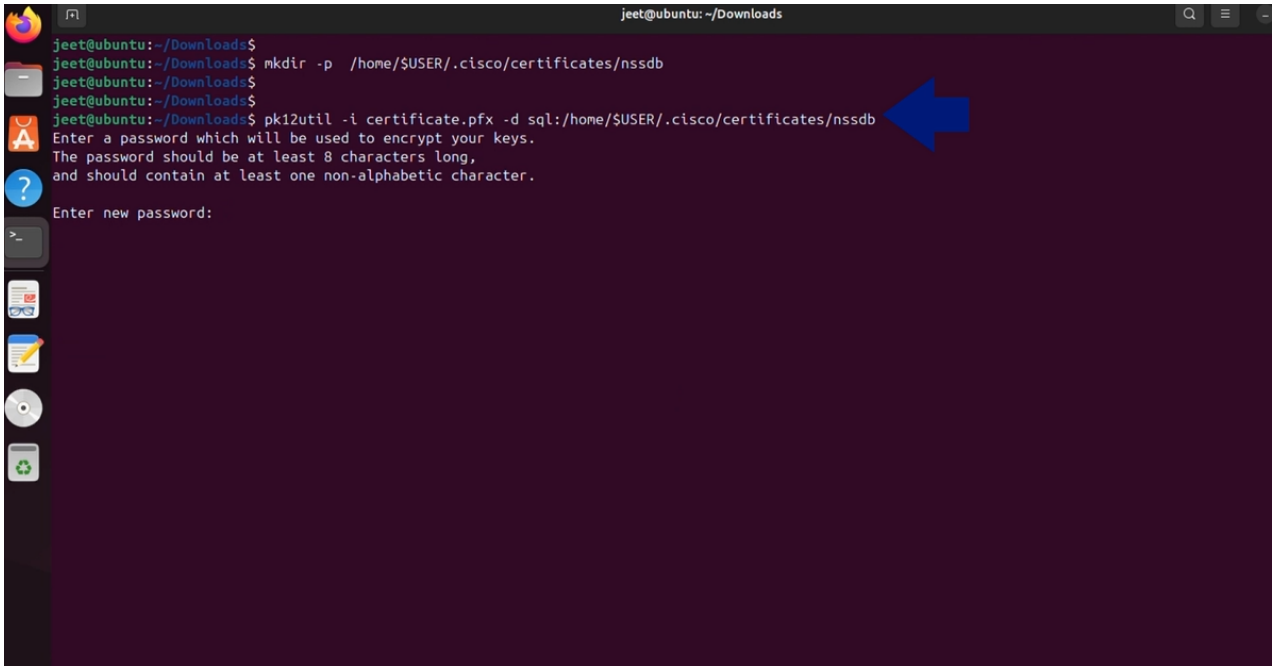
1.

Import Certificate to NSS Database

Import the **certificate** to the **NSS database** by running the following command.

a) pk12util -i certificate.pfx -d sql:/home/$USER/.cisco/certificates/nssdb

Note: The first password is of your choice for the certificate store, you can enter the password of your choice. Whereas the second password is the private key share with you on your registered contact number.

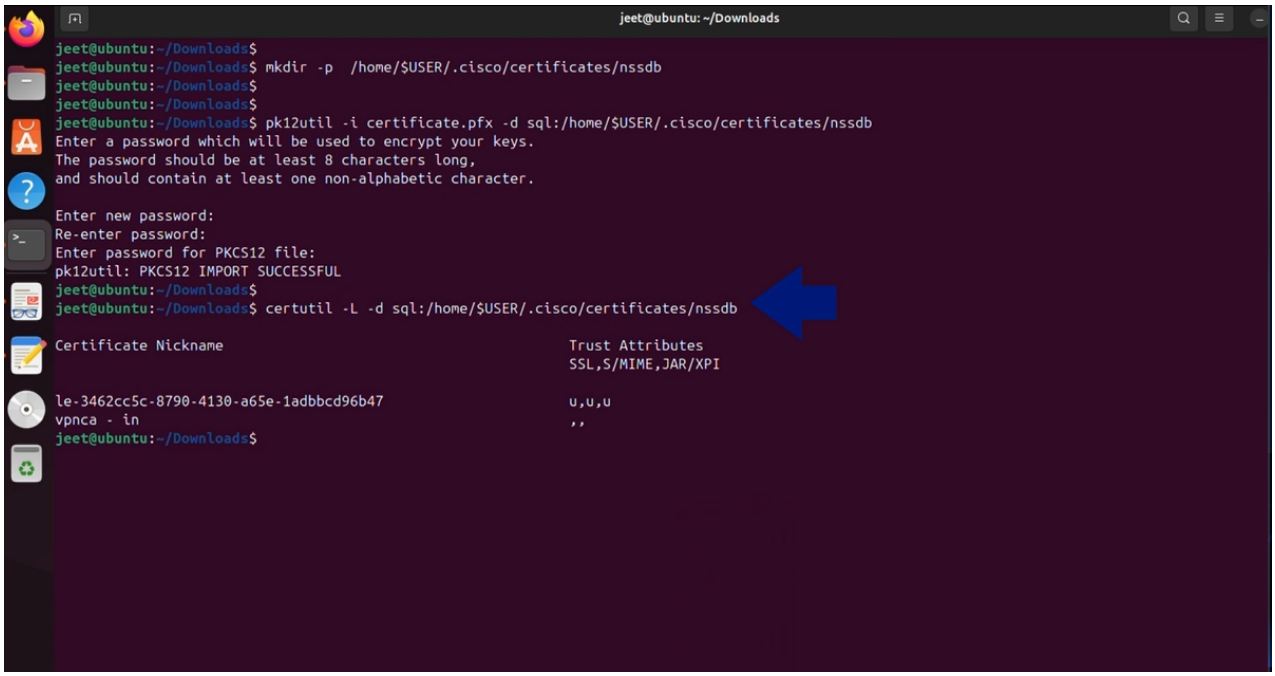


2.

To verify the certificate in nssdb

To verify the certificate in **nssdb**, run the following command.

a) certutil -L -d sql:/home/$USER/.cisco/certificates/nssdb



3.

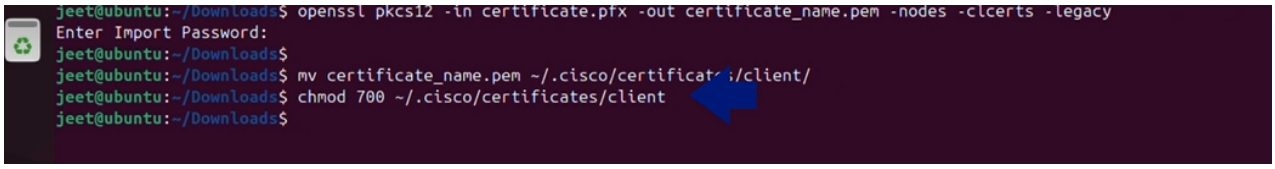
Extract and Secure PEM Certificate

Extract the **PEM certificate** and move it to the **client certificate directory** by running the following commands.

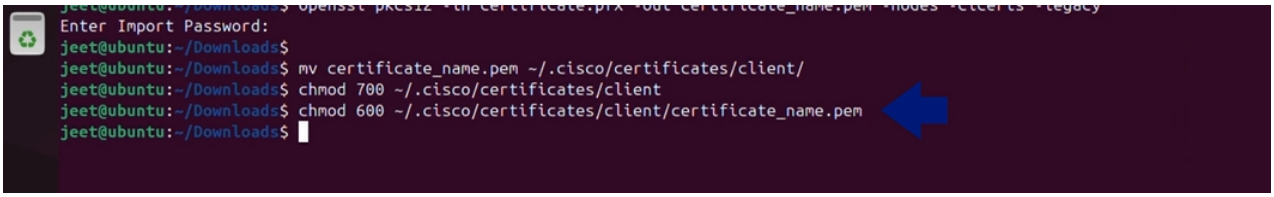
a) openssl pkcs12 -in certificate.pfx -out certificate_name.pem -nodes -clcerts -legacy

b) mv certificate_name.pem ~/.cisco/certificates/client/

c) chmod 700 ~/.cisco/certificates/client



d) chmod 600 ~/.cisco/certificates/client/certificate_name.pem



Note: Enter your private key after running first command.

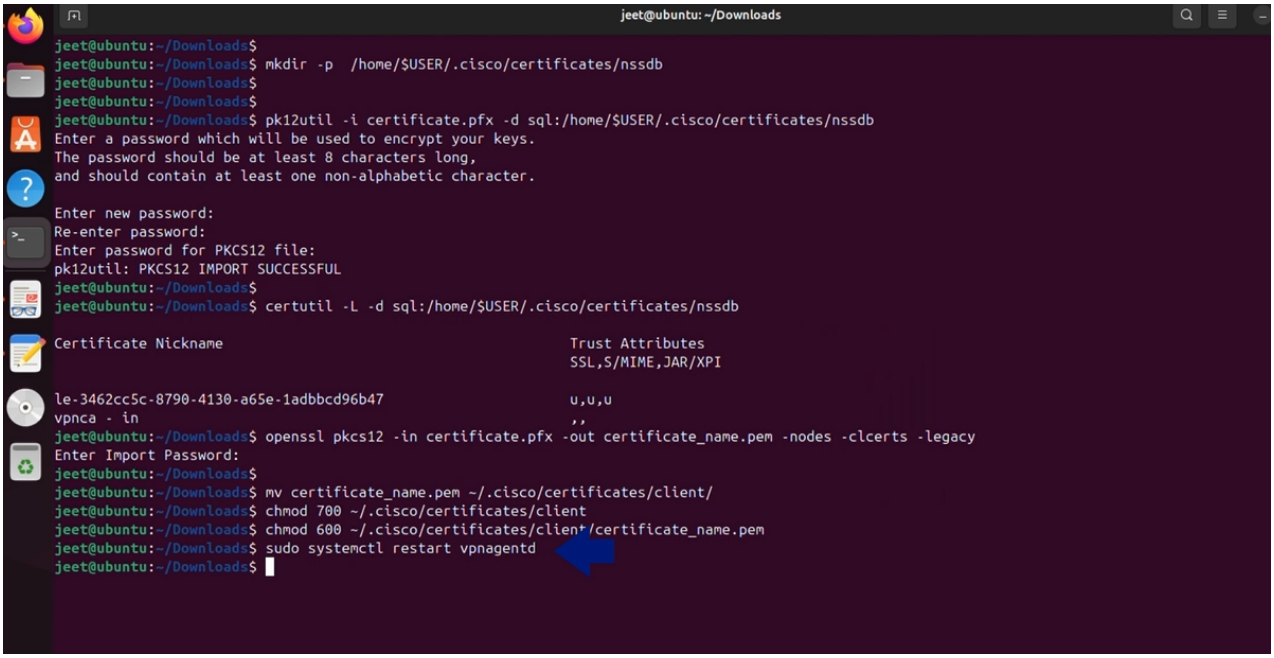
4. Connect to VPN

1.

Restart the certificate

Restart the **Certificate** by running the following **command**.

a) sudo systemctl restart vpnagentd



2.

Connect to Cisco Secure Client

Connect to the **Cisco Secure Client**. Enter **sconnect.nic.in** as the server address and enter your **username** and **password**.