


# Configuring Cisco Any Connect Secure Mobility Client

Manual: Configuring Cisco AnyConnect Client in RedHat

**Platform:**  RedHat

**Audience:**  NIC VPN Users

**Date:**  November 2025

---

# 1. Download & Extract

---

## 1.

### Download DSC

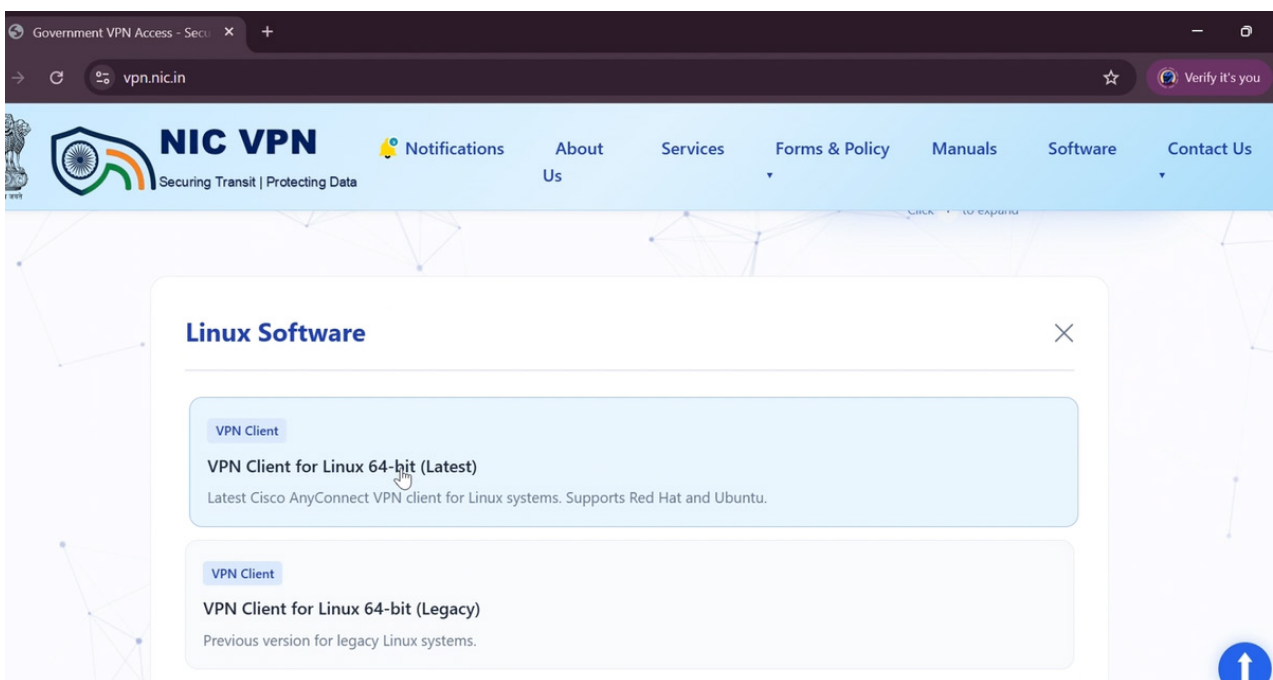
Download the DSC mailed to user by VPN Support (vpnservices@nic.in), save it on user computer.

---

## 2.

### Download Cisco AnyConnect Client

Download Cisco any connect secure mobility client through <https://vpn.nic.in>

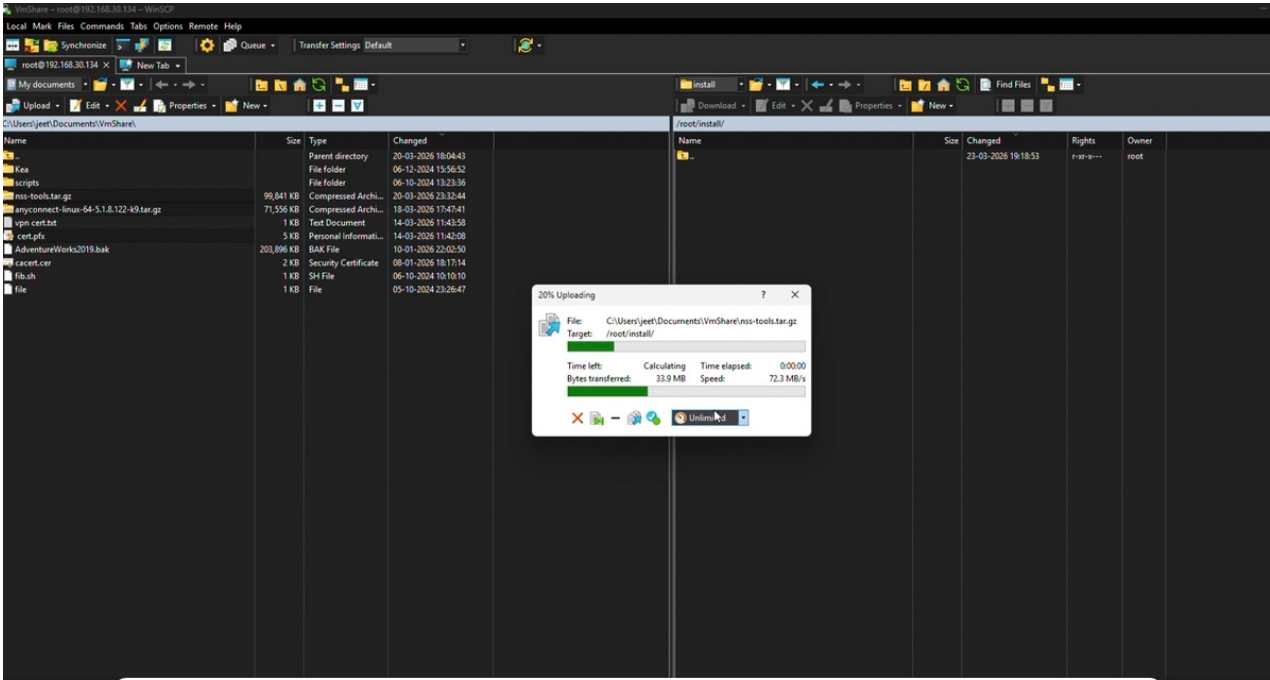


### 3.

#### Uploading Files to the server

Use **WinSCP** and upload the following files to the **server**.

- Certificate PFX file
- Cisco anyconnect client
- Nss-tool package



## 2. Tool Installation

1.

### Install the cisco anyconnect client

Run the following **commands** one by one for the **installation**:

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

```
root@localhost:~/install
[root@localhost ~]# mkdir install
[root@localhost ~]# ls
anaconda-ks.cfg  install
[root@localhost ~]# cd install/
[root@localhost install]# ls
anyconnect-linux-64-5.1.8.122-k9.tar.gz  cert.pfx  nss-tools.tar.gz
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# tar -xvf anyconnect-linux-64-5.1.8.122-k9.tar.gz
```

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

```
root@localhost:~/install/cisco-secure-client-linux64-5.1.8.122/vpn
root@localhost install]# ls
anyconnect-linux-64-5.1.8.122-k9.tar.gz  cert.pfx  cisco-secure-client-linux64-5.1.8.122  nss-tools.tar.gz
root@localhost install]# cd cisco-secure-client-linux64-5.1.8.122/vpn/
root@localhost vpn]#
```

#### c) ./vpn\_install.sh

```
rcwebhelper
AnyConnectLocalPolicy.xsd
AnyConnectProfile.xsd
fom.so
:cisco-secure-client.directory
:cisco-secure-client.menu
:cisco_secure_client_uninstall.sh
[root@localhost vpn]# ./vpn_install.sh

libacciscssl.so
libaccurl.so.4.8.0
libacdownloader.so
libacfeedback.so
libacruntime.so
libacwebhelper.so
libboost_atomic.so

libboost_regex.so
libboost_system.so
libboost_thread.so
libvpnagentutilities.so
libvpnapi.so
libvpncommoncrypt.so
libvpncommon.so

manifesttool_vpn
OpenSource.html
resources
update.txt
VeriSignClass3PublicPrimaryCertificationAuthority-G5.pem
vpn
vpnagentd
```

#### d) cd ../../

```
Please wait while Cisco Secure Client is being installed...
Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory
p: cannot create regular file '/usr/share/icons/hicolor/48x48/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/64x64/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/96x96/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/128x128/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/256x256/apps/cisco-secure-client.png': No such file or directory
Starting Cisco Secure Client Agent...
Exiting now.
root@localhost vpn]# cd ../../
```

#### e) restorecon -v /etc/systemd/system/vpnagentd.service

```
Please wait while Cisco Secure Client is being installed...
Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory
p: cannot create regular file '/usr/share/icons/hicolor/48x48/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/64x64/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/96x96/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/128x128/apps/cisco-secure-client.png': No such file or directory
p: cannot create regular file '/usr/share/icons/hicolor/256x256/apps/cisco-secure-client.png': No such file or directory
Starting Cisco Secure Client Agent...
Exiting now.
root@localhost vpn]# cd ../../
root@localhost install]# restorecon -v /etc/systemd/system/vpnagentd.service
```

#### f) systemctl status vpnagentd

```
root@localhost vpn]# cd ../../
root@localhost install]# restorecon -v /etc/systemd/system/vpnagentd.service
labeled /etc/systemd/system/vpnagentd.service from system_u:object_r:default_t:s0 to system_u:object_r:systemd_unit_file_t:s0
root@localhost install]# systemctl status vpnagentd
vpnagentd.service - Cisco Secure Client - AnyConnect VPN Agent
Loaded: loaded (/etc/systemd/system/vpnagentd.service; disabled; vendor preset: disabled)
Active: inactive (dead)
root@localhost install]#
root@localhost install]# systemctl enable --now vpnagentd
Created symlink /etc/systemd/system/multi-user.target.wants/vpnagentd.service → /etc/systemd/system/vpnagentd.service.
root@localhost install]#
```

## 2.

### Check if the service has been active

Run the following **command** to check if the service is **active**:

#### a) `systemctl status vpnapagentd`

```
root@localhost:~# install
cisco-secure-client.menu      libacwebhelper.so          libvpnccommoncrypt.so     vpn
cisco_secure_client_uninstall.sh libboost_atomic.so        libvpnccommon.so         vpnapagentd
[root@localhost vpn]# ./vpn_install.sh
Installing Cisco Secure Client...
Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively,
LA"). You also acknowledge and agree that you have read the "Cisco Privacy Statement".

If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. I
a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provid
stomer with access to all relevant terms.

The latest version of documents can be found at the following locations.
- Cisco End User License Agreement: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html
- Applicable Product Specific Terms: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html
- Cisco Privacy Statement: https://www.cisco.com/c/en/us/about/legal/privacy-full.html
Do you accept the terms in the license agreement? [y/n] y
You have accepted the license agreement.
Please wait while Cisco Secure Client is being installed...
Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory
cp: cannot create regular file '/usr/share/icons/hicolor/48x48/apps/cisco-secure-client.png': No such file or directory
cp: cannot create regular file '/usr/share/icons/hicolor/64x64/apps/cisco-secure-client.png': No such file or directory
cp: cannot create regular file '/usr/share/icons/hicolor/96x96/apps/cisco-secure-client.png': No such file or directory
cp: cannot create regular file '/usr/share/icons/hicolor/128x128/apps/cisco-secure-client.png': No such file or directory
cp: cannot create regular file '/usr/share/icons/hicolor/256x256/apps/cisco-secure-client.png': No such file or directory
Starting Cisco Secure Client Agent...
Exiting now.
[root@localhost vpn]# cd ../../
[root@localhost install]# restorecon -v /etc/systemd/system/vpnapagentd.service
relabeled /etc/systemd/system/vpnapagentd.service from system_u:object_r:default_t:s0 to system_u:object_r:systemd_unit_file_t:s0
[root@localhost install]# systemctl status vpnapagentd
● vpnapagentd.service - Cisco Secure Client - AnyConnect VPN Agent
   Loaded: loaded (/etc/systemd/system/vpnapagentd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost install]#
[root@localhost install]# systemctl enable --now vpnapagentd
Created symlink /etc/systemd/system/multi-user.target.wants/vpnapagentd.service → /etc/systemd/system/vpnapagentd.service.

[root@localhost install]#
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# systemctl status vpnapagentd
```

## 3.

### Install the nss-tools packages

Install the **nss-tools** packages and proceed to the next step.

**Note:** For complete installation instructions Click here on [Nss Tools Packages Installation](#).

### 3. Import Certificate (DSC)

---

#### 1.

#### Create the following directories

Run the following **commands** one by one to create the **directories**.

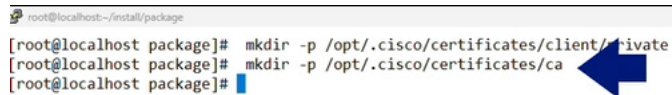
##### a) `mkdir -p /opt/.cisco/certificates/client/private`

```
root@localhost:~/install/package
root@localhost package]# mkdir -p /opt/.cisco/certificates/client/private
root@localhost package]#
```



##### b) `mkdir -p /opt/.cisco/certificates/ca`

```
root@localhost:~/install/package
[root@localhost package]# mkdir -p /opt/.cisco/certificates/client/private
[root@localhost package]# mkdir -p /opt/.cisco/certificates/ca
[root@localhost package]#
```



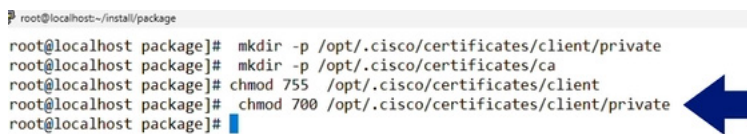
##### c) `chmod 755 /opt/.cisco/certificates/client`

```
root@localhost:~/install/package
root@localhost package]# mkdir -p /opt/.cisco/certificates/client/private
root@localhost package]# mkdir -p /opt/.cisco/certificates/ca
root@localhost package]# chmod 755 /opt/.cisco/certificates/client
```



##### d) `chmod 700 /opt/.cisco/certificates/client/private`

```
root@localhost:~/install/package
root@localhost package]# mkdir -p /opt/.cisco/certificates/client/private
root@localhost package]# mkdir -p /opt/.cisco/certificates/ca
root@localhost package]# chmod 755 /opt/.cisco/certificates/client
root@localhost package]# chmod 700 /opt/.cisco/certificates/client/private
root@localhost package]#
```



## 2.

### Install the certificates and keys

Install the **Certificate** by running the following **commands**.

**Note:** Enter the PKCS12 and Import password whenever its required during installation.

#### a) pk12util -i cert.pfx -d sql:/etc/pki/nssdb

```
root@localhost:~/install
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# pk12util -i cert.pfx -d sql:/etc/pki/nssdb
Enter password for PKCS12 file: █
```

#### b) openssl pkcs12 -in cert.pfx -out root\_ca.pem -nodes -cacerts

```
root@localhost install]#
root@localhost install]# pk12util -i cert.pfx -d sql:/etc/pki/nssdb
Enter password for PKCS12 file:
pk12util: PKCS12 IMPORT SUCCESSFUL
root@localhost install]#
root@localhost install]#
root@localhost install]# openssl pkcs12 -in cert.pfx -out root_ca.pem -nodes -cacerts
Enter Import Password: █
```

#### c) certutil -A -n "VPN\_Root\_CA" -t "CT,C,C" -i root\_ca.pem -d sql:/etc/pki/nssdb

```
Enter Import Password:
Enter password for PKCS12 file:
Enter Import Password:
root@localhost install]# certutil -A -n "VPN_Root_CA" -t "CT,C,C" -i root_ca.pem -d sql:/etc/pki/nssdb
root@localhost install]# █
```

#### d) openssl pkcs12 -in cert.pfx -clcerts -nokeys -out vpn\_client.pem

```
Enter Import Password:
Enter password for PKCS12 file:
root@localhost install]# openssl pkcs12 -in cert.pfx -out root_ca.pem -nodes -cacerts
Enter Import Password:
root@localhost install]# certutil -A -n "VPN_Root_CA" -t "CT,C,C" -i root_ca.pem -d sql:/etc/pki/nssdb
root@localhost install]# openssl pkcs12 -in cert.pfx -clcerts -nokeys -out vpn_client.pem █
```

#### e) mv vpn\_client.pem /opt/.cisco/certificates/client/

```
Enter Import Password:
root@localhost install]#
root@localhost install]#
root@localhost install]# mv vpn_client.pem /opt/.cisco/certificates/client/ █
```

#### f) openssl pkcs12 -in cert.pfx -nocerts -nodes -out vpn\_client.key

```
root@localhost install]#
root@localhost install]# mv vpn_client.pem /opt/.cisco/certificates/client/
root@localhost install]# openssl pkcs12 -in cert.pfx -nocerts -nodes -out vpn_client.key
Enter Import Password: █
```

#### g) mv vpn\_client.key /opt/.cisco/certificates/client/private/vpn\_client.key

```
root@localhost install]# openssl pkcs12 -in cert.pfx -nocerts -nodes -out vpn_client.key
Enter Import Password:
root@localhost install]# mv vpn_client.key /opt/.cisco/certificates/client/private/vpn_client.key
root@localhost install]# █
```

#### h) chmod 644 /opt/.cisco/certificates/client/vpn\_client.pem

```
Enter Import Password:
root@localhost install]# mv vpn_client.key /opt/.cisco/certificates/client/private/vpn_client.key
root@localhost install]# chmod 644 /opt/.cisco/certificates/client/vpn_client.pem
root@localhost install]# █
```

#### i) chmod 600 /opt/.cisco/certificates/client/private/vpn\_client.key

```
root@localhost install]# mv vpn_client.key /opt/.cisco/certificates/client/private/vpn_client.key
root@localhost install]# chmod 644 /opt/.cisco/certificates/client/vpn_client.pem
root@localhost install]# chmod 600 /opt/.cisco/certificates/client/private/vpn_client.key
root@localhost install]#
root@localhost install]# █
```

### 3.

#### Create a user profile

To create a **user profile**, open a **file** by running the following **command**.

a) `vi /opt/cisco/secureclient/vpn/profile/nic_vpn.xml`

```
root@localhost~# install
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# openssl pkcs12 -in cert.pfx -clcerts -nokeys -out vpn_client.pem
Enter Import Password:
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# mv vpn_client.pem /opt/.cisco/certificates/client/
[root@localhost install]# openssl pkcs12 -in cert.pfx -nocerts -nodes -out vpn_client.key
Enter Import Password:
[root@localhost install]# mv vpn_client.key /opt/.cisco/certificates/client/private/vpn_client.key
[root@localhost install]# chmod 644 /opt/.cisco/certificates/client/vpn_client.pem
[root@localhost install]# chmod 600 /opt/.cisco/certificates/client/private/vpn_client.key
[root@localhost install]#
[root@localhost install]# vi /opt/cisco/secureclient/vpn/profile/nic_vpn.xml
```

I

#### 4.

Paste the following content in the above file

After opening the file **paste** the following the **command** in the above file.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile>
<ClientInitialization>
<AutomaticCertSelection>true</AutomaticCertSelection>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>true</CertificateStoreOverride>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>sconnect.nic.in</HostName>
<HostAddress>sconnect.nic.in</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

```
root@localhost:~/install
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile>
  <ClientInitialization>
    <AutomaticCertSelection>true</AutomaticCertSelection>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreOverride>true</CertificateStoreOverride>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>sconnect.nic.in</HostName>
      <HostAddress>sconnect.nic.in</HostAddress>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
```

## 4. Connect to VPN

### 1.

#### Restart the service

Restart the Service by running the following command.

##### a) systemctl restart vpncgtd

```
root@localhost:~# install
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# openssl pkcs12 -in cert.pfx -clcerts -nokeys -out vpn_client.pem
Enter Import Password:
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# mv vpn_client.pem /opt/.cisco/certificates/client/
[root@localhost install]# openssl pkcs12 -in cert.pfx -nocerts -nodes -out vpn_client.key
Enter Import Password:
[root@localhost install]# mv vpn_client.key /opt/.cisco/certificates/client/private/vpn_client.key
[root@localhost install]# chmod 644 /opt/.cisco/certificates/client/vpn_client.pem
[root@localhost install]# chmod 600 /opt/.cisco/certificates/client/private/vpn_client.key
[root@localhost install]#
[root@localhost install]# vi /opt/cisco/secureclient/vpn/profile/nic_vpn.xml
[root@localhost install]#
[root@localhost install]# cat /opt/cisco/secureclient/vpn/profile/nic_vpn.xml
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile>
  <ClientInitialization>
    <AutomaticCertSelection>true</AutomaticCertSelection>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreOverride>true</CertificateStoreOverride>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>sconnect.nic.in</HostName>
      <HostAddress>sconnect.nic.in</HostAddress>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# systemctl restart vpncgtd
[root@localhost install]#
```

## 2.

### Connect with vpn service

Run the following **command** to **connect** with the vpn service.

a) `/opt/cisco/secureclient/bin/vpn connect sconnect.nic.in`

```
root@localhost:~# install
[root@localhost install]#
[root@localhost install]# vi /opt/cisco/secureclient/vpn/profile/nic_vpn.xml
[root@localhost install]#
[root@localhost install]# cat /opt/cisco/secureclient/vpn/profile/nic_vpn.xml
<?xml version="1.0" encoding="UTF-8"?>
  <AnyConnectProfiles>
    <ClientInitialization>
      <AutomaticCertSelection>true</AutomaticCertSelection>
      <CertificateStore>All</CertificateStore>
      <CertificateStoreOverride>true</CertificateStoreOverride>
    </ClientInitialization>
    <ServerList>
      <HostEntry>
        <HostName>sconnect.nic.in</HostName>
        <HostAddress>sconnect.nic.in</HostAddress>
      </HostEntry>
    </ServerList>
  </AnyConnectProfile>
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# systemctl restart vpnagentd
[root@localhost install]# systemctl status vpnagentd
● vpnagentd.service - Cisco Secure Client - AnyConnect VPN Agent
   Loaded: loaded (/etc/systemd/system/vpnagentd.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2026-03-23 19:47:21 IST; 6s ago
     Process: 11013 ExecStartPre=/opt/cisco/secureclient/bin/load_tun.sh (code=exited, status=0/SUCCESS)
    Main PID: 11019 (vpnagentd)
      Tasks: 5 (limit: 18572)
     Memory: 21.5M
    CGroup: /system.slice/vpnagentd.service
            └─11019 /opt/cisco/secureclient/bin/vpnagentd -execv_instance

4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: CDefaultPluginHandler File: ../../vpn/Common/Utility/DefaultPluginHandler.cpp Line: 58 Created Default plugin han
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: createThread File: ../../vpn/Common/Utility/Thread.cpp Line: 290 A thread has been successfully created, Referenc
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: OnTimerExpired File: ../../vpn/Agent/MainThread.cpp Line: 7707 Applying Automatic VPN Policy
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: startParser File: ../../vpn/Common/Xml/CVCParser.cpp Line: 188 Invoked Function: xmlCreateFileParserCtx Retur
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: LoadSettingsFromXmlFile File: ../../vpn/PhoneHome/PhoneHomeAgent.cpp Line: 626 Invoked Function: XmlParser::parse
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: LoadFileToMap File: ../../vpn/PhoneHome/PhoneHomeAgent.cpp Line: 2267 Can't open file /opt/cisco/secureclient/Cus
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: determinePublicAddrCandidateFromDefRoute File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 3094 Invoked Func
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: updatePotentialPublicAddresses File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 3228 Invoked Function: CHos
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Customer Experience Feedback Module: Enabled Endpoint ID: a49485ce806e2550b0b06b714acb2e812cf9a5a Customer ID: release
4ar 23 19:47:21 localhost.localdomain csc_vpnagent[11019]: Function: Start File: ../../vpn/PhoneHome/PhoneHomeAgent.cpp Line: 773 Starting Customer Experience Feedback module
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# /opt/cisco/secureclient/bin/vpn connect sconnect.nic.in
```

### 3. To Disconnect with vpn services

Run the following **command** to disconnect with the vpn service.

a) `/opt/cisco/secureclient/bin/vpn disconnect`

```
root@localhost:~# install
>> Please enter your username and password.
Username: Vpn Support/1132108000600018AA5
Password:
>> notice: Please respond to banner.
Kindly upgrade Windows7, Windows8 and Windows8.1 as Microsoft has stopped support and patches for these operating systems are no longer released, leaving them vulnerable. VPN service
not be available on Windows7, Windows8 and Windows8.1 clients from March 31, 2024.Select Continue/Accept to logon..
accept? [y/n]: y
>> state: Connecting
>> notice: Establishing VPN session...
The Cisco Secure Client - Downloader is analyzing this computer. Please wait...
Initializing the Cisco Secure Client - Downloader...
The Cisco Secure Client - Downloader is performing update checks...
>> notice: The Cisco Secure Client - Downloader is performing update checks...
>> notice: Checking for profile updates...
>> state: Disconnected

Downloading Cisco Secure Client VPN Profile. Please wait...
Time Left: 0 secs (2.7 KB of 2.7 KB copied)
Transfer rate: 63.7 KB/Sec
Downloading Cisco Secure Client VPN Profile. Please wait...
Time Left: 0 secs (2.7 KB of 2.7 KB copied)
Transfer rate: 19.1 KB/Sec
Downloading Cisco Secure Client VPN Profile. Please wait...
Time Left: 0 secs (2.7 KB of 2.7 KB copied)
Transfer rate: 5.73 KB/Sec
Downloading Cisco Secure Client VPN Profile. Please wait...
Time Left: 0 secs (2.7 KB of 2.7 KB copied)
Transfer rate: 1.72 KB/Sec
The Cisco Secure Client - Downloader update checks have been completed.
Please wait while the VPN connection is established...
[root@localhost install]#
[root@localhost install]#
[root@localhost install]# ip -br a
lo                UNKNOWN    127.0.0.1/8  ::1/128
ens160            UP        192.168.30.134/24  fe80::20c:29ff:feb7:265/64
csicotun0        UNKNOWN    10.26.116.10/8  fe80::ce0d:3c3b:4522:4399/126  fe80::ef83:9c35:b080:2710/64
[root@localhost install]#
[root@localhost install]# /opt/cisco/secureclient/bin/vpn disconnect
```