iVPN AnyConnect Client Installation

Version 2.4

ASX Telecommunications Group

Publication Date: Jan 2015
Review Date: Apr 2017
Property of: ASX Connectivity Team

This document describes the process of installing Cisco AnyConnect client used in the ASX iVPN environment for functioning Linux and Windows clients.

Cisco AnyConnect Secure Mobility Client 3.1 supports the following operating systems:

Operating System	Version
Windows	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 x86(32-bit) and x64(64-bit)
	Windows Vista x86(32-bit) and x64(64-bit)
	Windows XP SP3 x86(32-bit) Windows XP SP2 x64 (64-bit)
Linux	Red Hat 6 (32-bit)* and (64-bit)
	Ubuntu 11.10 (32-bit only)* and Ubuntu 12.x (64-bit)

There are further requirements for Linux platforms such as libstdc++ users, zlib and dtk/gdk. Please visit the link below for further details:
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect31/release/notes/anyconnect31rn.html
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect31/feature/guide/anyconnect31features.html

1. Download and install the relevant client software from https://asxonline.com/intvpn and install client, see Appendix A for details

2. Create certificate request by emailing ASX Customer Technical Support (CTS) – cts@asx.com.au and submit the following details:

First Name	Last Name	Email	ParticipantID	Username	Project
Project Code	Full Name	email@address.com	Company Name	CompanyName and Project Code (see example)	Project Code

Note **Please use unique username for each certificate request**
You are required to have one certificate for each ASX application (per Windows Profile User per machine, same for Linux)

Important - **Choose a Project Code as your First Name in the request** based on the application requirement, this value should match the "Project" field and this is essential for a successful connection. If you are not sure please consult with ASX Customer Technical Support on 1800 663 053. Please also use a generic/group email address in case the certificate renewal is handled by another person / team.

Table 1.1 - Project Code for ASX Applications		
ASX Application	**Project Code**	**Username Req'd**
CHESS	IVPNCHESS	N
PTE/ASX BEST/DCS/FTE/ETE/Genium Clearing/CDE & CDE plus – EQUITY	IVPNPTE	Y
Reference Service	IVPNDSS	Y
Comm News	IVPNIDS	N
SFE Test/PFG/ CDE & CDE plus - DERIVATIVE	IVPNQAOEI	N

Note: These services "ASX Best, DCS, FTE, ETE, Genium Clearing" fall under this "PTE"

Example

First Name	Last Name	Email	ParticipantID	Username	Project
IVPNCHESS	Andrew Smith	a.smith@companyx.com	CompanyX	CompanyXCHESS	IVPNCHESS
IVPNPTE	James Jones	j.jones@companyx.com	CompanyX	CompanyXPTE	IVPNPTE

3. You will get an email from Enterprise PKI Team (noreply@symantec.com) once ASX Customer Technical Support create the iVPN user. Please refer to the Step by Step Enrolment Guide (https://www.asxonline.com/intradoc-cgi/groups/public/documents/participantapplicationkitsfe/asx_046515.pdf) to complete your certificate enrolment.

4. Please refer to Appendix A for Cisco AnyConnect client installation and verification of your certificates

5. Open AnyConnect, depending on the platform and version you should see a similar window as below:

Figure 1 Windows Client

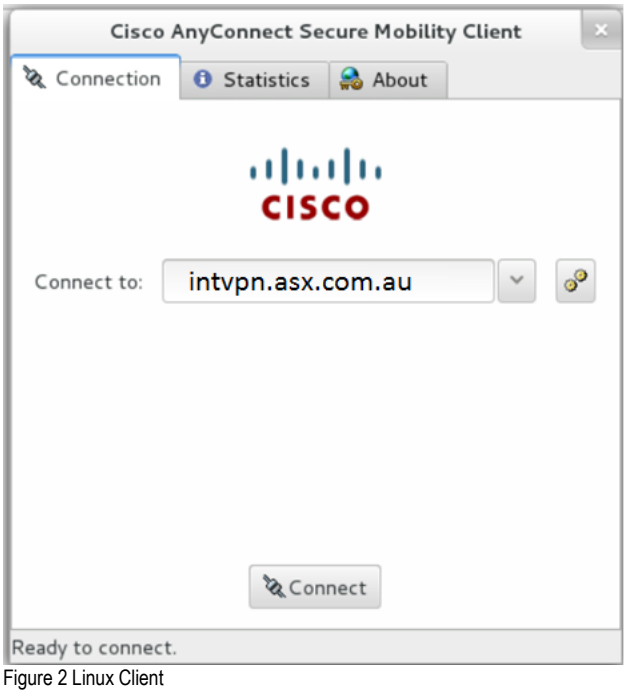


Figure 2 Linux Client

6. Type in intvpn.asx.com.au in the connection box and click connect, you should then see the Welcome message similar to below:

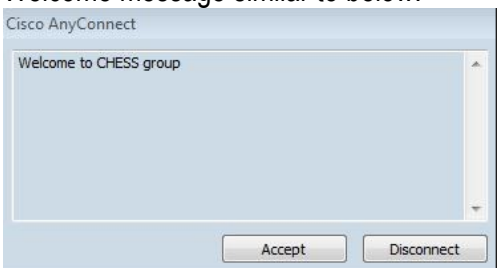


Figure 3 Windows Client Welcome Banner

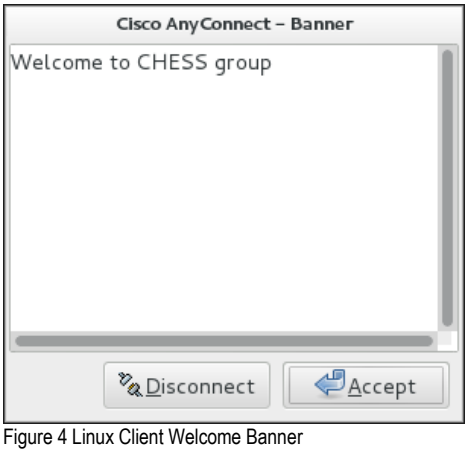


Figure 4 Linux Client Welcome Banner

7. Click Accept and now you are connected.

Note: For **PTE & Reference Service**, you need to fill in your user details given by CTS.

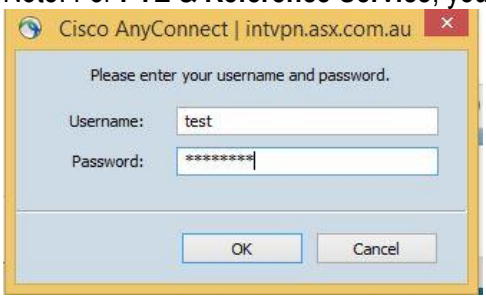


Figure 5 Windows Client Connected

Figure 6 Linux Client Connected

8. You can also verify this by checking the local IP address.

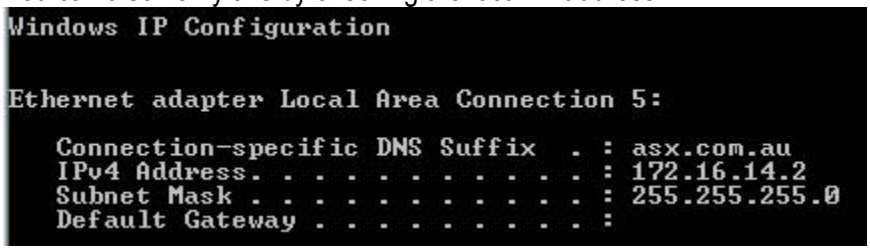


Figure 7 Windows Client IP check

```
[root@localhost ~]# ifconfig
cscotun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1406
        inet 172.16.14.2  netmask 255.255.255.0  destination 172.16.14.2
        inet6 fe80::cae4:73b5:d5f8:d642  prefixlen 128  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500
```

Figure 8 Linux Client IP check

Appendix A – client software download and installation

Download your Cisco AnyConnect VPN client form the link below

https://www.asxonline.com/intvpn

The page looks similar to below:

Cisco AnyConnect VPN client

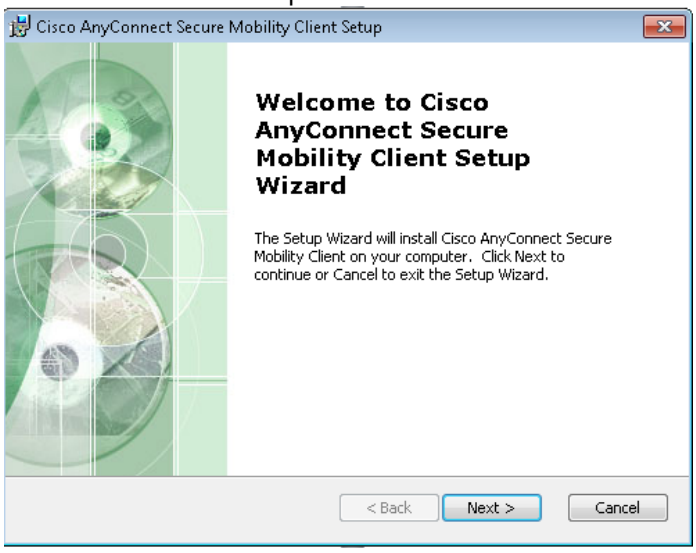
32 / 64 Bit Windows Client
Release notes 3.1.05152
Anyconnect-win-3.1.05152-pre-deploy-k9.msi (4.1 MB)

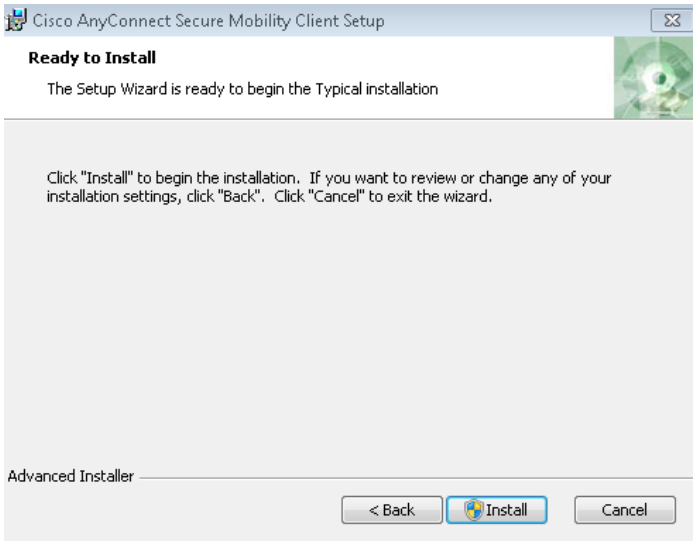
32 Bit Linux Client:
Release notes 3.1.05152
anyconnect-predeploy-linux-3.1.05152-k9.tar.gz (7.6MB)

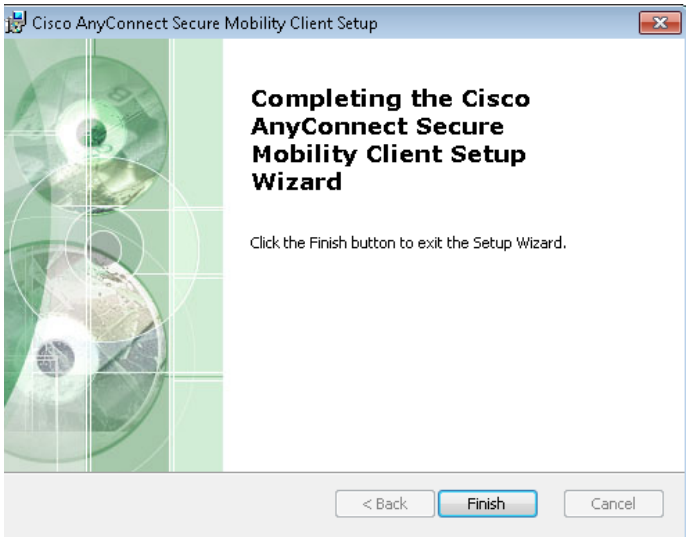
64 Bit Linux Client
Release notes 3.1.05152
anyconnect-predeploy-linux-64-3.1.05152-k9.tar.gz (7.7MB)

Please proceed A.1 for Windows client and A.2 for Linux client

A.1 Windows Client setup:







A.2 Linux Client setup:

Linux client setup:
Note – you may need additional packages in order to have the client installed, please consult with your Linux administrator for further assistance.

```
gunzip anyconnect-predeploy-linux-64-3.1.05152-k9.tar.gz
tar -xvf anyconnect-predeploy-linux-64-3.1.05152-k9.tar
cd anyconnect-3.1.05152/vpn
./vpn_install.sh
*accept licence*



[root@localhost anyconnect-3.1.05152]# cd vpn/
[root@localhost vpn]# ls
ACManifestVPN.xml            cisco-anyconnect.menu    libvpnapi.so
OpenSource.html                                           vpnagentd_init
AnyConnectLocalPolicy.xsd    libacciscocrypto.so      libvpncommoncrypt.so
pixmaps                                                   vpndownloader
AnyConnectProfile.xsd        libacciscossl.so         libvpncommon.so
update.txt                                                vpndownloader-cli
anyconnect_uninstall.sh      libaccurl.so.4.2.0       libvpnipsec.so
VeriSignClass3PublicPrimaryCertificationAuthority-G5.pem  vpn_install.sh
cisco-anyconnect.desktop     libacfeedback.so         license.txt
vpn                                                       vpnui
cisco-anyconnect.directory   libvpnagentutilities.so  manifesttool
vpnagentd                                                 vpn_uninstall.sh
[root@localhost vpn]# ./vpn_install.sh
Installing Cisco AnyConnect Secure Mobility Client...
Supplemental End User License Agreement for Cisco Systems AnyConnect Secure Mobility and other related
Client Software

IMPORTANT: READ CAREFULLY
This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the
Software Product licensed under the End User License Agreement ("EULA") between You ("You" as used herein
means You and the business entity you represent) and Cisco (collectively, the "Agreement"). Capitalized
terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent
that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and
conditions of this SEULA will take precedence.
In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to
comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING
THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY
THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF
THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL
OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN
MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER
PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30
DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END
USER PURCHASER.
```

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following ("Software"):
- Cisco AnyConnect Secure Mobility Client
- Cisco AnyConnect VPN Client
- Cisco AnyConnect Profile Editor
- Cisco AnyConnect Host Scan (HostScan)
- Cisco AnyConnect Diagnostics and Reporting Tool (DART)
- Cisco SSL VPN Client
- Cisco VPN Client
- Cisco Secure Desktop
- Smart Tunnels
- Port Forwarding
- Additional SSL VPN delivered applets

Definitions
For purposes of this SEULA, the following definitions apply:
"Endpoint" means a computer, smartphone or other mobile device used in conjunction with any of the Software.
"Network Access Manager Module" means a separate module in the Cisco AnyConnect Secure Mobility Client with IEEE 802.1X authentication functionality to manage wired and wireless network connections.
"Non-personal Information" means technical and related information that is not personally identifiable, including, but not limited to, the operating system type and version, origin and nature of identified malicious system threats, and the Software modules installed on an Endpoint device.
"Personal Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

Additional License Terms and Conditions
1. Installation and Use on Unlimited Number of Endpoint Devices
Cisco hereby grants You the right to install and use any of the Software listed above in this SEULA on an unlimited number of Endpoint devices, provided that, except with respect to the Network Access Manager Module as described in Section 2 below, each of those Endpoint devices must use the Software only to connect to Cisco equipment. These license grants are subject to export restrictions in the EULA and to the network equipment license restrictions in Section 3 below. You may make one copy of the Software for each such Endpoint device and a reasonable number of backup copies for the purpose of installing the Software on that Endpoint device.
2. Cisco AnyConnect Network Access Manager Module
The Network Access Manager Module, as described in the Cisco AnyConnect Secure Mobility Client Administrator Guide, may be used by You in conjunction with non-Cisco wired and wireless equipment for the purpose of connecting to non-Cisco network equipment. Support services (including Technical Assistance or TAC support) are only available if You have an active support contract for Cisco Products used in conjunction with the Network Access Manager Module. Support services will not be provided directly to your end users by Cisco.
3. Cisco Network Equipment and Hosted Service License Entitlements and Restrictions
Your use of the Software or specific features thereof with Cisco network equipment shall be subject to license entitlements and restrictions for the applicable Cisco network equipment or hosted services. Please consult Your administrator guide for the applicable Cisco network equipment or hosted services for the relevant license entitlements and restrictions.

```
4. Distribution to Third Party Business Partners and Customers
You may copy and distribute the Software to your third party business partners and customers solely and
exclusively for the purposes of accessing your Cisco equipment, provided that You shall remain responsible
for compliance with the EULA and this SEULA by each such third party business partner and customer. Each
such distribution of the Software to a third party must be accompanied by a copy of the EULA and this SEULA.
5. No Support to Third Party Business Partners or Customers
Cisco will not provide end-user support (including Technical Assistance or TAC support) to any third party
business partner or customer that receives the Software in accordance with Section 4 hereof. You shall be
responsible for providing all support to each such third party.
6. Effect of Termination on Third Party Business Partners or Customers
In the event of termination of the Agreement, You must use commercially reasonable efforts to notify the
third party business partner or customer to whom You have distributed the Software that their rights of
access and use of the Software have also ceased.
7. Data, Information and Privacy
If You agree to this Agreement, You consent to Cisco's collection, use, processing and storage of Personal
Information and Non-personal Information, and the transfer of Personal Information and Non-personal
Information to Cisco, including the transfer of such information to the United States and/or another country
outside the European Economic Area, as described in Cisco's Privacy Statement and the AnyConnect Secure
Mobility Client Supplement, available at http://www.cisco.com/web/siteassets/legal/privacy.html.

Description of Other Rights and Obligations
Please refer to the Cisco Systems, Inc. End User License Agreement.


Do you accept the terms in the license agreement? [y/n] y
You have accepted the license agreement.
Please wait while Cisco AnyConnect Secure Mobility Client is being installed...
Removing previous installation...
mv: cannot stat '/opt/cisco/vpn/*.log': No such file or directory
Starting Cisco AnyConnect Secure Mobility Client Agent...
Done!
[root@localhost vpn]#
```

Appendix B – Frequent Issues and Solutions

B.1 - Windows client

Issue: The VPN Client indicates Certification Validation Failure

Possible solution: After installation, select “my personal certificate” and enable the certificate for "Client Authentication" in the advanced properties for the certificate.

B.2 – Linux client

Issue: The VPN Client indicates Certification Validation Failure

Possible solution (this applies to Debian Distro and may apply to RHEL): Using debian, user had to symlink libnssckbi.so from /usr/lib/x86_64-linux-gnu/nss/libnssckbi.so to /usr/lib/x86_64-linux-gnu/libnssckbi.so. Without the symlink, the vpnclient cannot validate the certificate.

.