UNIVERSITY of HOUSTON

UNIVERSITY INFORMATION TECHNOLOGY

VPN SERVICE MODEL

A RESEARCH ON A VPN SERVICE MODEL

Table of Contents

1.0 Introduction

1.1 Objective

The objective of this research is to provide a VPN service model, based on best practices of the industry state of the art for our specific application, which is the University Academic System.

1.2 Methodology

The approach of this research involved searching for the best implementations of VPN services in the Top Universities in the US, UK and Australia. Based on categories such as: Security Implementation, VPN services offered and Documentation, a couple of schools were identified as the obvious best. They Are:

a. Stanford University
b. New York University
c. University of Cambridge
d. University of Edinburgh
e. La Trobe University
f. University of Auckland

Of these Universities, Stanford university was the best in all three categories. This model was developed using Stanford's implementation as a template and supplemented with other school's features.

1.3 Summary

The state of the art of today's VPN service model for Academic institutions are shown in *figure 1* below. Two types of services offered, the Split-Tunnel and the Non-Split Tunnel, each used by different college departments based on their needs and utility. In all schools researched, Cisco AnyConnect VPN client was used to simultaneously provide both types of tunneling service. With Two Factor authentication used as a security implementation to avoid unauthorized access.

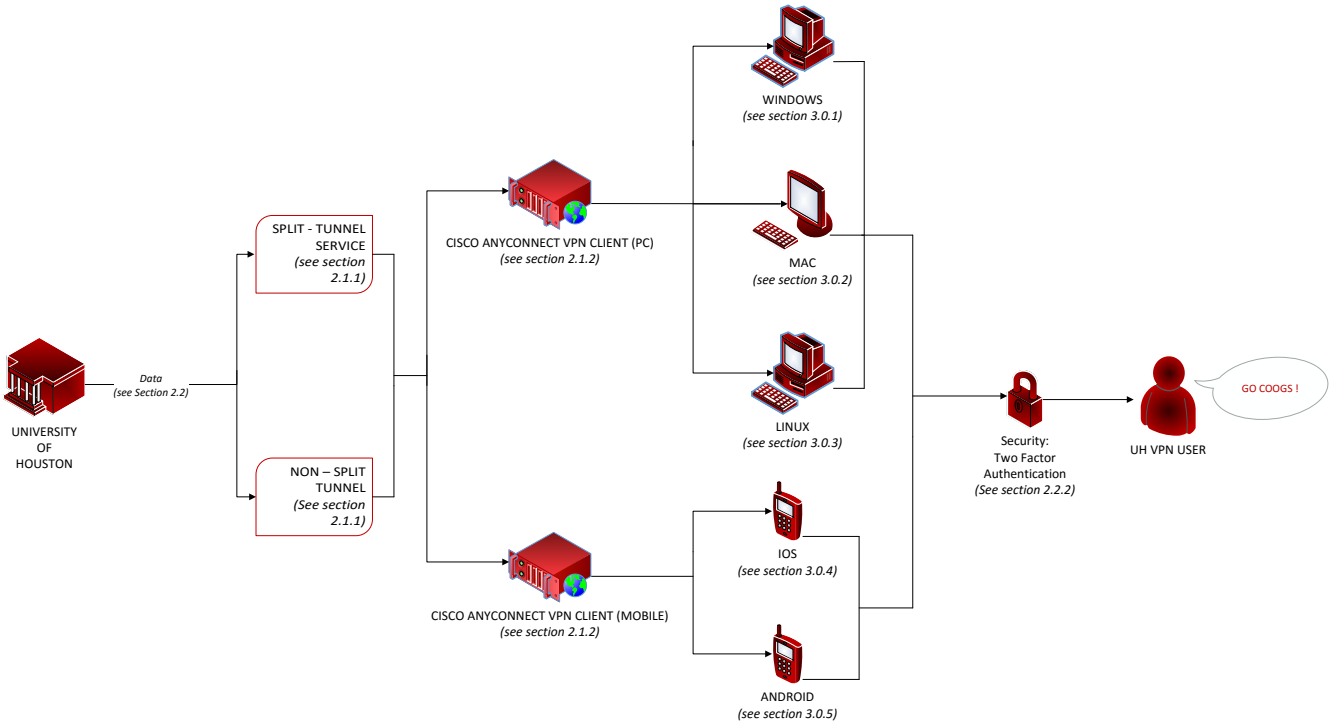


Figure 1: VPN Service Model

To implement this VPN service model would result in three phases *(see Figure 2 below)*;

a. **Setup Phase**: Configuration of the VPN client, Security Implementations, Servers and other back-end Setup.
b. **Installation Phase**: Testing and developing instructions for VPN client installation and Two-factor Authentication.
c. **Support Phase**: Developing documentation for Troubleshooting, FAQs and maintenance model through the Help request workflow.

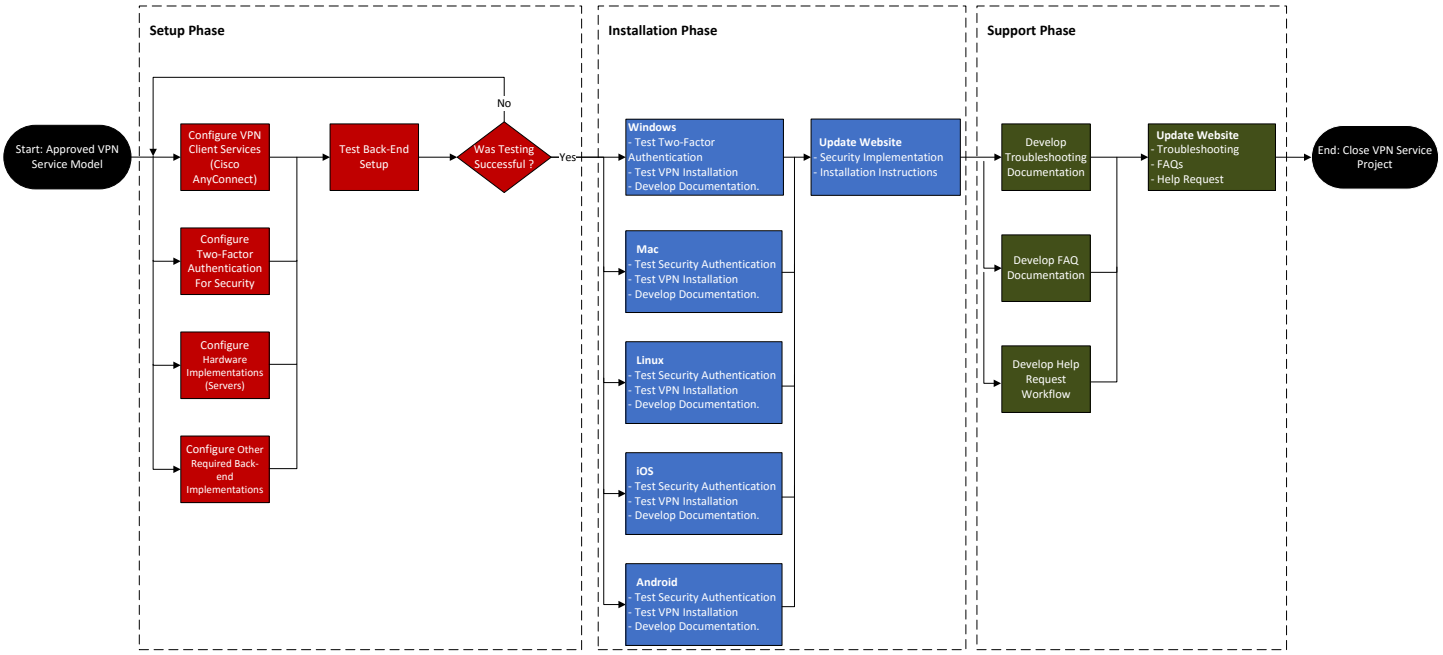


Figure 2: VPN Setup Workflow

The following chapters of this report provides a template for each of these phases.

Chapter 2 (Setup Phase Template): defines the service types in more detail, provides a data risk classification and the Two-Factor authentication options.
Chapter 3 (Installation Phase Template): Installation Instructions for the various Operating systems.
Chapter 4 (Support Phase Template): Template for Troubleshooting documentations and Help Request workflow.

1.4 Research Insights

From the research of the VPN service model, the philosophy used by some of the most successful VPN service Implementations (e.g. Stanford University) is to make the Installation phase as clear as can possibly be to the End User, for achieving this would lower the demand for Help and Support. And this was achieved using two techniques;

a. **A Cross-Platform VPN Client**; of which Cisco AnyConnect Client was widely implemented across Universities.
b. **A robust website design;** Containing a detailed step by step instruction with images on how to install the VPN service for supported operating systems.

These two techniques worked in unison by acknowledging that the VPN Target Users (students, faculty and Staff) are most likely non-technical and thereby technical jargons and vague illustrations were avoided and procedural image laden instructions used.

2.0 Setup Phase Template

2.1 Configuration of VPN Client

2.1.1 VPN Service Types

Split Tunnel VPN Service

Split tunneling is a computer network concept which allows users to access different security domains (e.g. The internet) and a local LAN or WAN at the same time, using the same or different network connectors, though the simultaneous use of a LAN or wireless Network. With configurations such as Split-Exclude and Split-Include, the latter which allows only traffic destined to a domain and is currently used by UH VPN setup (vpn.uh.edu).

For example; Suppose a user utilizes a remote Access VPN software client connecting to a university of Houston (uh.edu) network through a home installed network. The User split tunneling allows the connection to UH file Servers, Mail servers and database Servers and other servers through the VPN network. When the user connects to other websites, the connection request goes directly out of the Hone network's gateway.

One advantage is the conservation of Bandwidth as all internet traffic does not pass through the VPN server. The disadvantage is the vulnerability to the Security threats.

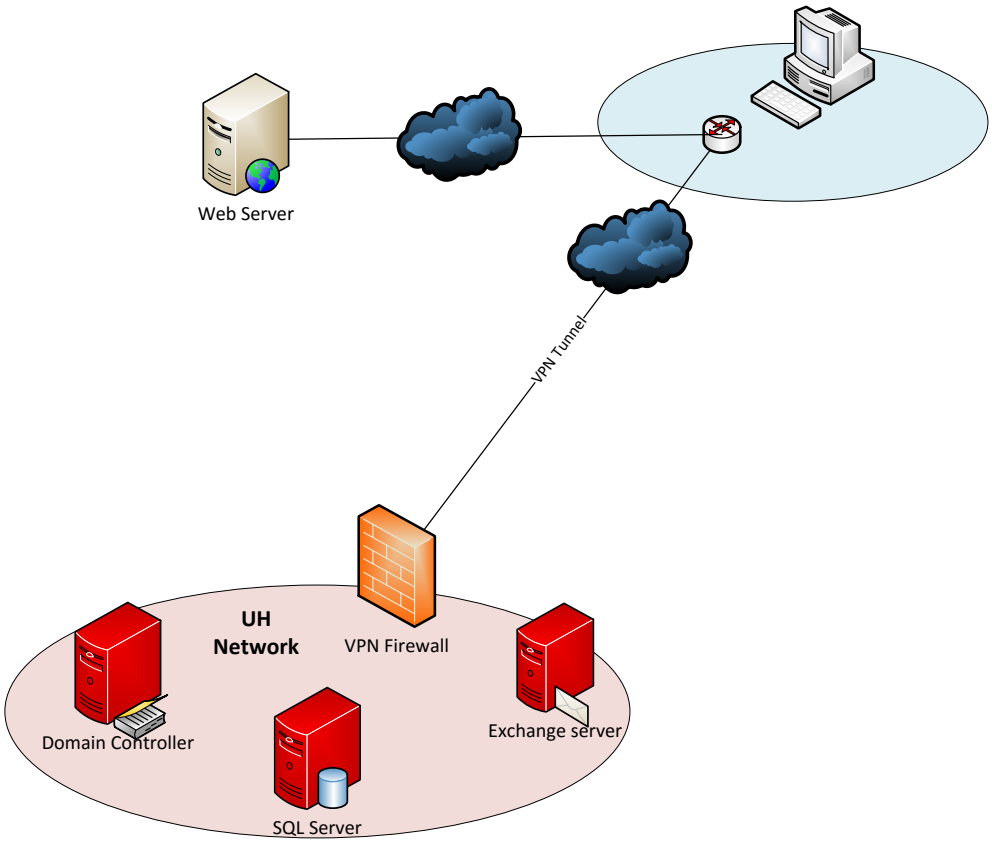


Figure 3: Split- Tunnel VPN Service

Non-Split Tunnel VPN Service

Non-Split tunneling is the contrast to split tunneling and encrypts all user domain accessed. For example, suppose a user utilizes a remote Access VPN connecting to the UH Network at home, a non-split VPN service would flow internet traffic through the UH VPN servers.

The advantages are improved security and access to databases (such as library catalogs), the disadvantage though is the increased bandwidth flowing through the VPN server and isolation of devices installed in your local network.

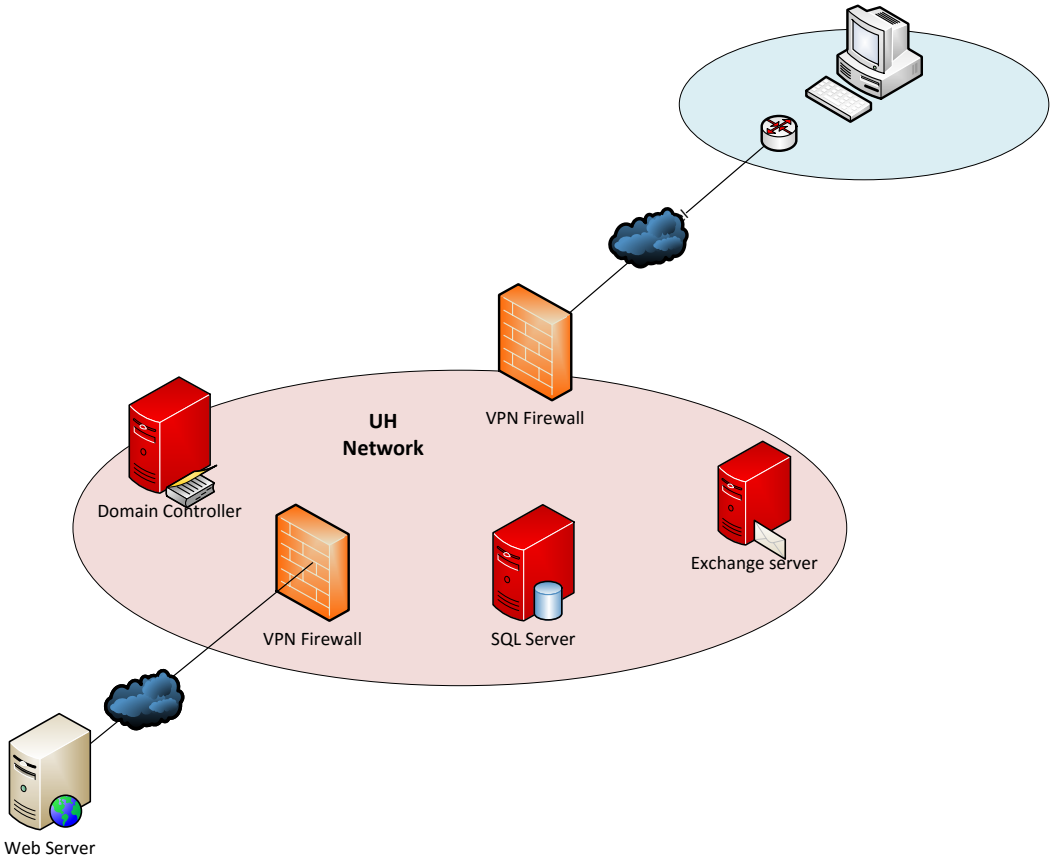


Figure 4: Non- Split Tunnel VPN Service

2.1.2 Cisco AnyConnect VPN Client

About Cisco AnyConnect

Cisco AnyConnect is a VPN client service that provides a remote secured connection to institution's network servers and database. For our application, Cisco AnyConnect comes with the advantage of being a cross-platform service, hence singularly used to provide both full service and split tunneling VPN service. The UH provides Cisco AnyConnect VPN client in split-tunnel mode only.

Mobile VPN Client

Available for download through the Android and Apple App stores and compatible versions shown in *Table 1* below.

Operating System	Version
Android	Android Version 4.x to 7.x
iOS	iOS Version 6.0 to later

Table 1: Supported mobile operating systems

PC VPN Client

Available for windows, Mac and Linux operating systems and specific versions shown in *Table 2* below.

Operating System	Version
Windows	Windows 10 x86(32-bit) and x64(64-bit)
	Windows 8.1 x86(32-bit) and x64(64-bit)
	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 SP1 x86(32-bit) and x64(64-bit)
Mac	Mac OS X 10.12
	Mac OS X 10.11
	Mac OS X 10.10
Linux	Red Hat 6 and 7 (64-bit only)
	Ubuntu12.04(LTS),14.04 (LTS), and 16.04 (LTS) (64-bit only)

Table 2: Supported PC operating systems

2.2 Configuration of Data Security

The data transferred through the VPN tunnel falls within categories of High Risk (such as Health Records) and Low Risk (such as job posting). Although the VPN tunnel provides a secured encryption, measures must be taken to confirm the identity of the user requesting access to the data. This section begins with the classification of data types and then recommendation of Two-factor Authentication, with a template for implementation

2.2.1 Data Risk Classification

Low Risk	Medium Risk	High Risk
▪ The data is intended for public disclosure. ▪ The loss of confidentiality, integrity or availability of the data or system could have **No adverse** effect on safety and finances.	▪ The data is not generally available to the public. ▪ The loss of confidentiality, integrity or availability of the data or system could have a **Mild adverse** effect on safety and finances.	▪ Protection of the data is required by law/regulation. ▪ UH is required to report to the government and/or provide notice to the individual if the data is inappropriately accessed. ▪ The loss of confidentiality, integrity or availability of the data or system could have a **significant adverse** effect on safety and finances.

Table 3: Data Risk Classification

Data Risk Classification Examples

The examples listed below can be used to determine the appropriate classification of various data types.

Low Risk	Medium Risk	High Risk
▪ Research data (at data owner's discretion ▪ CougarNet ID ▪ Non-Authentication required website postings. ▪ Policy and procedural manuals designated by the owner as public ▪ Job postings ▪ University contact information not designated by the owner as private. ▪ Information in the public domain (maps, directories, etc.)	▪ Unpublished Research data (at data owner's discretion) ▪ Student records and admission application ▪ Faculty/Staff employment applications, personnel files, benefits, salary, birthdate, personal contact information. ▪ Non-public UH policies and policy manuals ▪ Non-public contracts ▪ UH internal memos and email, non-public reports, budget, plans, financial info. ▪ University and employee ID numbers ▪ Project/Task/Award (PTA) numbers ▪ Engineering design and operational information regarding UH campus infrastructure.	▪ Health Information, including Protected Health Information (PHI) ▪ Health Insurance policy ID numbers ▪ Social Security Numbers ▪ Credit Card Numbers ▪ Financial Account Numbers ▪ Export controlled information under U.S laws ▪ Driver's License numbers ▪ Passport and visa numbers ▪ Donor contact information and non-public gift information

Table 4: Data Risk Classification Examples

2.2.2 Two-Factor Authentication

Two factor authentication requires two types of authentication to verify the user's identity. First, the user login with their CougarNet ID and password, then a physical device in control by the user such as mobile phone, tablet or landline phone to verify their identity. There are five physical devices that can be used to provide the second factor of the Two-factor authentication, see *Table 5* below for details.

Device Type	Authentication Options	Supported Platforms
Smartphone	▪ Push notification ▪ Passcode ▪ SMS text message ▪ Phone call	▪ iOS ▪ Android ▪ Windows Mobile
Tablet	▪ Push notification ▪ Passcode	▪ iOS ▪ Android ▪ Windows Mobile
Mobile Phone	▪ SMS text message ▪ Phone call	▪ Mobile phones with SMS and text messaging capability
Landline	▪ Phone call	▪ All phones
Hardware Token	▪ Passcode	▪ A "keychain" hardware token displays two-factor codes at a push of a button

Table 5: Two-Factor authentication device options

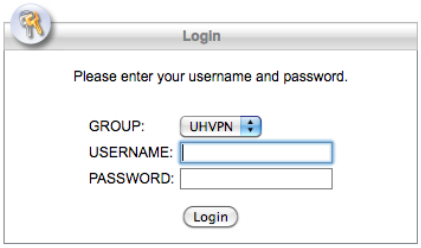
3.0 Installation Phase Template

3.1 VPN Installation Instructions

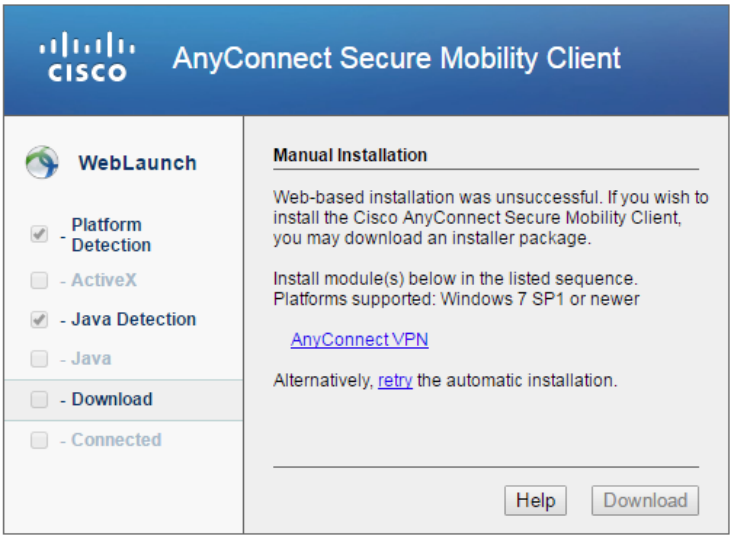
3.1.1 Windows

Installing the VPN Client

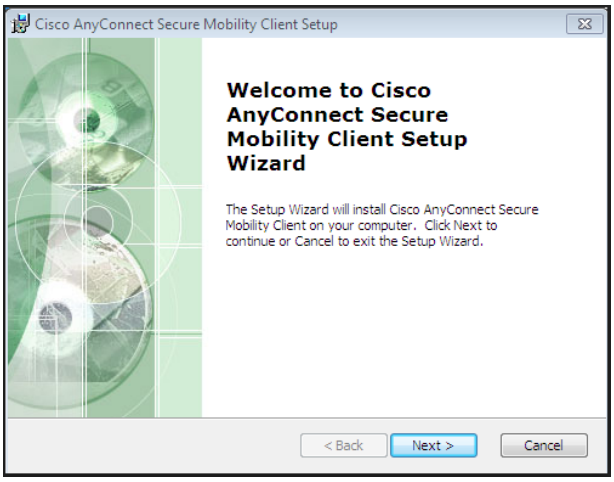
1. Download the Cisco AnyConnect VPN for Windows installer from: **vpn.uh.edu**.
2. Enter the **Cougarnet** credentials.



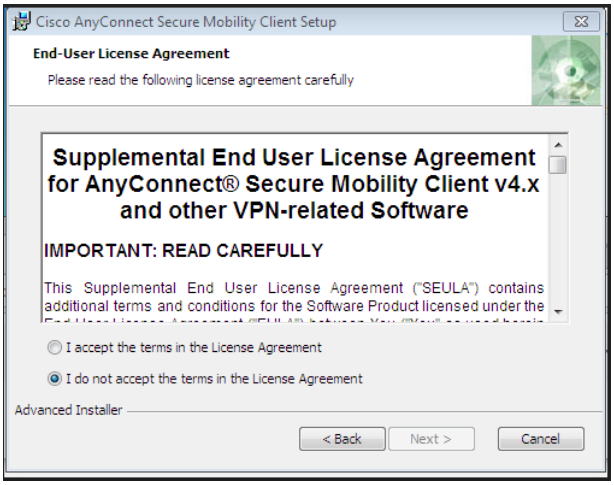
3. Click the **AnyConnect VPN** link to download the software.



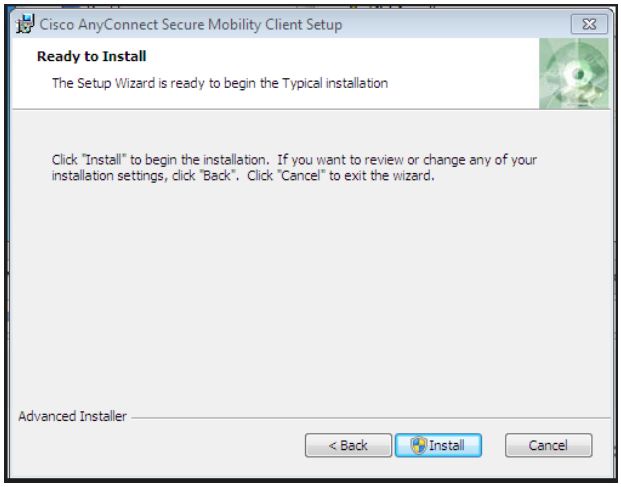
4. Double-click the **AnyConnect.exe** file. (Note: You may encounter a Security Warning screen and have to click Run to proceed.)
5. Click **Next**.



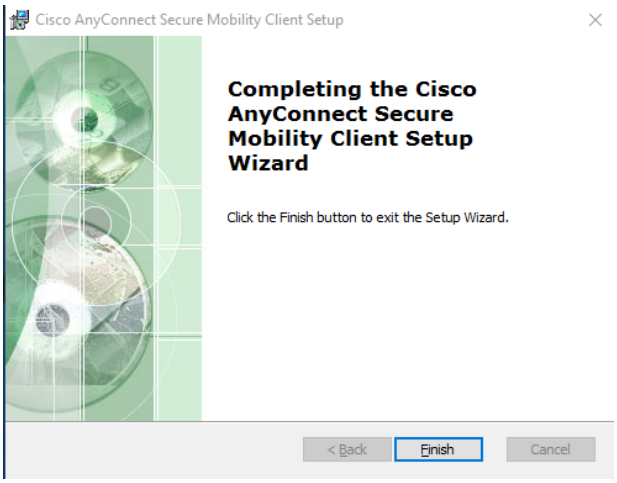
6. **Accept** the terms of the License Agreement.
7. Click **Next**.



8. Click **Install**.



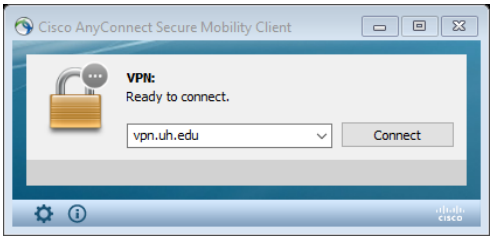
9. Install the VPN client and, when a message appears saying the Cisco AnyConnect client has been installed, click **Finish**.



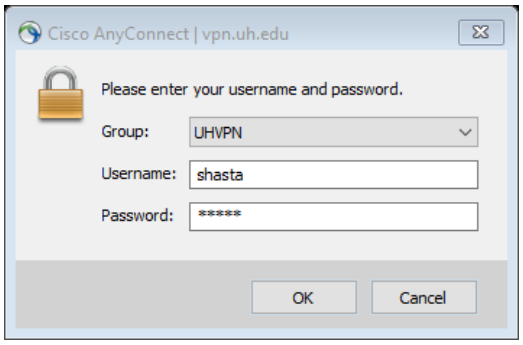
Note: If you get a User Account Control screen asking if you want to allow the following program from an unknown publisher to make changes to your computer click **Allow** or **Accept**.

Connecting to the UH VPN

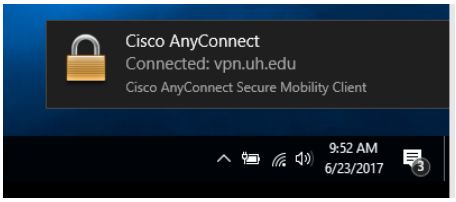
1. Launch the **Cisco AnyConnect Secure Mobility Client**.
   If you don't see **Cisco AnyConnect Secure Mobility Client** in the list of programs, navigate to **Cisco > Cisco AnyConnect Secure Mobility Client.**
2. When prompted for a VPN, enter vpn.uh.edu and then click **Connect**.



3. Enter the following information and then click **OK**:
   - **Group**: select **UHVPN** (this is a split- tunnel service i.e. non-UH traffic flows normally on an unencrypted internet connection) or **Full Traffic non-split-tunnel** (all internet traffic flows through the VPN connection) if available.
   - **Username**: your COUGARNET ID
   - **Password**: your COUGARNET ID password

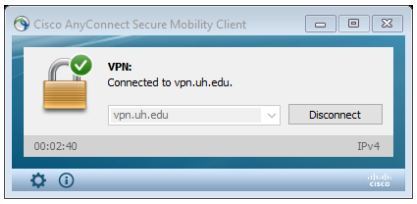


4. Once the VPN connection is established, a message displays in the lower-right corner of your screen, informing you that you are now connected to the VPN.



Disconnect from the UH VPN

1. In the notification area, click the Cisco AnyConnect icon if it is displayed. Otherwise, go to your list of programs and click **Cisco AnyConnect Secure Mobility Client**.
2. At the prompt, click **Disconnect.**



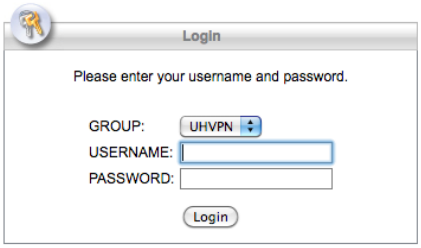
Note: If you disconnect from UH VPN you will be required to re-enter your password for reconnections.

3.1.2 Mac

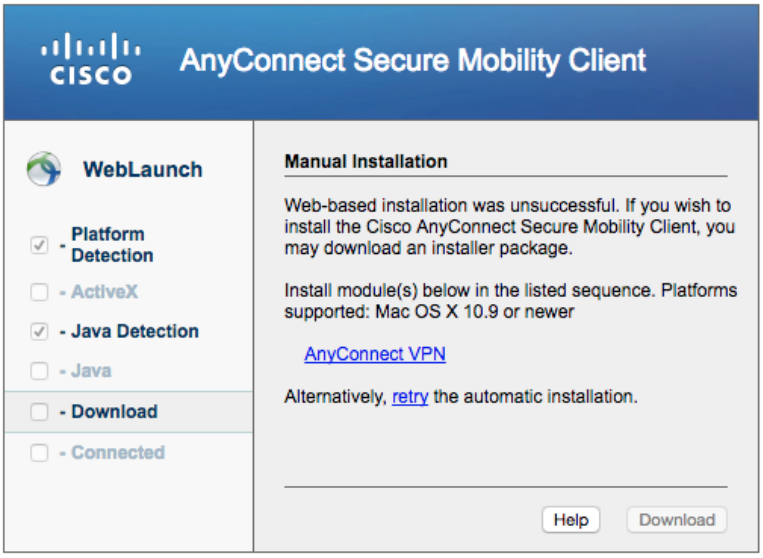
Note: ONLY Mac OS 10.9.x and newer versions are supported by the CISCO AnyConnect software.

Installing the VPN Client

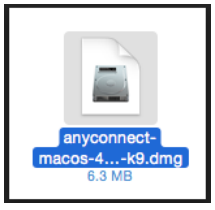
1. Download the Cisco AnyConnect installer for Mac from: **vpn.uh.edu**.
2. Enter the **Cougarnet** credentials.



3. Click the **AnyConnect VPN** link to download the software.

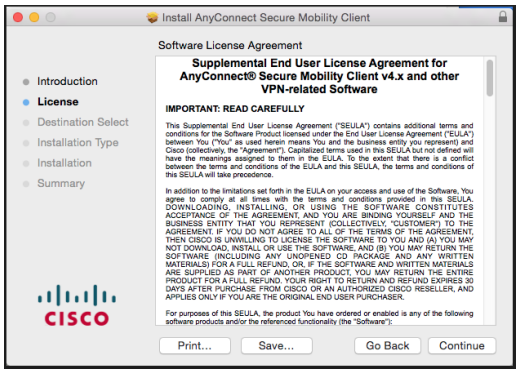


4. If you get a **DMG** file double click the file.

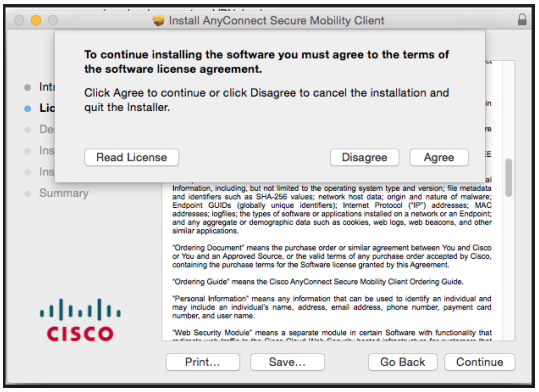


5. Double-click the **AnyConnect.pkg** file to start the Cisco AnyConnect Installer wizard.

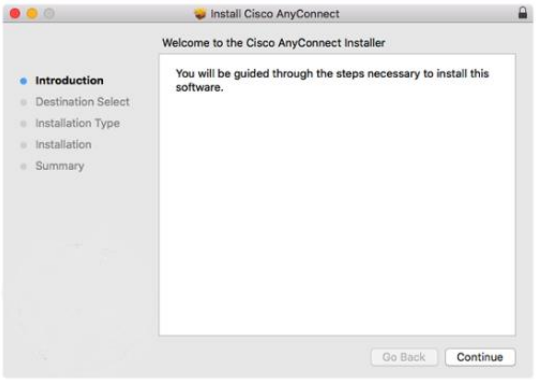
6. Click **Continue**.



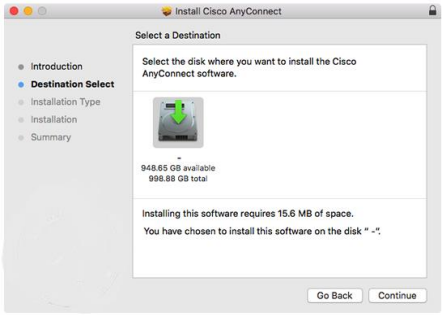
7. Click **Agree**.



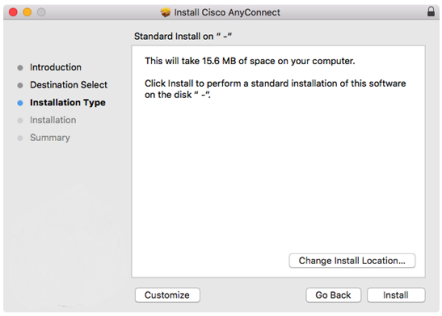
8. When the Welcome window displays, click **Continue**.



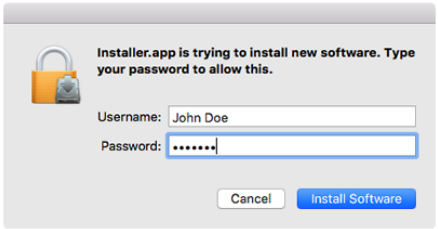
9. Select your hard drive as the destination where you want to install Cisco AnyConnect and then click **Continue** if you receive this screen.



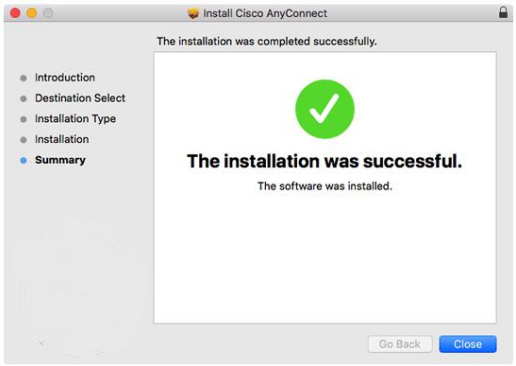
10. Click **Install** to perform a standard installation of the software.



11. At the prompt, enter your administrator account password for the Mac and click **Install Software.**

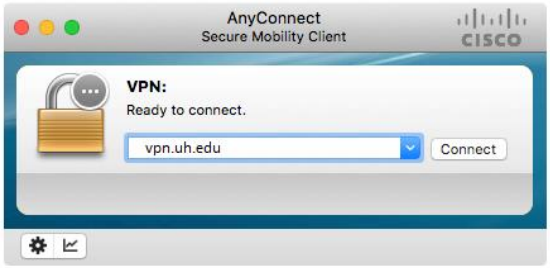


12. When the software has finished installing, click **Close**.

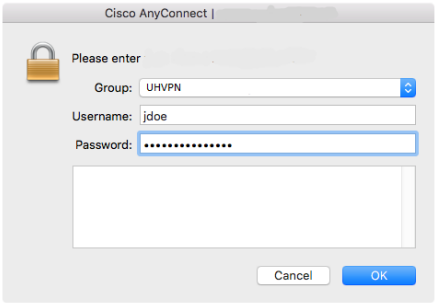


Connecting to the UH VPN

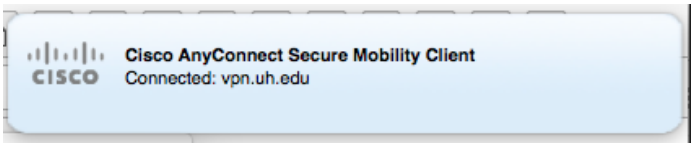
1. To launch the VPN client, open your **Applications** folder and navigate to **Cisco** > **Cisco AnyConnect Secure Mobility Client**.
2. When prompted for a VPN, enter **vpn.uh.edu** and then click **Connect**.



3. Enter the following information and then click **OK**:
   - **Group**: select **UHVPN** (this is a split- tunnel service i.e. non-UH traffic flows normally on an unencrypted internet connection) or **Full Traffic non-split-tunnel** (all internet traffic flows through the VPN connection) if available.
   - **Username**: your COUGARNET ID
   - **Password**: your COUGARNET ID password



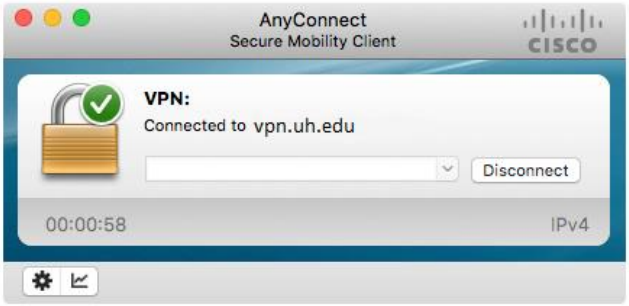
Note: You should now be connected to UH VPN.



4. Once the VPN connection is established, the Cisco AnyConnect icon with a small lock appears in the dock.

Disconnect from the UH VPN

1. Click the Cisco AnyConnect icon with a small lock.
2. At the prompt, click **Disconnect**.



Note: If you disconnect from UH VPN you will be required to re-enter your password for reconnections.

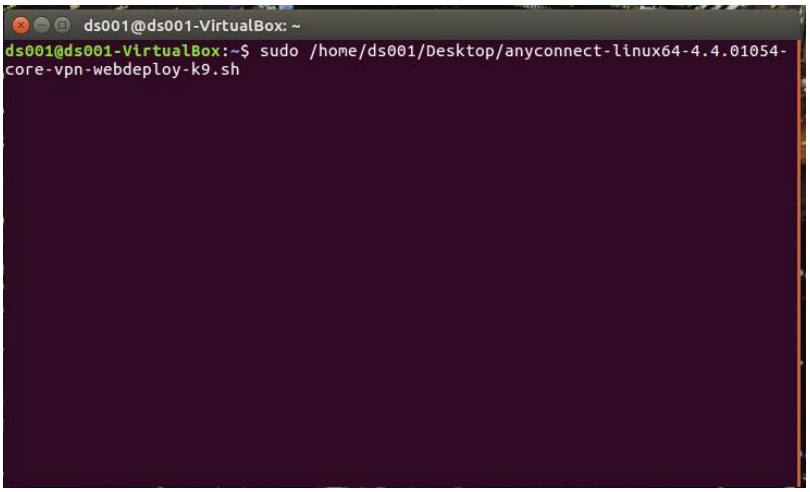
3.1.3 Linux (Ubuntu)

Note: If you disconnect from VPN you will be required to re-enter your password for reconnections.

Install and configure AnyConnect

1. Download the Cisco AnyConnect VPN for Linux installer from: **vpn.uh.edu**. Enter the **Cougarnet** credentials. Copy the file to your desktop.

2. Open Terminal. Drag the file into Terminal. Remove the quotes and type sudo in front of the file location. Press Enter

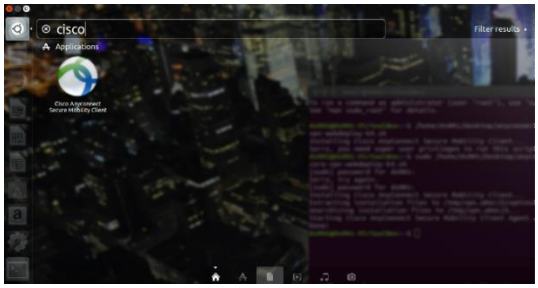


3. Type your password and installation should begin.
4. Installation is done when you see the following.

```
Installing Cisco AnyConnect Secure Mobility Client...
Extracting installation files to /tmp/vpn.uRecJ3/vpninst843528333.tgz...
Unarchiving installation files to /tmp/vpn.uRecJ3...
Starting Cisco AnyConnect Secure Mobility Client Agent...
Done!
ds001@ds001-VirtualBox:~$
```

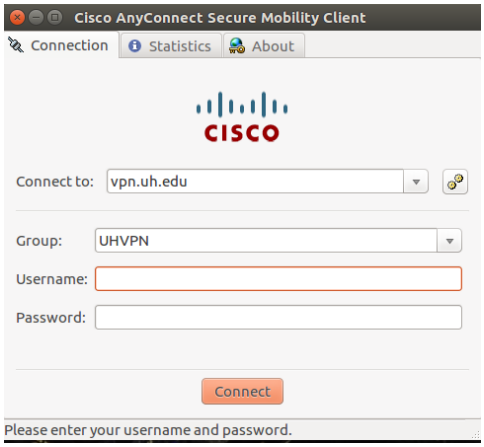
Connecting to the UH VPN

1. Open the search bar and search for Cisco. You should see the Cisco icon. Click to open.



2. Type in **vpn.uh.edu** in the Connect to address bar. Press **Connect**.

3. Make sure Group is set to UHVPN. Insert your Cougarnet ID credentials. Press Connect.

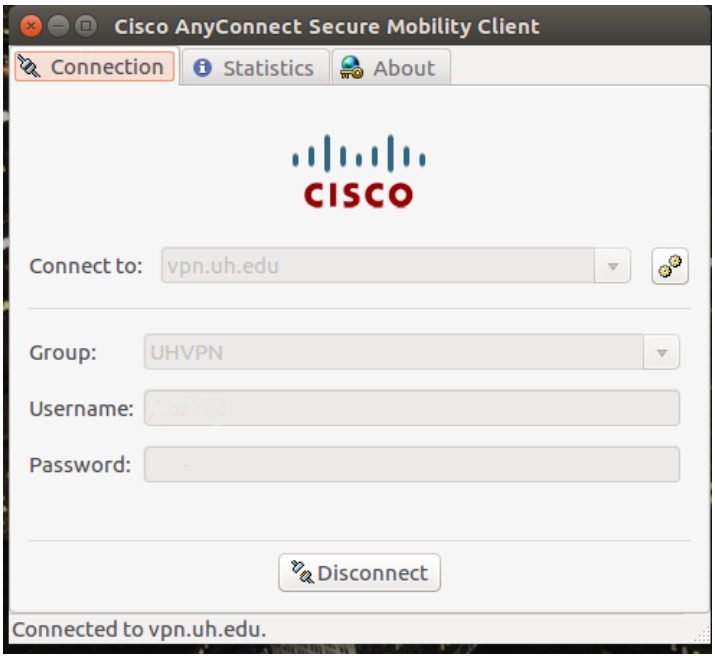


Note: You should now be connected to UH VPN.

Disconnect from the UH VPN

1. Click on the Cisco icon to open the connection box.

2. The connection box will open. Press Disconnect.



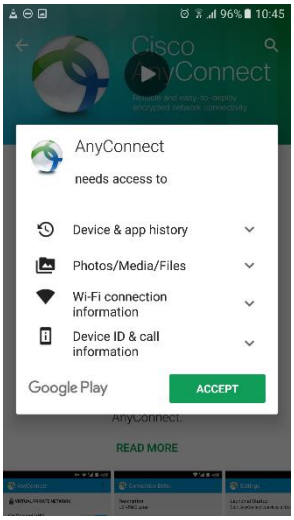
Note: You are now disconnected from UH VPN and will be required to re-enter your password to reconnect.

3.1.4 Android

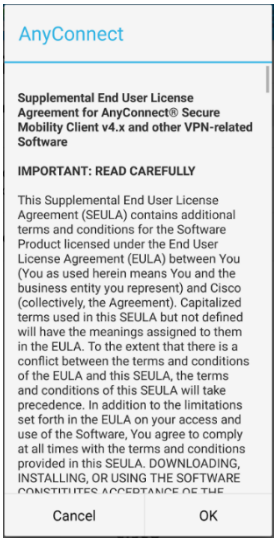
Install and configure AnyConnect

1. Go to the Google Play Store and search for Cisco AnyConnect.
2. Choose the **AnyConnect** app and tap **Install**.

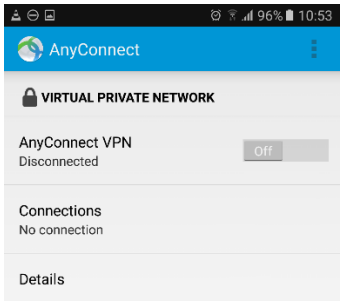
3. If prompted, tap **Accept** to give AnyConnect permission to access other apps.



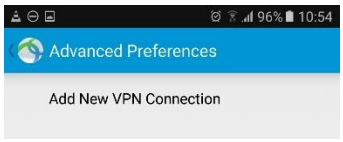
4. Tap **Open** and accept the license agreement if one is presented.



5. Choose to add a new VPN connection by tapping **Connections**.

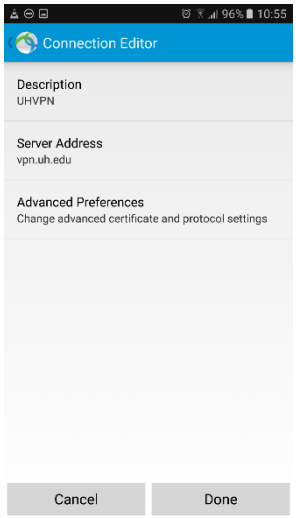


6. If the Advanced Preferences screen displays, tap **Add a New VPN Connection.**



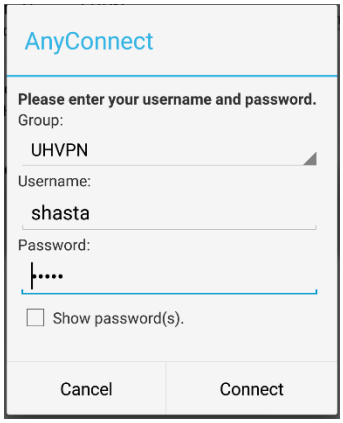
7. Enter the following information:
   - **Description**: label the configuration with a unique identifier (for example, UHVPN)
   - **Server Address**: vpn.uh.edu

8. Tap **Done**.

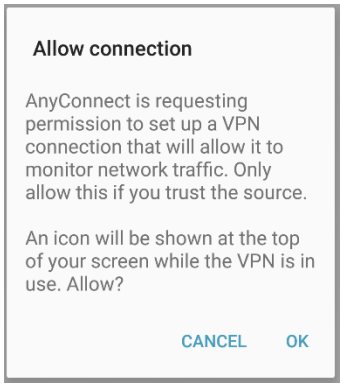

96% 10:55
Connection Editor
Description
UHVPN
Server Address
vpn.uh.edu
Advanced Preferences
Change advanced certificate and protocol settings
Cancel
Done

Connect to UH VPN

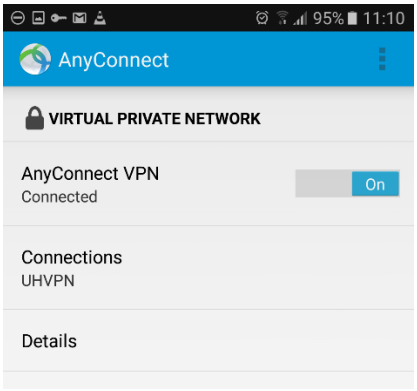
1. Open the AnyConnect app.
2. Tap the AnyConnect VPN **Off** button.
3. When prompted for your username and password, enter the following and then tap **Connect**:
   - **Group**: select **UHVPN** (this is a split- tunnel service i.e. non-UH traffic flows normally on an unencrypted internet connection) or **Full Traffic non-split-tunnel** (all internet traffic flows through the VPN connection) if available.
   - **Username**: your COUGARNET ID
   - **Password**: your COUGARNET ID password



4. If you see a message seeking your attention, tap **OK**.



5. When you are connected to VPN, the AnyConnect app shows the VPN as turned on.



Disconnect from UH VPN

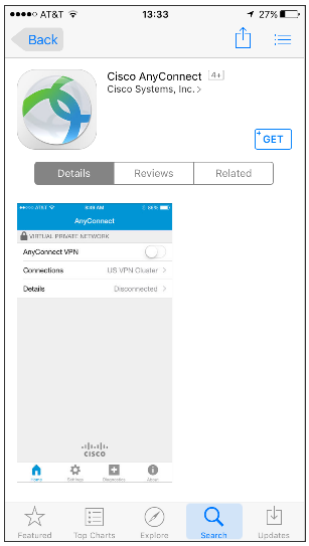
To disconnect from the UH VPN, open the AnyConnect app and tap the **On** button. It toggles to **Off**, disconnecting your device from the UH VPN Service.

Note: If you disconnect from UH VPN you will be required to re-enter your password for reconnections.

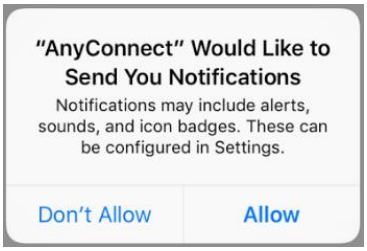
3.1.5 iOS

Install and configure AnyConnect

1. Go to the Apple App Store and search for Cisco AnyConnect.
2. Choose the **AnyConnect** app and tap **get** to install.

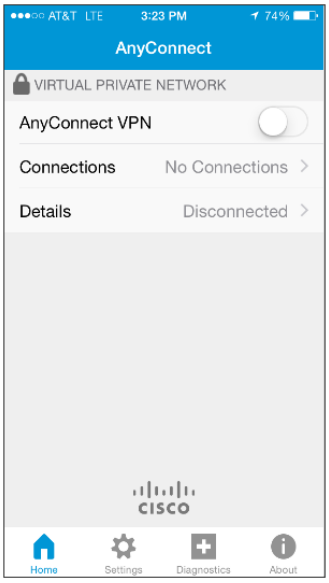


3. Tap **Open** and accept the license agreement if one is presented.
4. Click **Allow**.

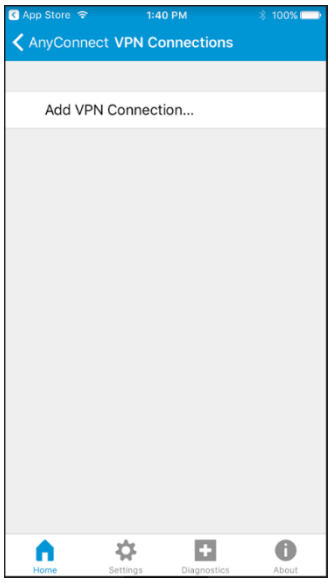


Note: AnyConnect will now be sending you notifications.

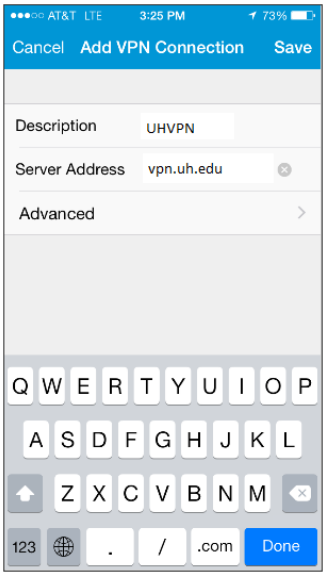
5. Choose to add a new VPN connection by tapping **Connections**.



6. If the Advanced Preferences screen displays, tap **Add a New VPN Connection.**

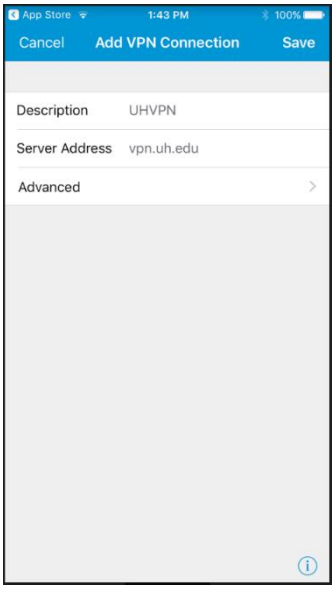


7. Enter the following information:
   - **Description**: label the configuration with a unique identifier (for example, UHVPN)
   - **Server Address**: vpn.uh.edu

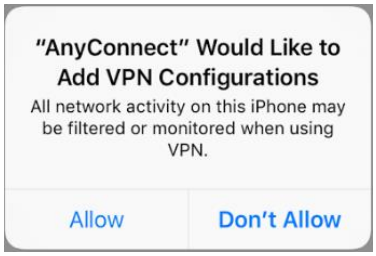


8. Tap **Done**.

9. Tap **Save**.

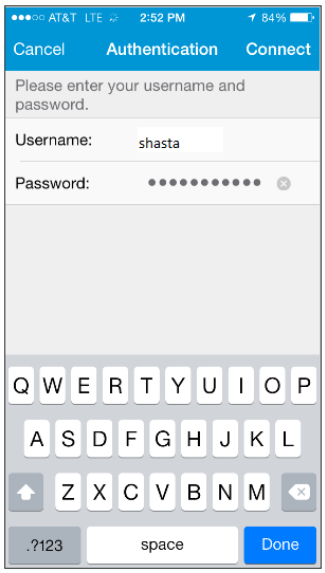


10. Tap **Allow**.

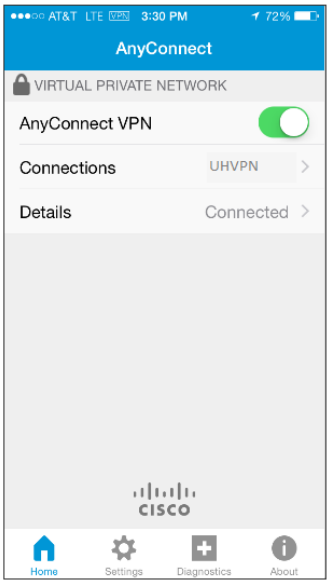


Connect to UH VPN

1. Open the **AnyConnect** app.
2. Tap the AnyConnect VPN **Off** button.
3. When prompted for your username and password, enter the following and then tap **Connect**:
   - **Group**: select **UHVPN** (this is a split- tunnel service i.e. non-UH traffic flows normally on an unencrypted internet connection) or **Full Traffic non-split-tunnel** (all internet traffic flows through the VPN connection) if available.
   - **Username**: your COUGARNET ID
   - **Password**: your COUGARNET ID password



4. When you are connected to VPN, the AnyConnect app shows the VPN as turned on.



Disconnect from UH VPN

To disconnect from the UH VPN, open the AnyConnect app and tap the **On** button. It toggles to **Off**, disconnecting your device from the UH VPN Service.

Note: If you disconnect from UH VPN you will be required to re-enter your password for reconnections.

4.0 Support Phase Template

4.1 Request Workflow

The VPN if provided by default with two service options; the Split-Tunnel and Non-Split-Tunnel, coupled with detailed instructions provided on the UH website would nullify the need for client's request. Since all the university of Houston remote application falls within the Split (uh.edu) and Non-Split (library services) options, the customers would have all the information needed and a request workflow maybe obsolete, therefore Help and Support are the required services.

4.2 Support Model

Although issues in the installation phase has been mostly addressed by the instructions on the UH website and a robust Cisco AnyConnect VPN Client, like all things technology faults must arise. These faults are processed through a help request section of which the workflow model is displayed in *figure 4* below and the template for the help request and Troubleshooting guide provided in the next section.

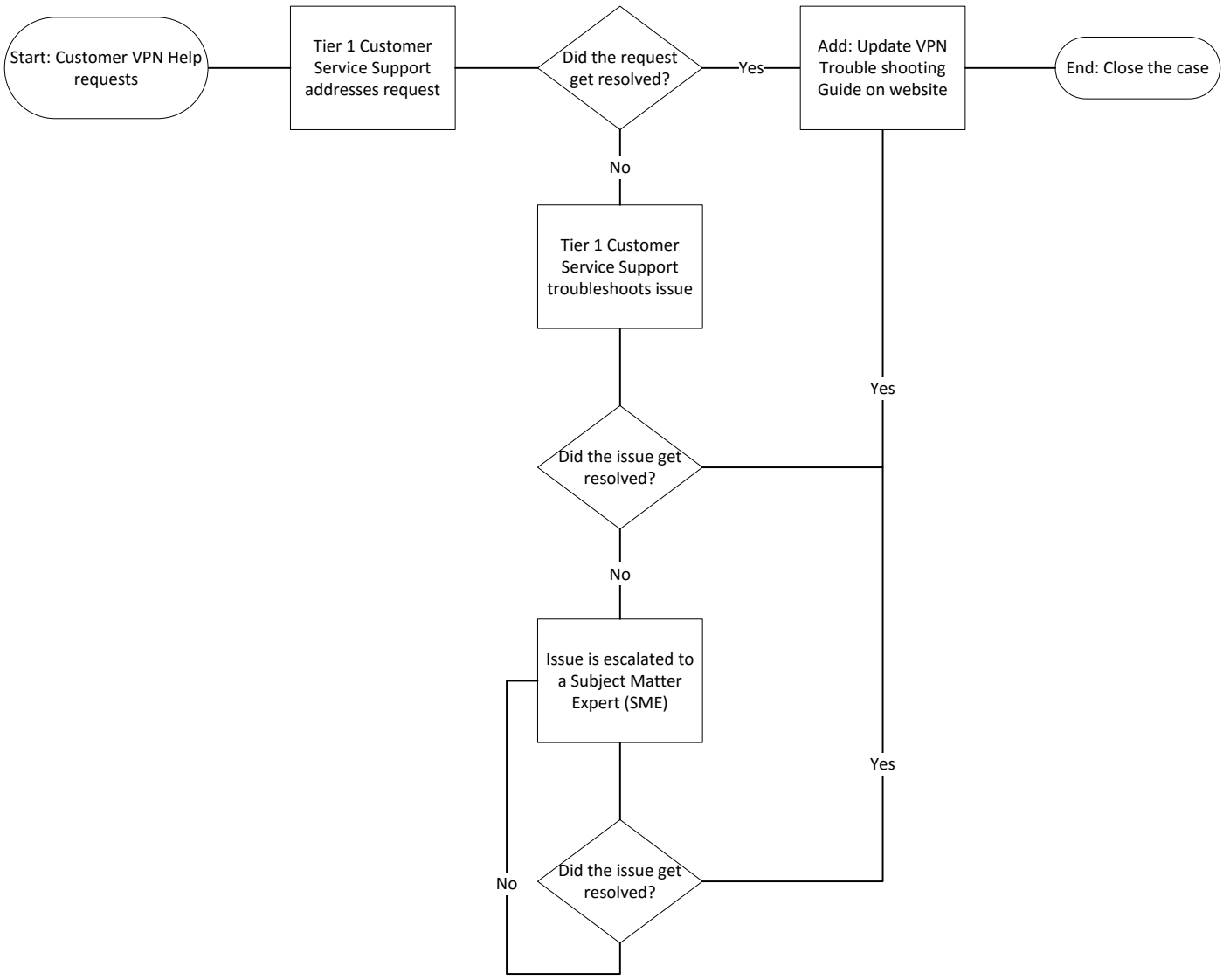


Figure 5: Help Request workflow

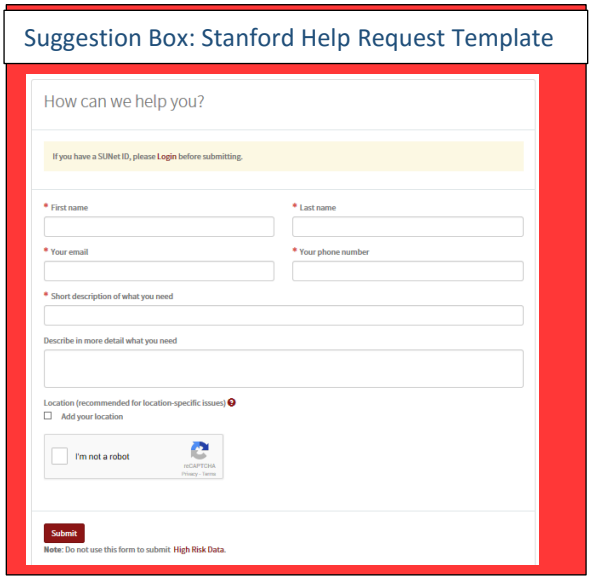
4.3 Help and Troubleshooting

4.3.1 Help

The help options request for special request from users would require details such as;

- Name (First, Last)
- Email Address
- Phone Number
- Short and Detailed description of Request.

Suggestion Box: Stanford Help Request Template



4.3.2 Troubleshooting

This section includes answers to frequently Encountered Problems from the VPN service Usages

First, check that you have installed the correct client for your computer and you meet all the dependencies. If you still have problems connecting, please continue reading.

1. Connect to the internet
   To connect to the VPN server, you must be connected to the internet first.
2. Try again later
   If your VPN connection was working recently and has suddenly stopped, the server may be down temporarily, unavailable or too many users are connected. Try again later.
3. Error message
   There are several error messages that can appear when a VPN connection is unsuccessful.
   They usually have a number like ‘Error 721’. By searching for this error message and number online, you can often find what it means and why it has appeared. Also, you can often find out how other people have dealt with the problem themselves. Try Google.
   Quite often, it a configuration or software version incompatibility on your home computer that you should update.
   Built-in PPTP clients on all OS's aren't supported on the new VPNs.
4. Check VPN settings
   Verify your VPN configuration settings or delete and reinstall the client from this page.
5. At what stage does it fail?
   If you are sure all your settings are correct, think about the error message you have received (if any) and see if it relates to any of the issues listed below.
   The number of possible problems can be reduced by watching how and when the connection attempt fails.
   If it fails as it is trying to connect (i.e. before the 'verifying username and password' stage) then see the 'Failing to connect?' section below.
   If you can connect but cannot login successfully, then see the 'Failing to verify username and password?' section below.
6. Failing to connect?
   Firewall settings
   Some software firewalls have been known to stop users connecting to our VPN server, especially if the settings are too 'restrictive'.
   You can usually tell if it is your firewall causing the problem by turning it off and trying again.

Versions of Microsoft Windows XP service pack 2 and above have a built-in firewall already turned on. However, its default settings have not been known to interfere with University VPN connections.

Router / Firewall firmware version

Out-of-date 'firmware' versions on ADSL routers are one of the most frequent causes of VPN problems.

If you are using an ADSL Router or Firewall device to connect to broadband at home, and are getting the error message 'Error 800 - Unable to establish the VPN connection' when you try to connect, then you should check that the router's software or firmware version is up to date.

The manufacturers of these devices often develop the latest firmware versions and make them available for download from their own websites. Download and install the latest available firmware code for your model of Router and try to connect again. (Note: this does not usually apply standard ADSL modem devices.)

Often some older versions of router firmware are not programmed to cope with running multiple VPN connections at the same time. If you have more than one computer connecting to VPN behind your router, check that the router firmware is capable of this and try upgrading it to the latest firmware version.

ISP's VPN availability

Some Internet Service Providers (ISP) restrict certain traffic or network ports over their service.

If protocols are not supported, or VPN is blocked by your ISP, you will not be able to connect.

Using NAT

If you are using an ADSL router and have Network Address Translation (NAT) set up, this can cause problems if two people try to connect at once.

Some routers can still detect which computer to send the two separate sets of traffic to and some can't. Firmware updates may improve this.

7. Failing to verify username and password

CougarNet Account: To log into any University system or computer your account must already be registered and active.

Username: Log in with your username and password.

8. Unexpected disconnections

Automatic timeouts: We do not have any timeouts from the VPN server side, but your VPN connection will terminate if your internet connection stops or your computer powers off.

Server busy: The server can only support a limited number of concurrent users and can occasionally get too busy. This may cause your connection to stall or disconnect unexpectedly. If you suspect this is happening too frequently or for days at a time, report the problem to the IT Service Desk.

9. Contact the Staff Service Centre

Call Us: 713-743-1411

Fax Us: 713-743-1410

Email Us: support@uh.edu

Mail Code: TSS 2002e