UNT System Campus VPN Guide

Contents

Introduction....2
SSL Web Portal....3
Installing AnyConnect VPNClient....11
Connecting AnyConnect VPN client....15
Apple OS X Configuration....16
Android Configuration....21
Apple iOS Configuration....26
IKEv2 (Internet Key Exchange Version 2)....32
SBL (Start Before Logon)....33

Version 3.3
March 10, 2021

Introduction

This is a guide on the different ways to connect to the University of North Texas System Campus VPN. There are several different methods of connecting to the VPN that this guide will discuss. Each method accomplishes the same goal just in a different way, which allows the users more flexibility. This flexibility is important since we have a wide range of users that have different needs and different hardware requirements.

The UNT System Campus VPN is a device that will allow you to connect remotely to on-campus resources. This will allow employees and students of the University of North Texas to work from off campus using resources they otherwise couldn't access. The connection from the user machine to the Campus VPN is an encrypted connection which allows us to securely allow access to resources we otherwise wouldn't allow.

As stated above there are three different methods to connect to the Campus VPN. Each method is available for all employees and students of the University of North Texas. There may be a preferred method that your network manager or teacher would like you to use, so it's always best to discuss the issue with them first.

The first method is the web portal. This is an SSL web page that acts as a proxy server to the on-campus resources. This will allow access to the on-campus resources from machines that you might not want or need to install a client. This way uses SSL and Java to accomplish this goal.

The second method is the AnyConnect client. This is an ActiveX or Java client which uses SSL protocols to setup an encrypted connection to the Campus VPN. The AnyConnect client gives the user a UNT IP address making their machine logically part of the network. Only traffic going to the University of North Texas will use the encrypted tunnel. All other traffic will not be encrypted and use your normal internet provider connection.

The final method is the third party IPSec client. This is a client that uses the IPSec protocols to connect to the Campus VPN. Any third party IPSec client that uses the standard IPSec protocols should work, however they may have problems which may not be supportable. Just like the AnyConnect client this method will also give the user a UNT IP address. It will also only use the encrypted tunnel for traffic going to the UNT like the AnyConnect client does. Just like the AnyConnect client all other traffic will use your normal internet provider connection.

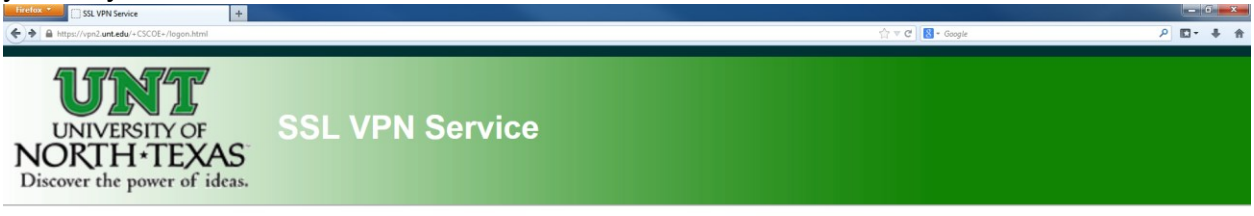
.

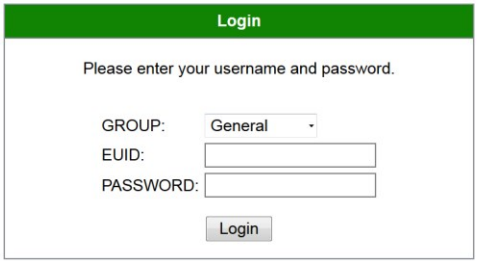
SSL Web Portal

The web portal is the easiest way to connect to the Campus VPN without having to install a client on your machine. Just point a web browser to:

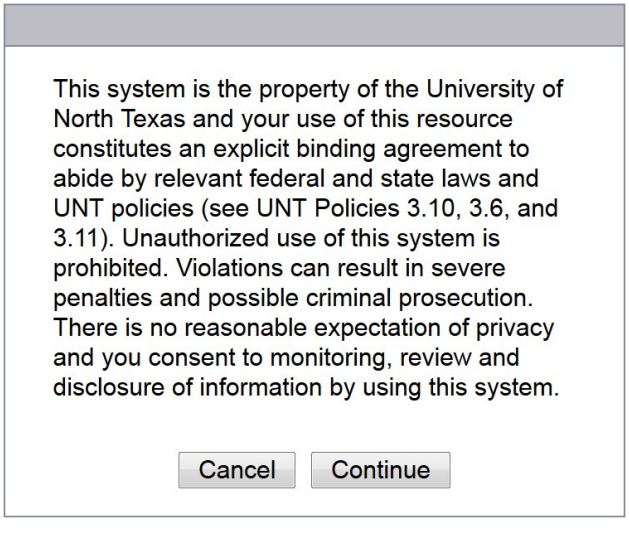
vpn.unt.edu

You will have to accept the certificates first and you can setup a permanent exception so you only have to do this once.

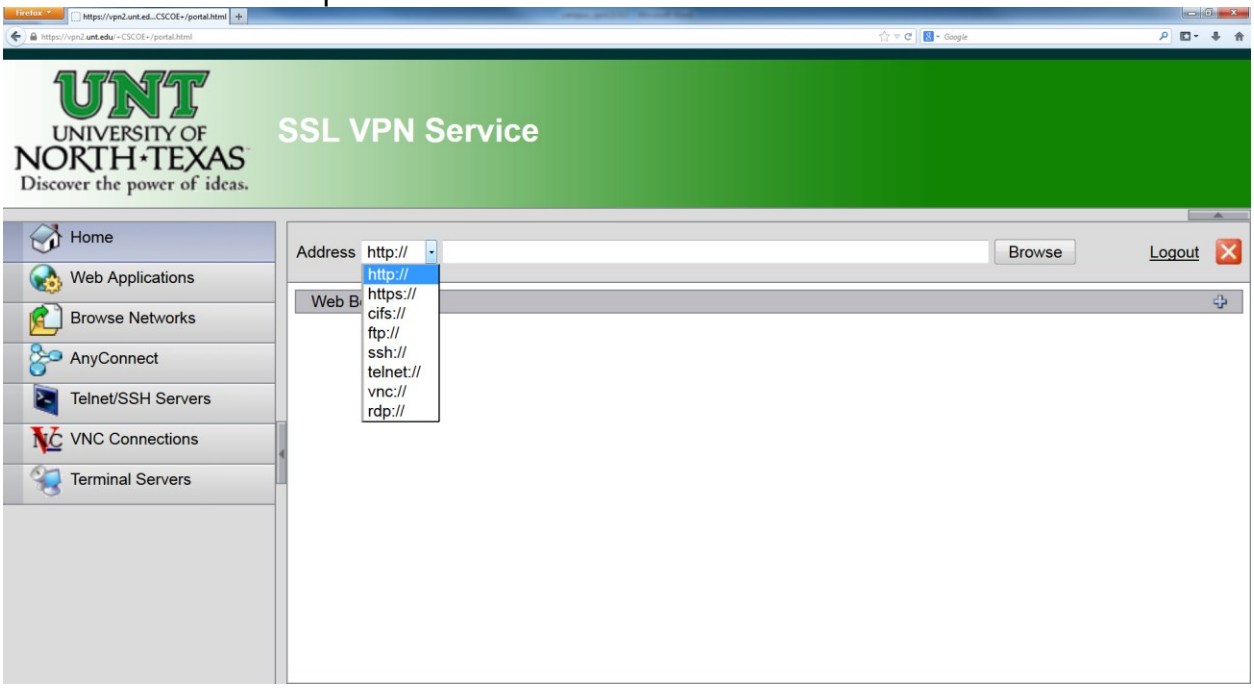




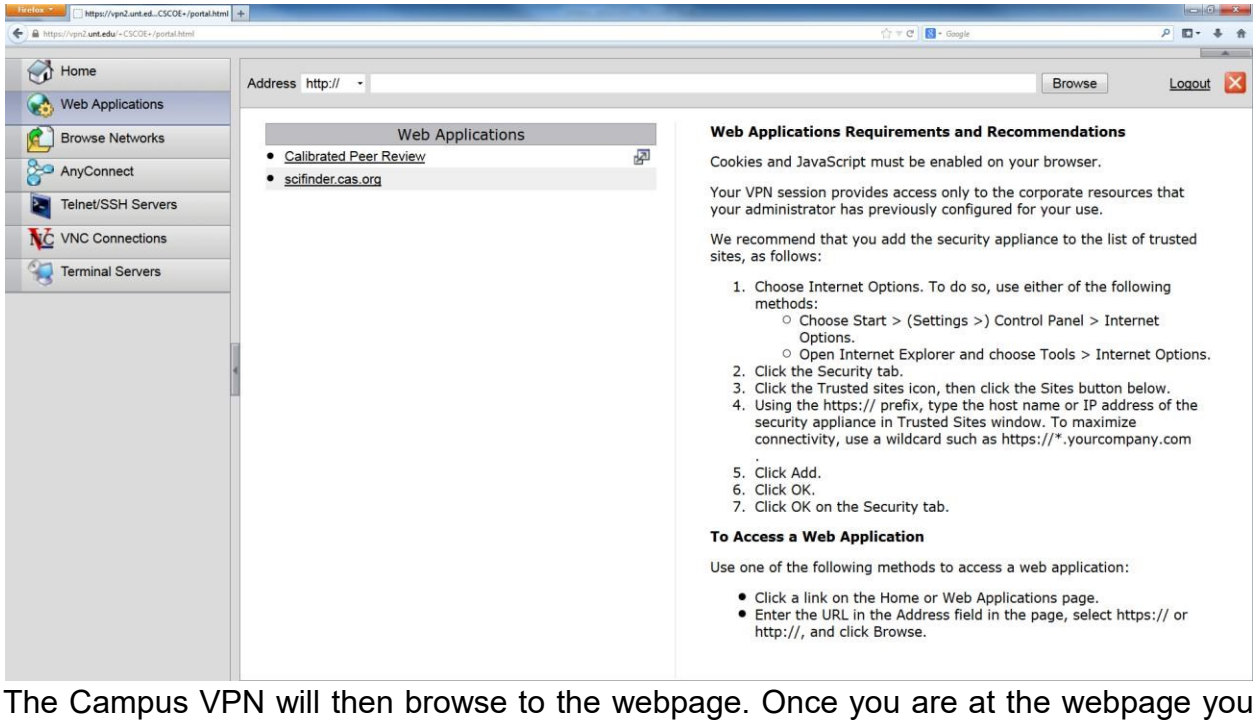
To login you will need to enter in your EUID and password. After that the computer usage policy will appear. You will have to accept the policy before you can continue on to the web portal home page.



Once you accept the computer usage policy you will be taken to the web portal home page. From this page you can go to the different areas of the web portal by using the menu to the left or the pull down menu show below.



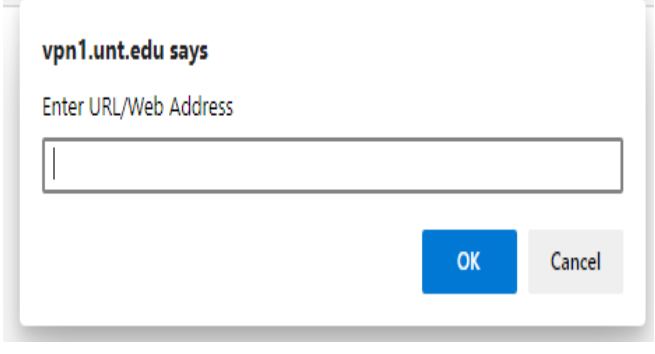
The first menu item is for web applications. This is where you can use the Campus VPN as a web proxy. On the right side of the page you will see instructions on how to use this function. Just enter in a web address in the address bar and hit enter or the browse button.



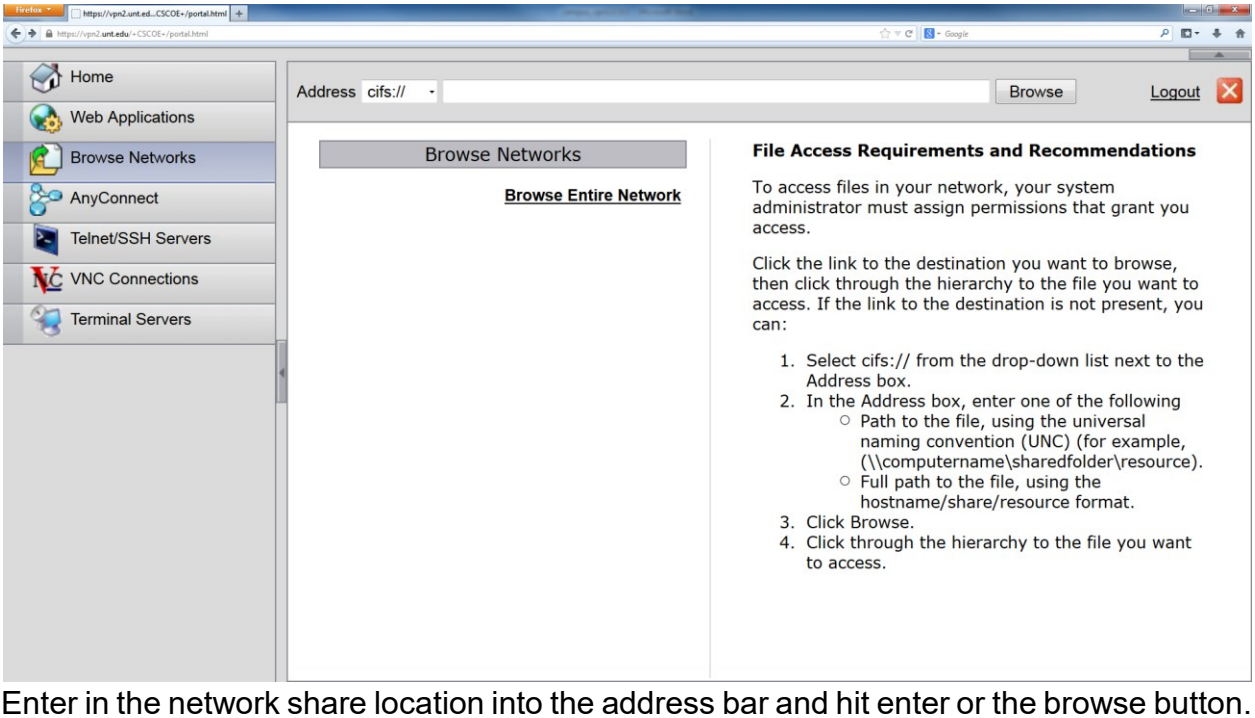
The Campus VPN will then browse to the webpage. Once you are at the webpage you will notice two strange things. The first thing is the address in the URL bar. You will notice that it has the Campus VPN address first then the webpage where you are. This is

because you are using the Campus VPN as a proxy, piping the webpage through the Campus VPN. The second thing you will notice is the strange menu bar on the top right side of the screen.

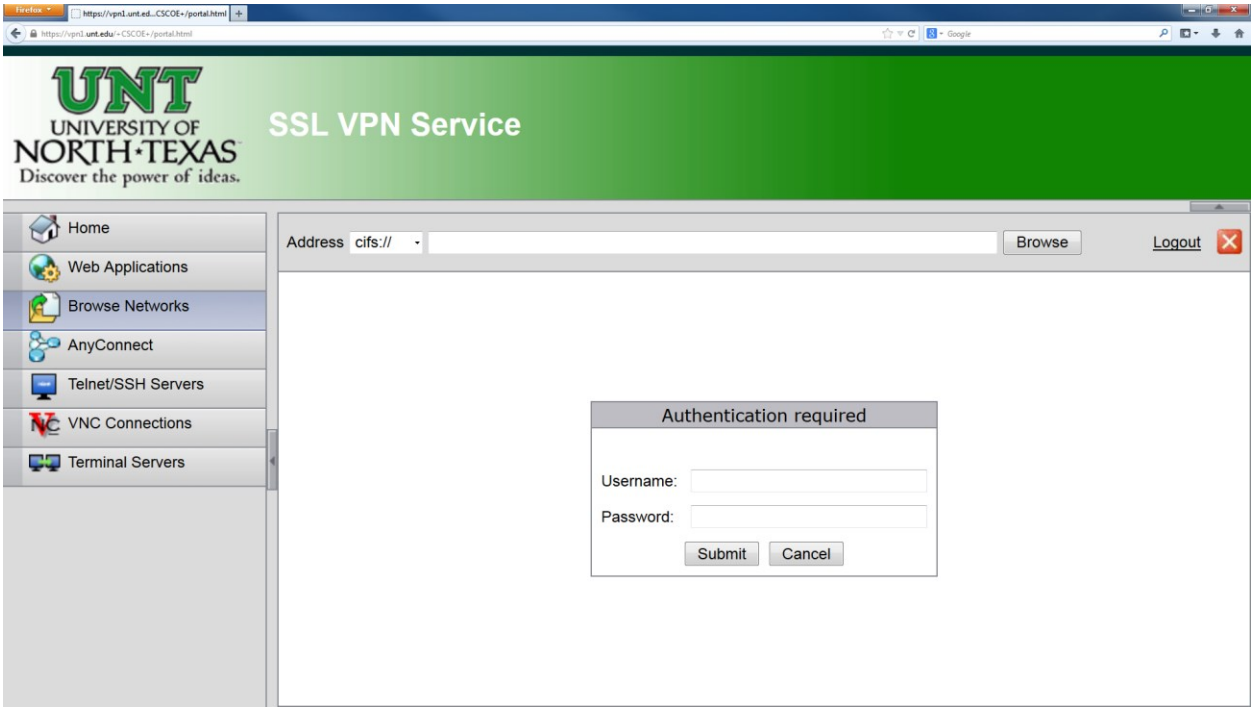
From left to right this menu will allow you to switch the menu to the other side, enter in a new address, go back to the web portal home page, and logoff the Campus VPN. If you hit the new address button it will pop up a window that you can enter in a new web address.



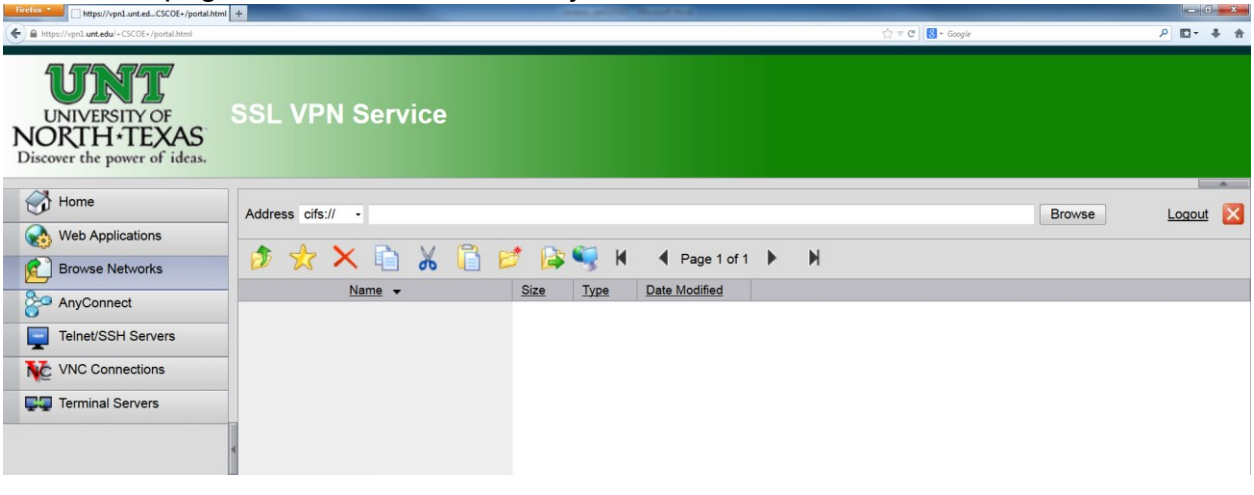
The next menu item is the browse network page. This page will allow you to browse network shares and files.



Enter in the network share location into the address bar and hit enter or the browse button. This will bring up the network login screen shown below. Your network manager or teacher may have to give you access to the network share you are trying to access.

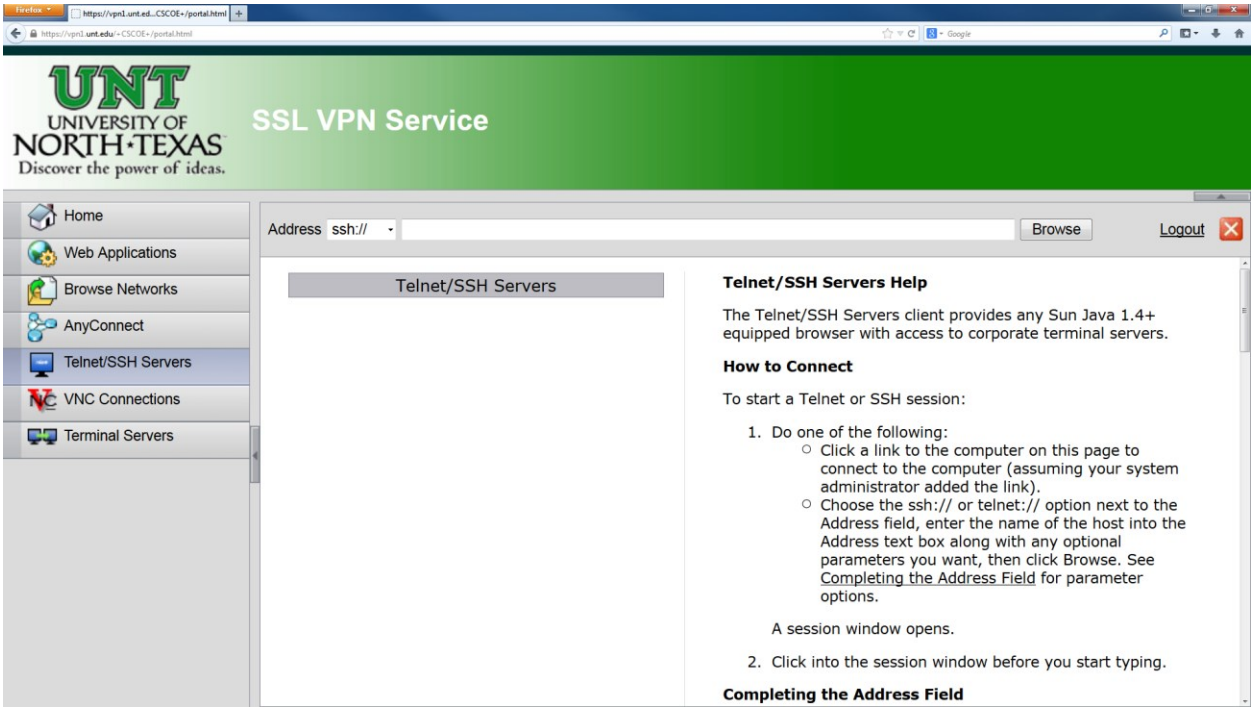


Once you have access enter in your username and password for that network share. After you login, you will be able to browse the network share and access the files. Below is what the page will look like without any network folders or files.

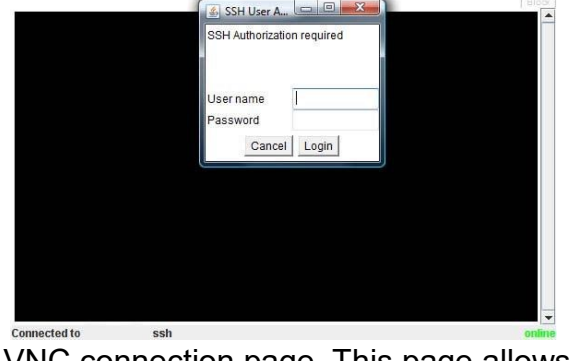


The third menu item is the AnyConnect page. From this page you will install the AnyConnect client on your machine. We will discuss the AnyConnect client and the installation later on in this guide.

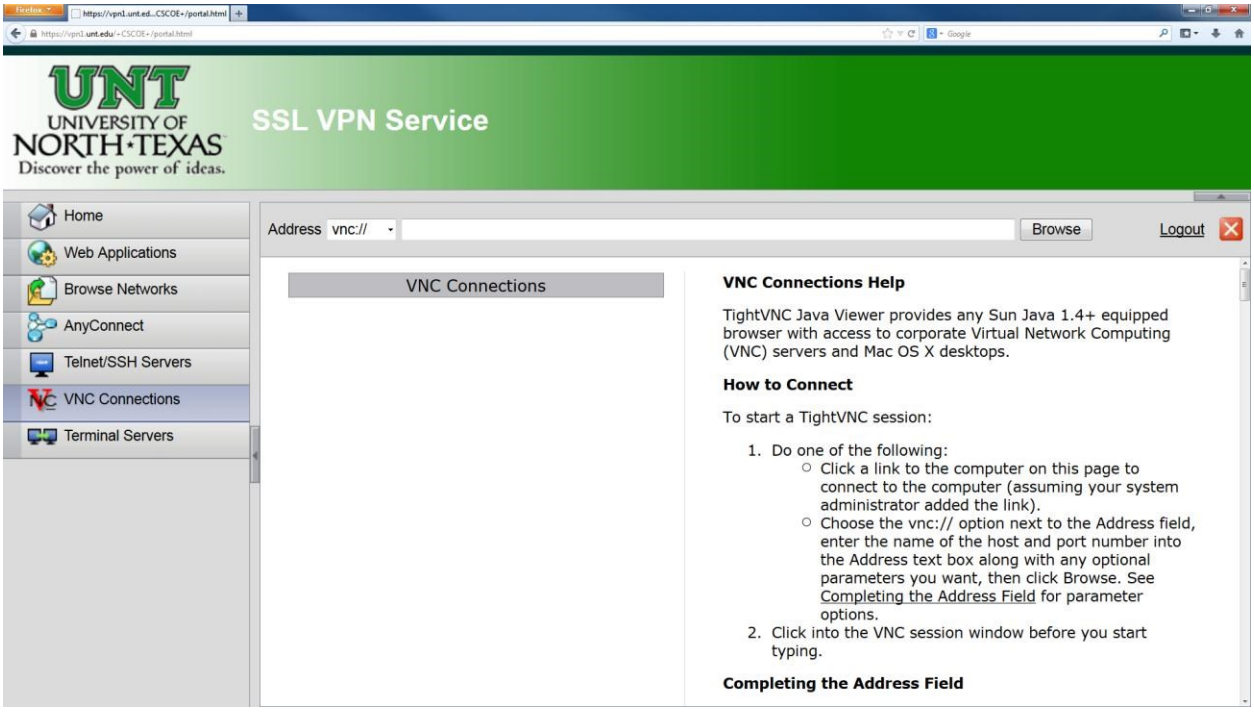
The next menu item is the Telnet/SSH page. This page will allow you to telnet or SSH to servers on campus. Just like all the other pages, just enter in the server address you are trying to SSH or telnet to in the address bar.



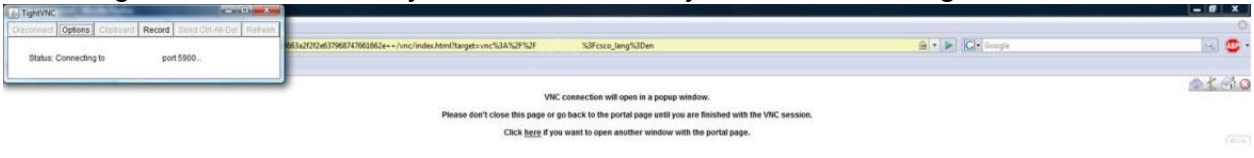
After you enter in the server address and hit enter a java applet will show up on page. Once it connects to the server you will get a login screen shown below. Enter in your username and password for that server and you will be logged in like normal.



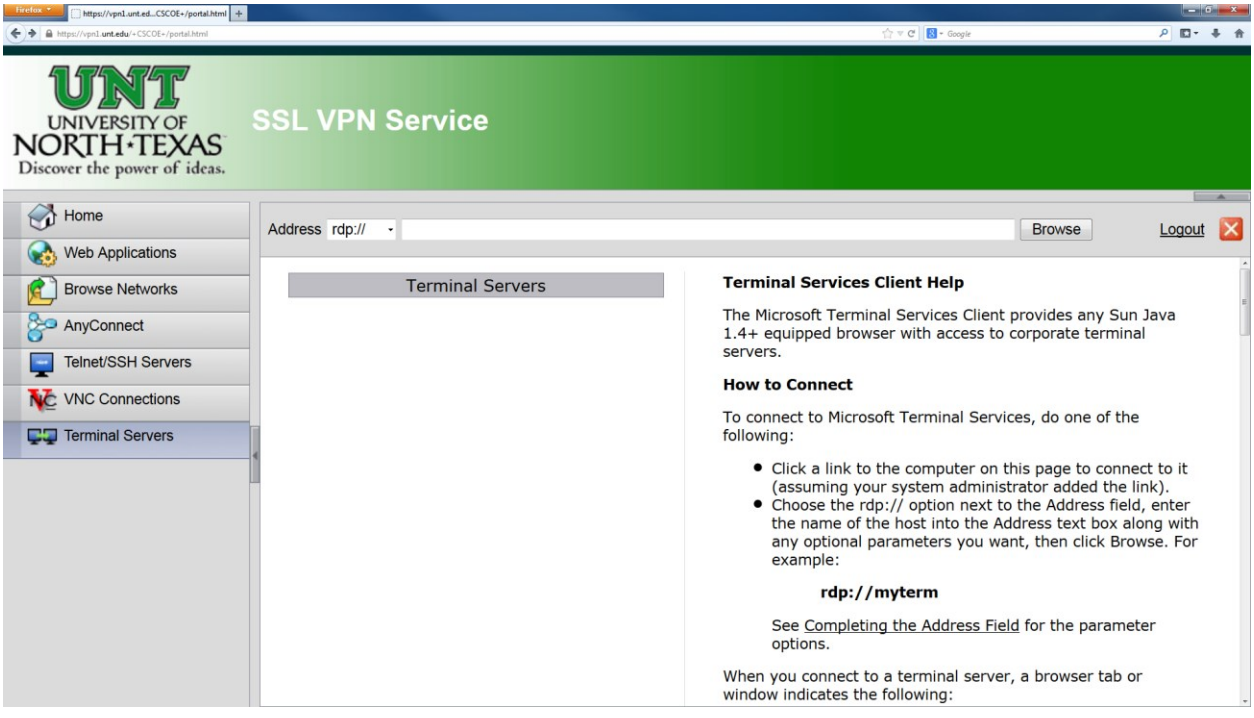
The next menu item the VNC connection page. This page allows you to use the Campus VPN as a VNC proxy.



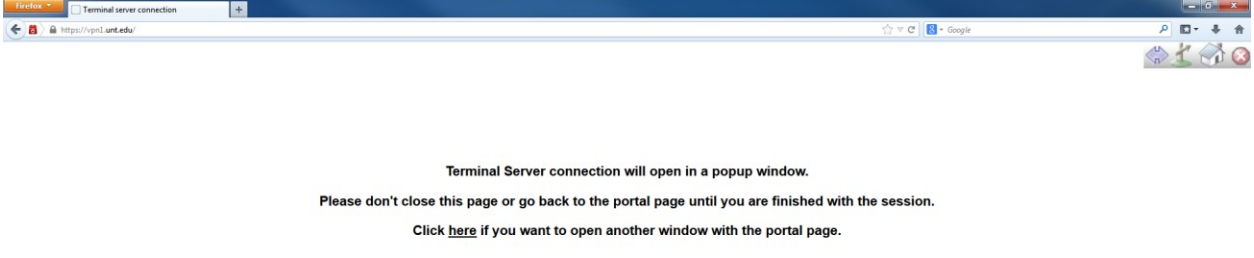
Once you enter in the address of the machine you are trying to VNC to you will be taken to a new page. The new page uses a Java program called TightVNC as shown below. Once TightVNC connects to your VNC machine you will need to login as normal.



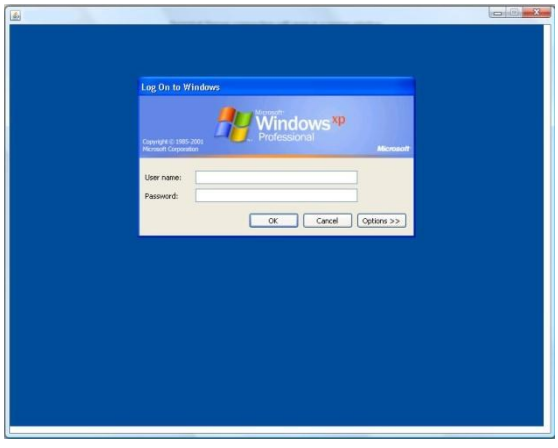
The final menu item is for terminal services usually called remote desktop. This page allows you to remote desktop to machines on campus that would otherwise be blocked from the outside.



After you enter in the address of the machine you want to remote desktop to, a page like the one below will appear. This page is showing that it's trying to connect to the machine you have entered.



Once connected, the Campus VPN will pop up java window showing your remote desktop connection to the machine. Below is an example of the remote desktop window.

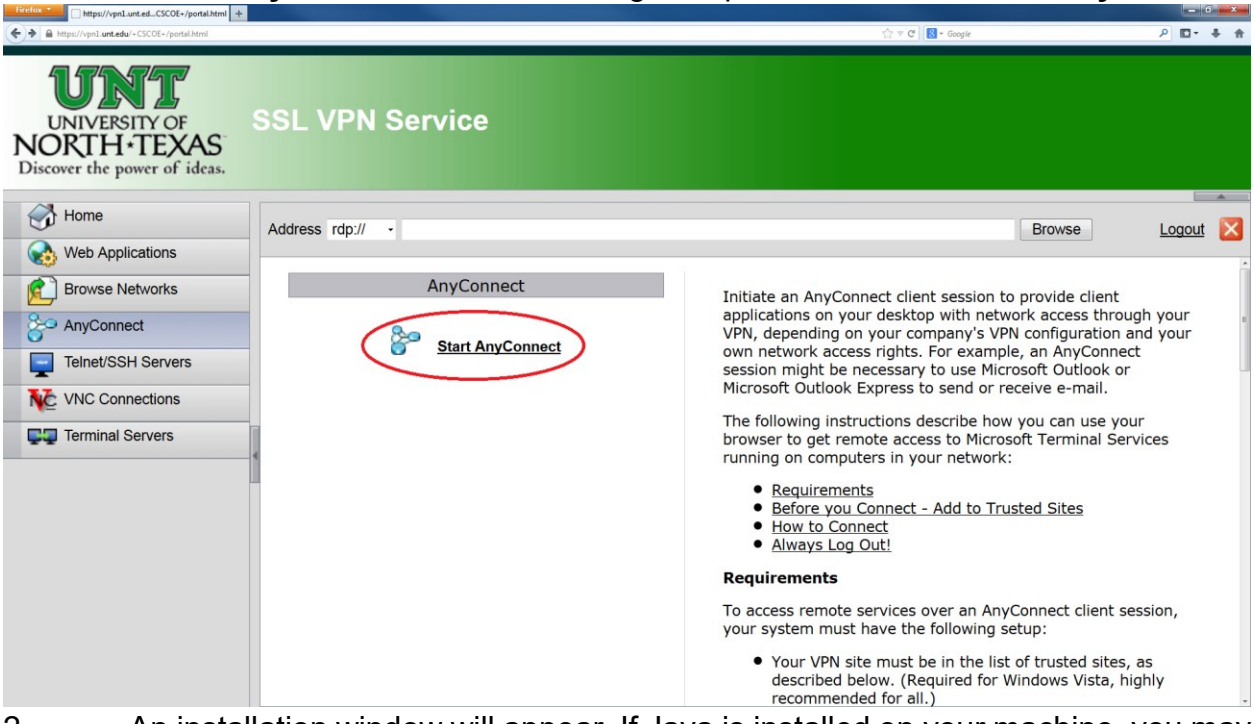


That is all the features of the Campus VPN web portal. The web portal is the easiest and fastest way to connect to on campus resources without having to worry about installing any software. It provides a secure encrypted connection from your machine to the resources you are accessing.

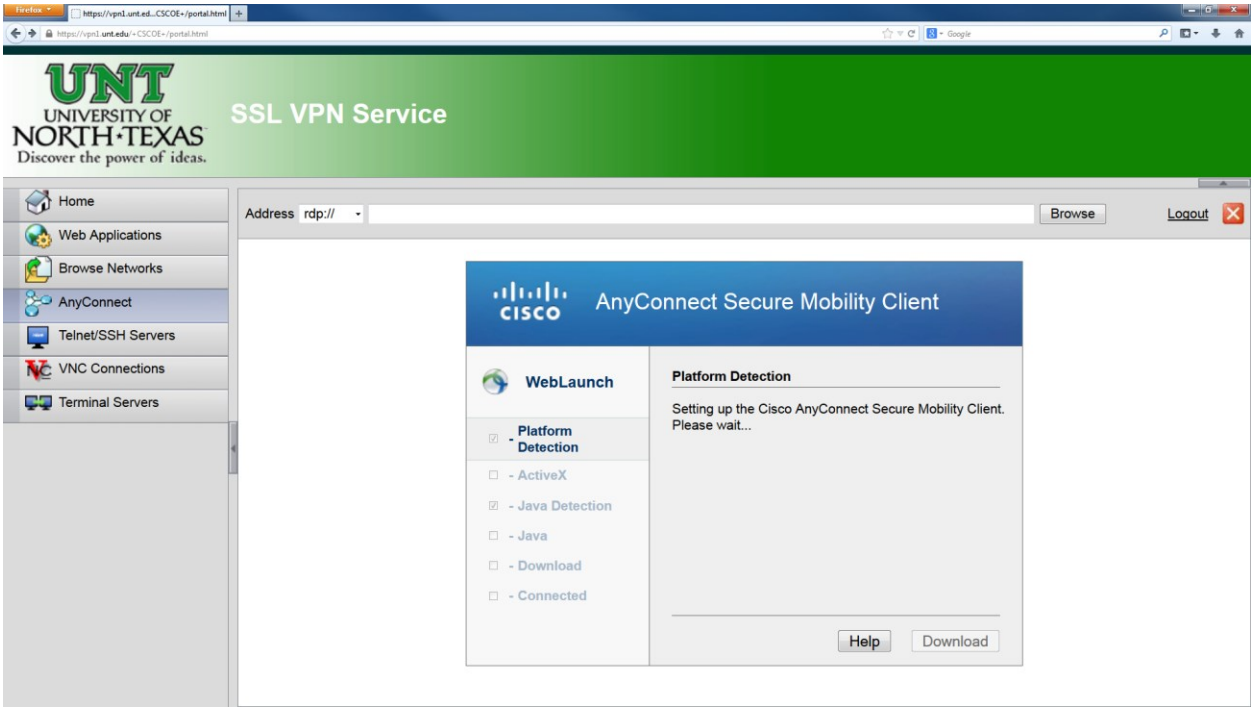
Installing AnyConnect VPNClient

As discussed earlier the AnyConnect client is an ActiveX or Java client that uses the SSL protocols to make an encrypted connection from your machine to the Campus VPN. To install the client you need to login to the Campus VPN web portal. If you need help logging in, please read the above section titled SSL Web Portal.

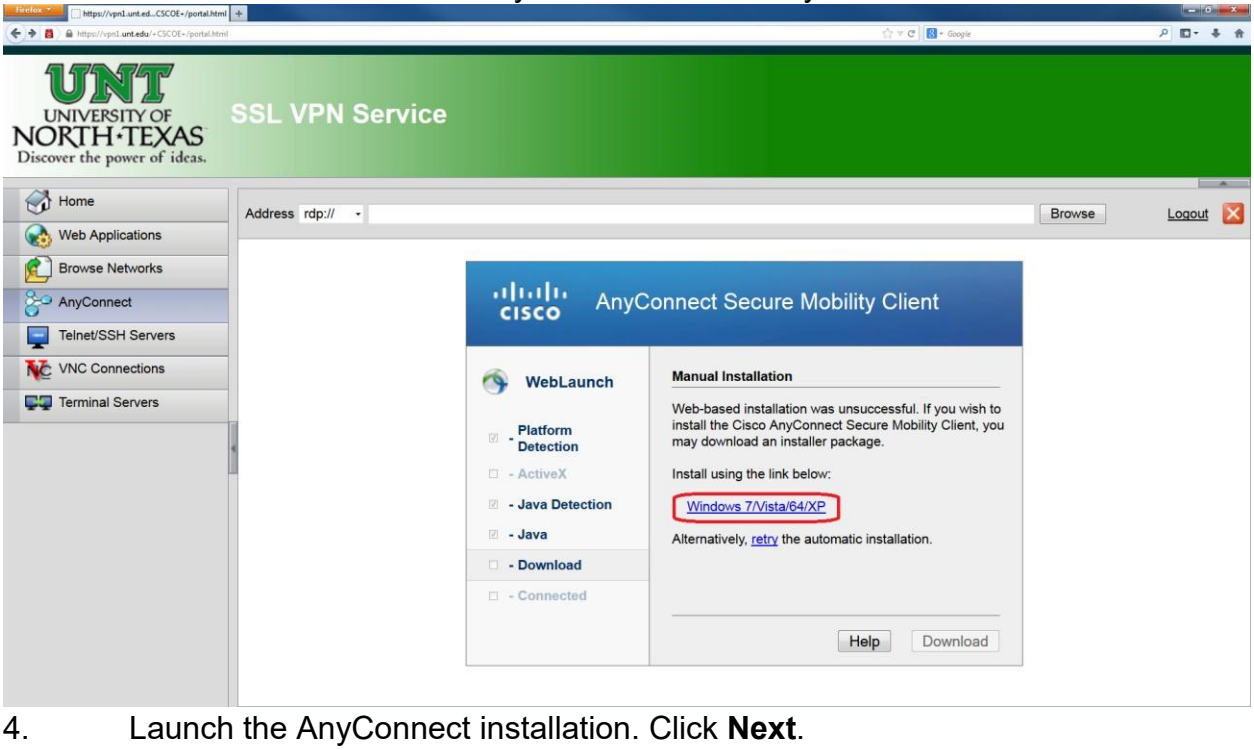
1. Select **AnyConnect** on the left navigation pane. Then, click **Start AnyConnect**.



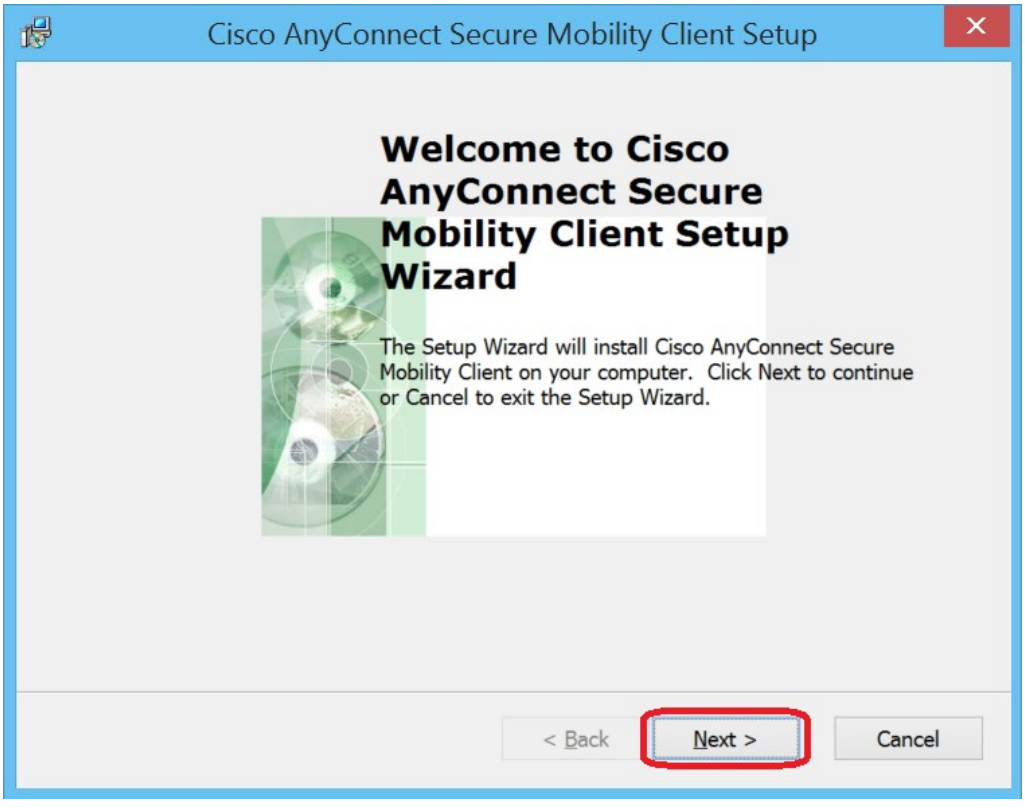
2. An installation window will appear. If Java is installed on your machine, you may follow the automatic installation prompts.



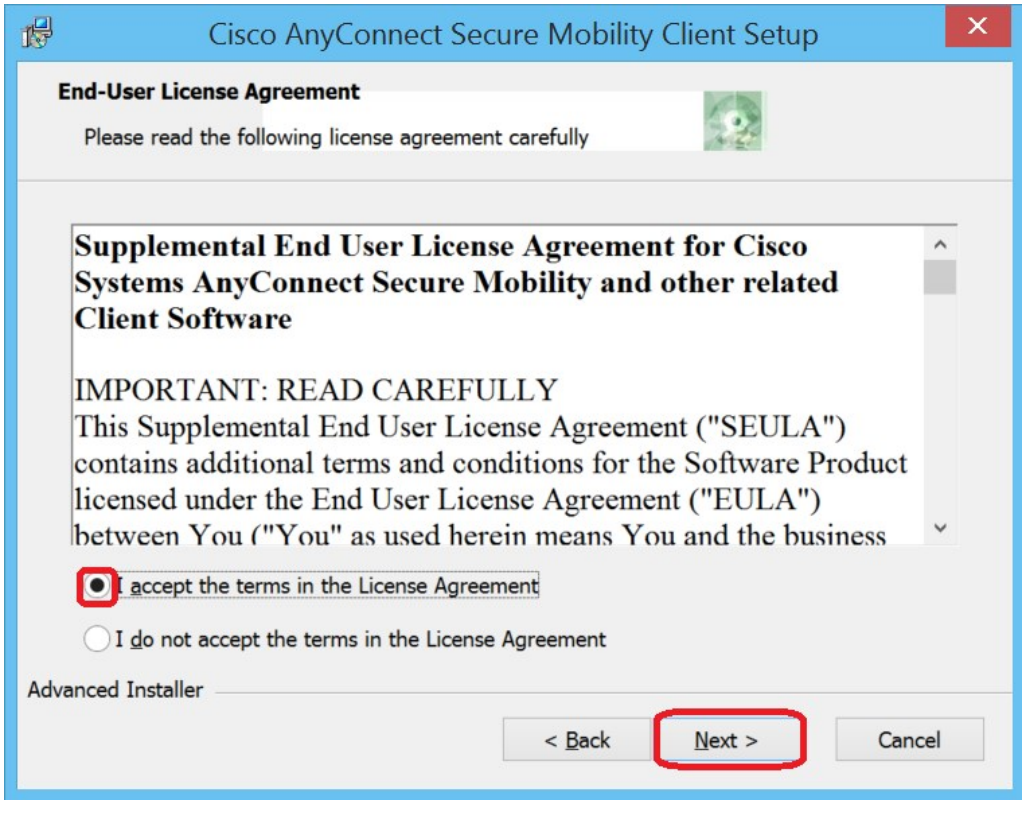
3. If the automatic web install fails for any reason, click on the **Windows 7/Vista/64/XP** link. You may either install directly or save the installation file.



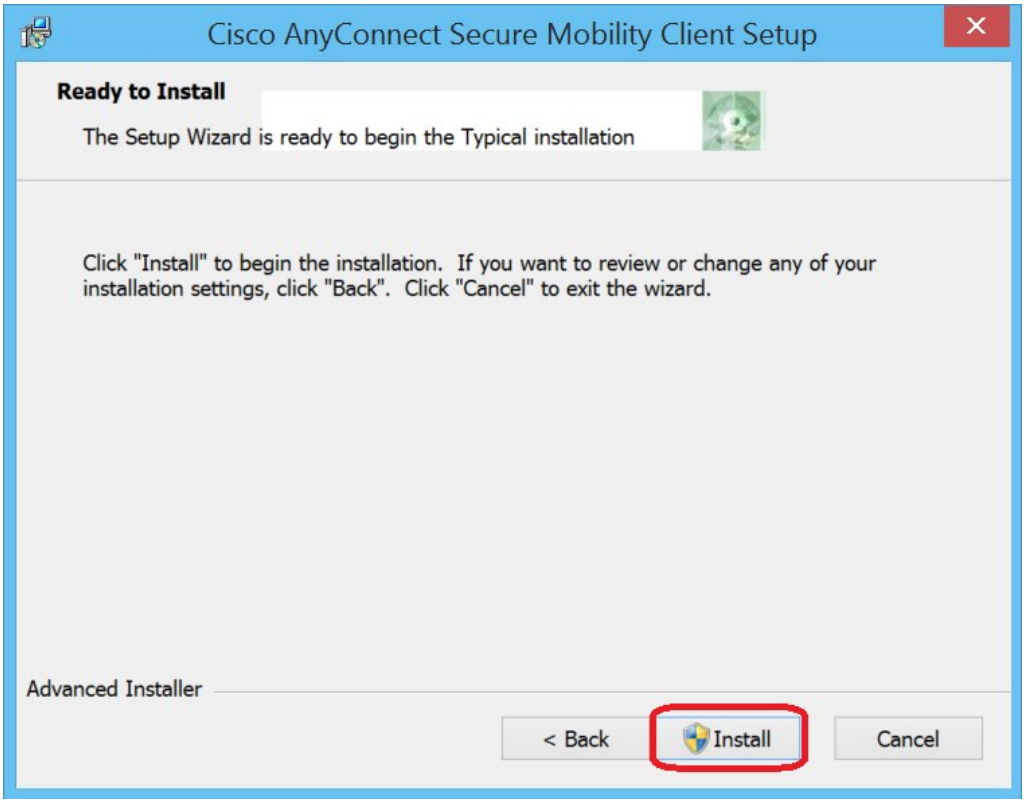
4. Launch the AnyConnect installation. Click **Next**.



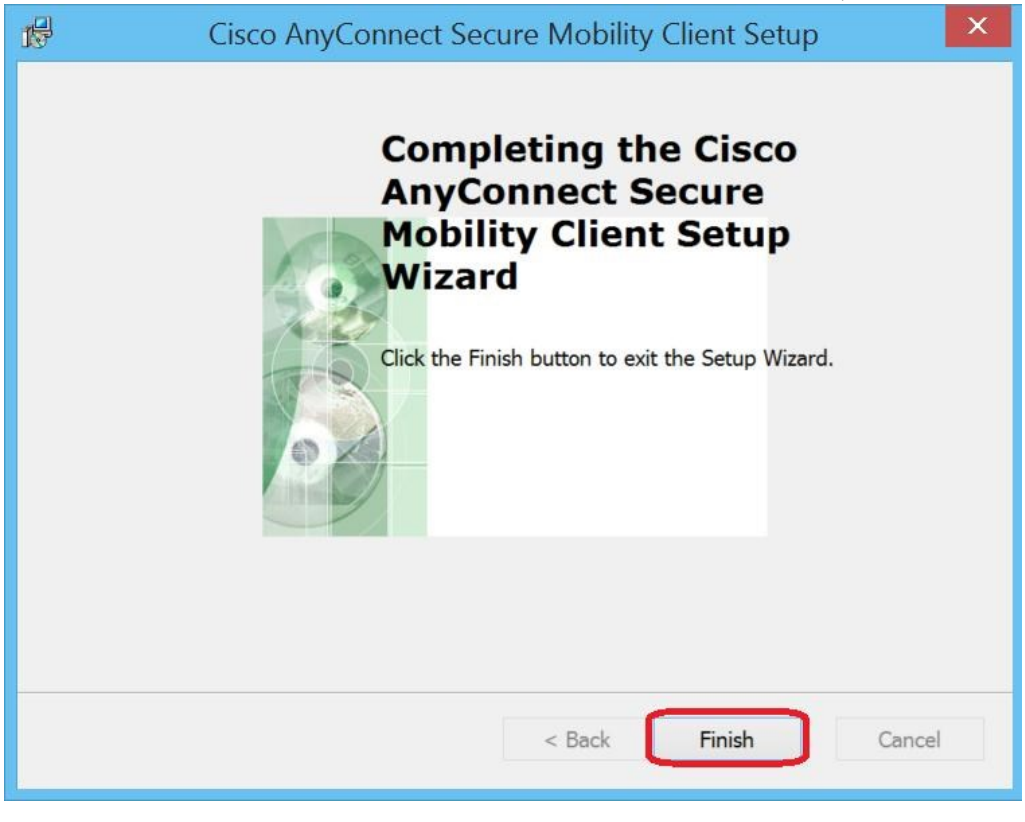
5. Click on the button for “I accept the terms in the License Agreement.” Then, click **Next**.



6. **Install**.



7. It will take a few seconds for the installation to finish. Then, click **Finish**.

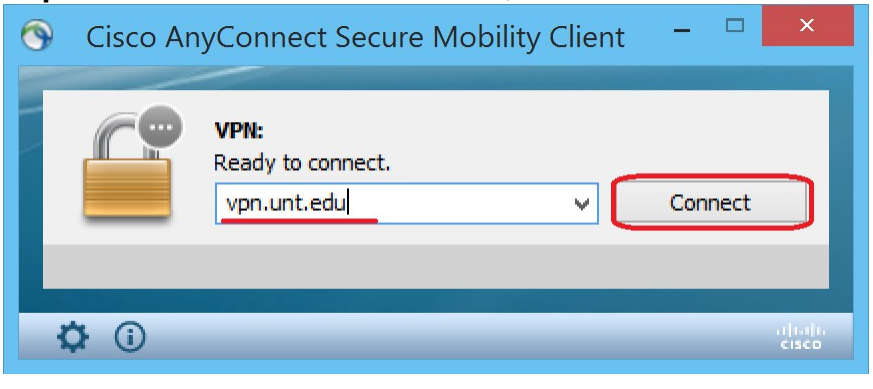


Click

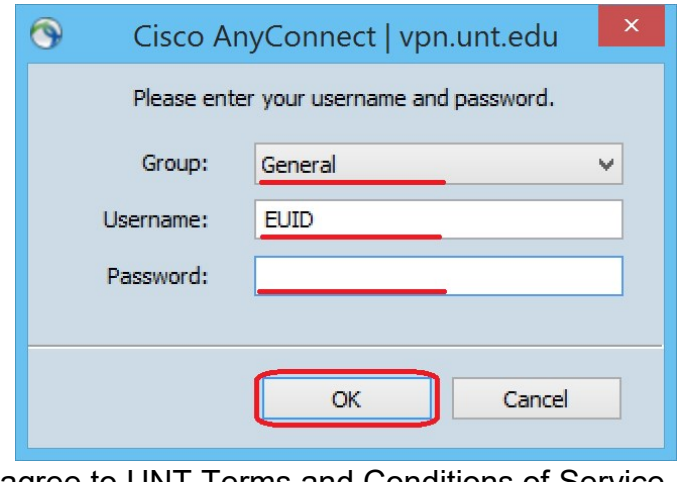
Connecting AnyConnect VPN client

1. Select the Cisco AnyConnect Secure Mobility Client from the Metro or Start menu.

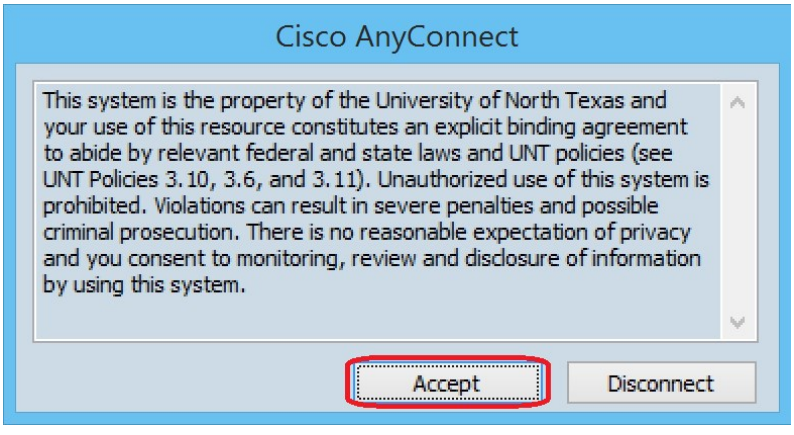
2. Enter **vpn.unt.edu** in the text box. Then, click **Connect**.



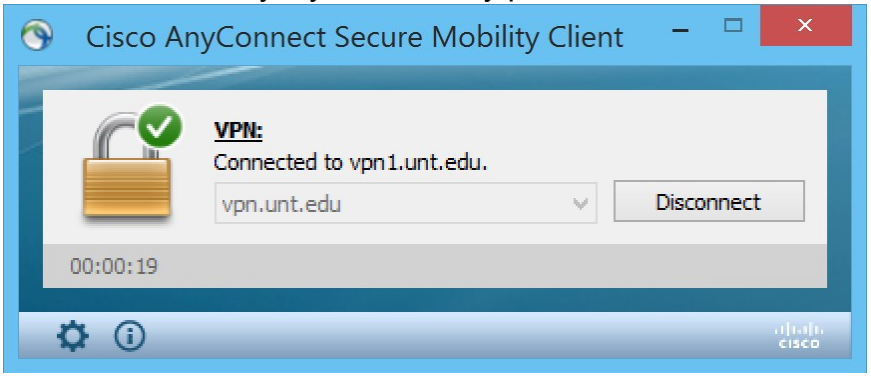
3. Enter your **EUID** and **EUID Password**. Then, click **OK**.



4. **Accept** to agree to UNT Terms and Conditions of Service.



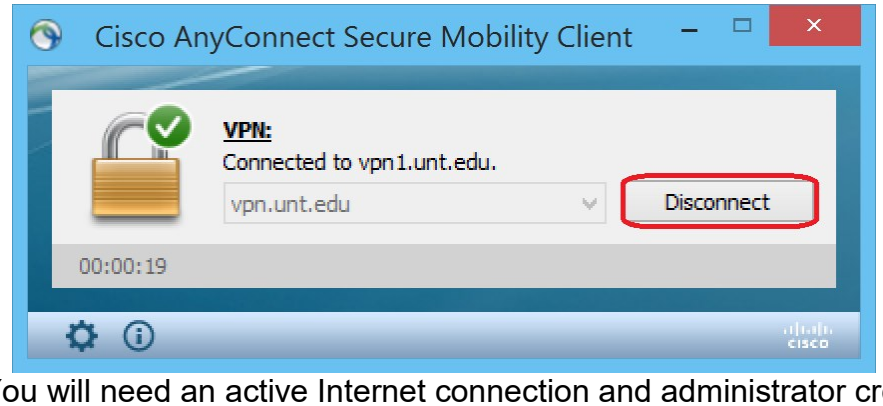
You will be connected to the Campus VPN and you are now logically on the UNT network. If you look at the bottom right side of your task bar you should notice an icon  . You can double click on that icon to bring up the AnyConnect client. Once the client is up you can see stats and details on what the Campus VPN gave you. This is a good way to make sure you are connected correctly if you have any problems.



To log off from the AnyConnect client, you can right click the icon and then select disconnect or bring up the AnyConnect client and click the "**Disconnect**" button

Apple OS X Configuration

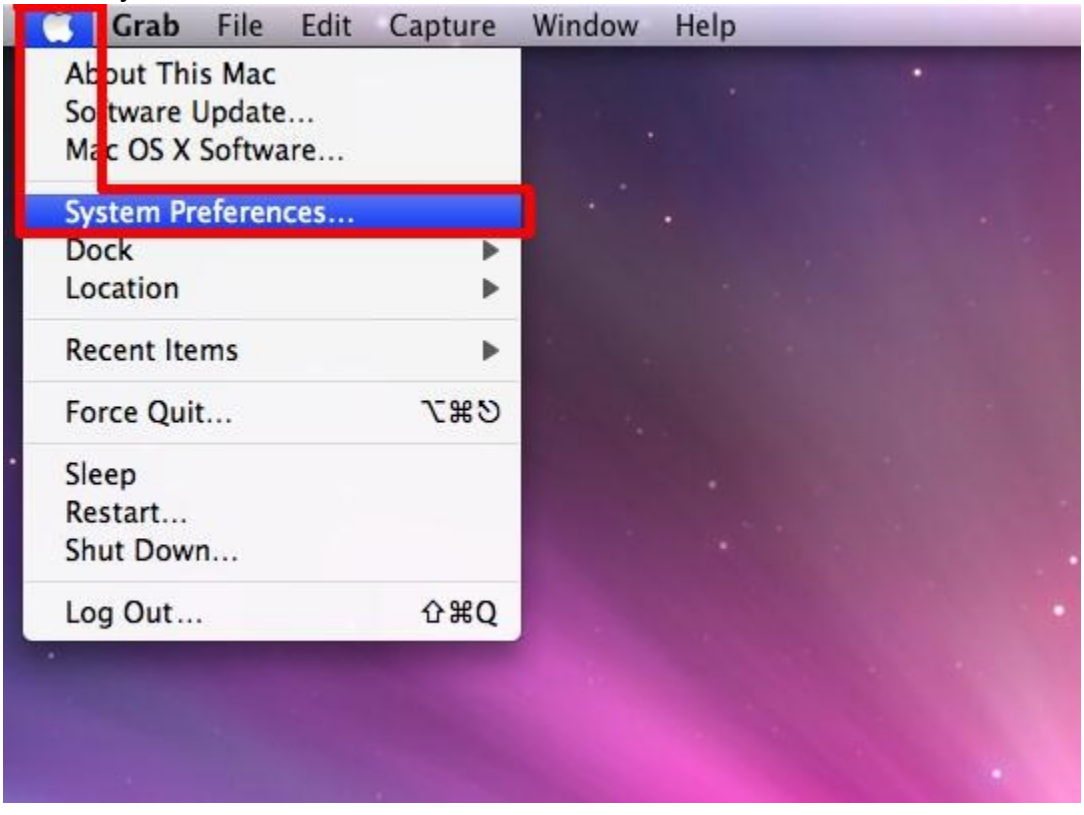
This series of steps applies to Apple OS X Snow Leopard, Lion, Mountain Lion, or



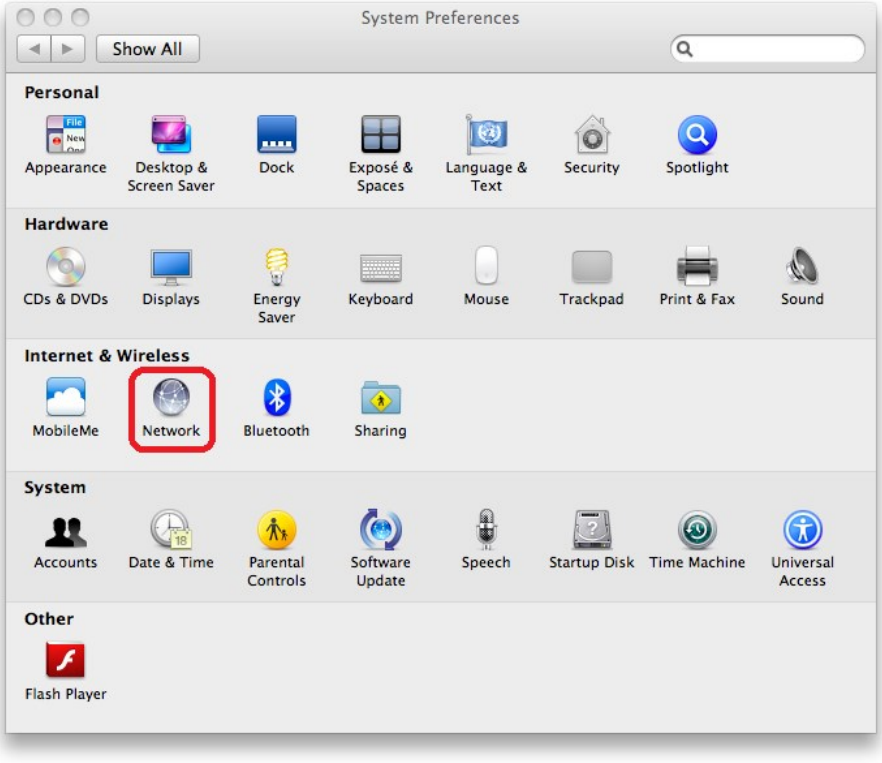
Mavericks. You will need an active Internet connection and administrator credentials to access the Campus VPN.

Click

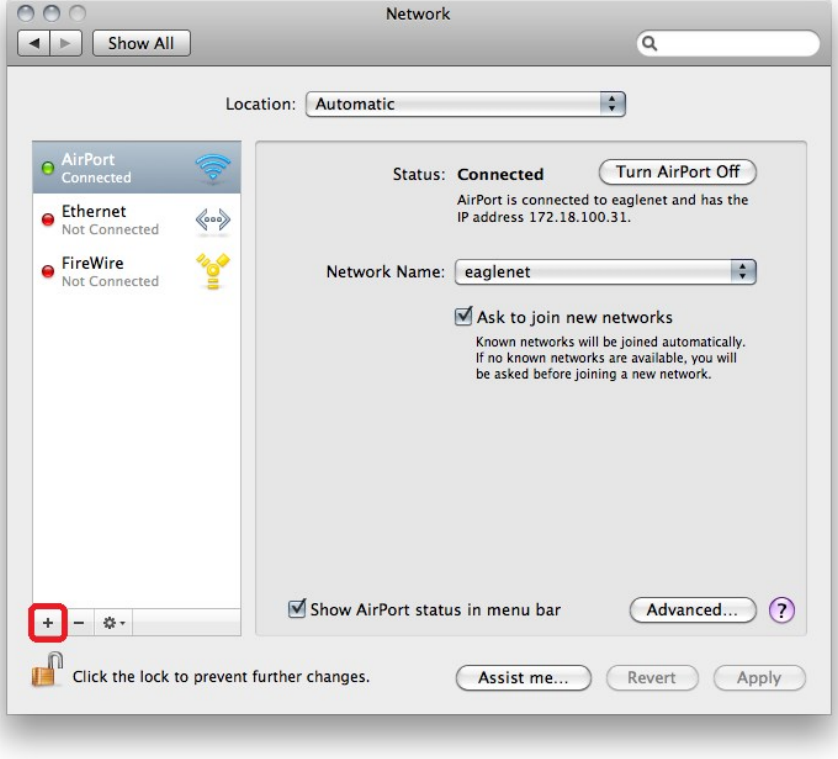
1. Access **System Preferences** by choosing it from the Apple menu or by opening it from your Dock.



2. **Network**.



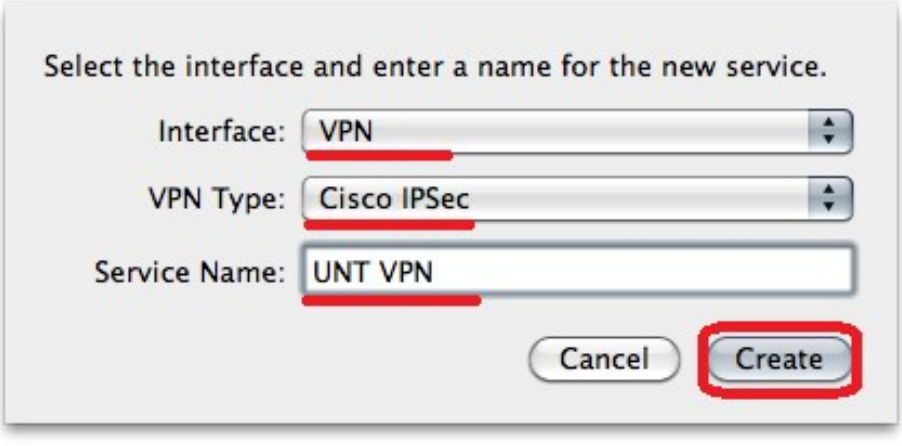
3. Click on the **plus sign (+)** in the bottom left corner to add a new connection.



4. Configure the following items. Then, click **Create**.

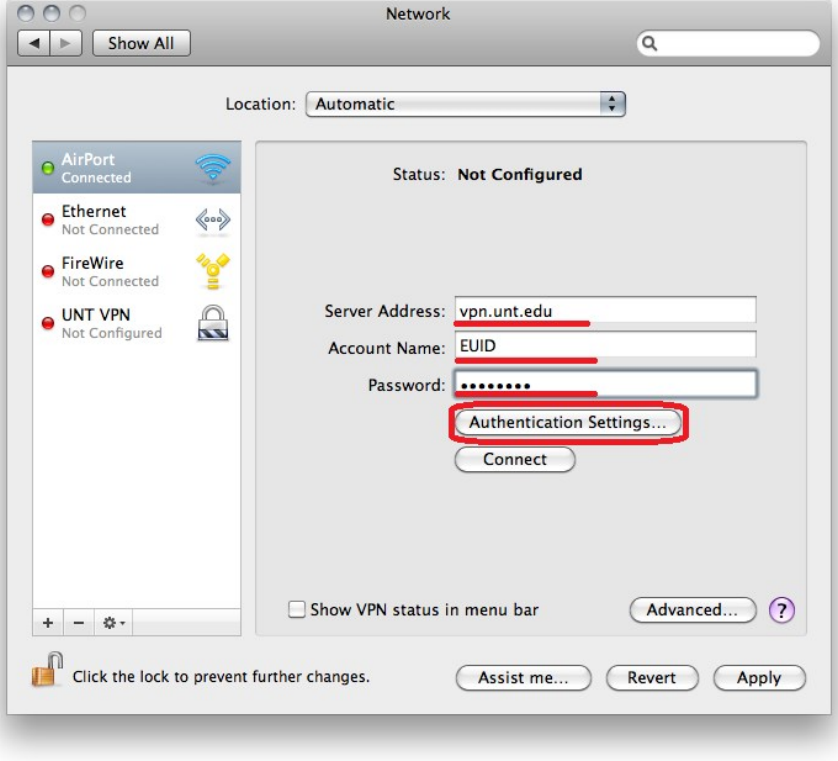
Click

Interface: **VPN** VPN
Type: **Cisco IPSec**
Service Name: **UNT VPN**



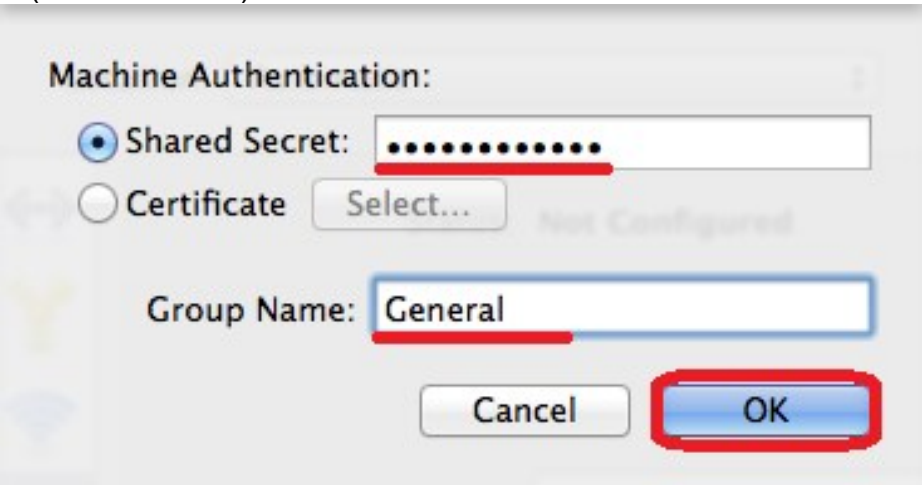
5. Configure the following items. Then, click **Authentication Settings**.

Server Address: **vpn.unt.edu**
Account Name: **EUID**
Password: **EUID Password**

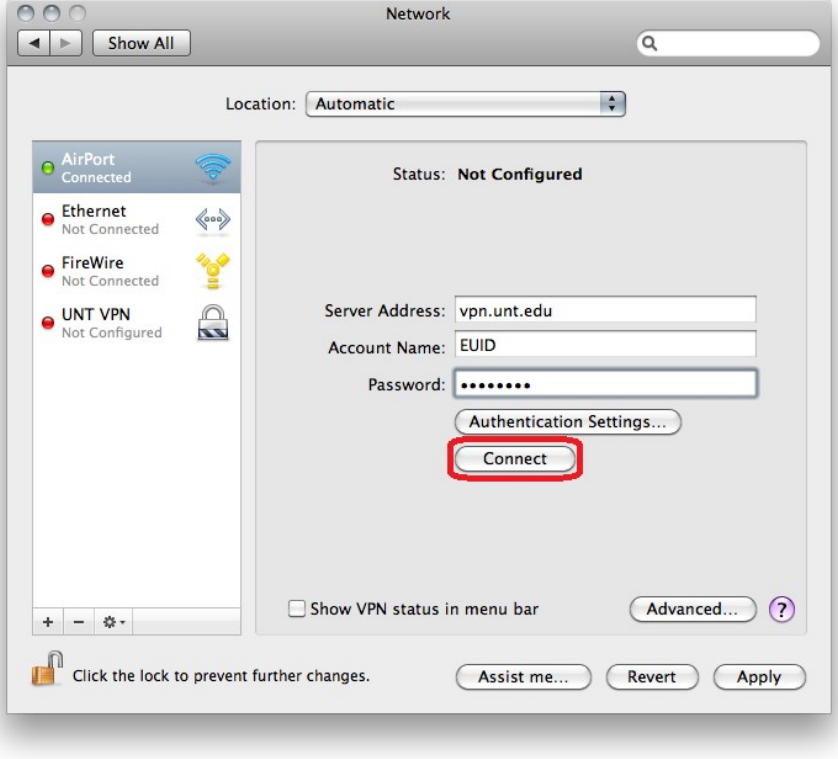


6. Configure the following items. Then, click **OK**.

Shared Secret (case sensitive): **untvpnaccess** Group
Name (case sensitive): **General**

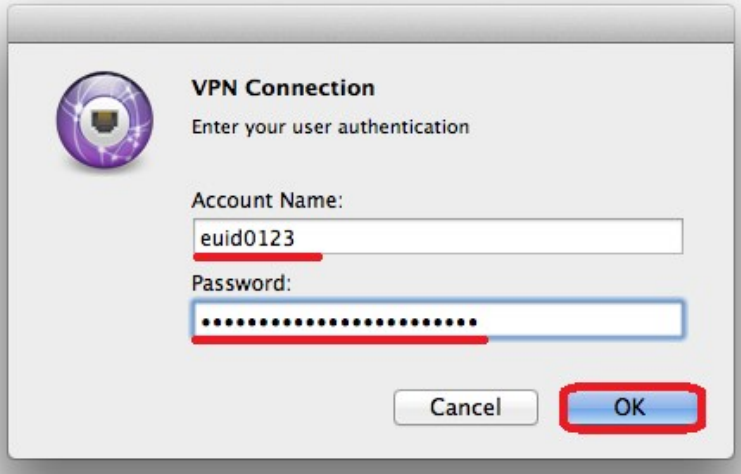


7. Click **Connect**.

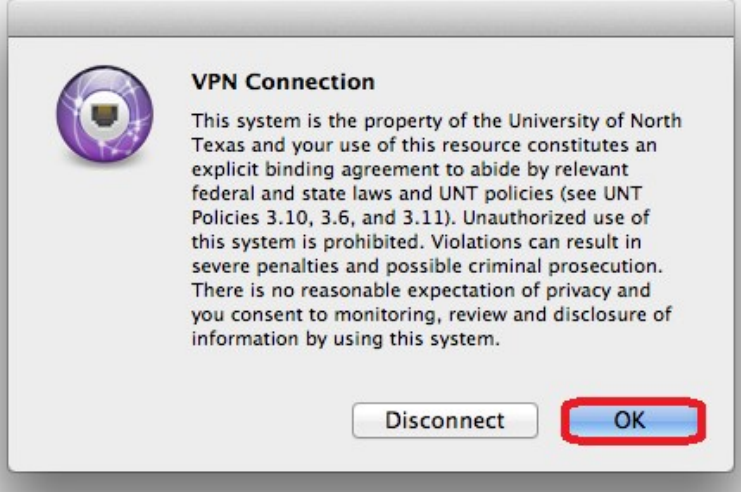


8. A prompt will appear. Configure the following items. Then, click **OK**.

Account Name: **EUID**
Password: **EUID Password**



9. Read the UNT Terms of Service. Click OK if you understand and agree to the Terms of Service.



Android Configuration

Most Android devices can also support a VPN connection using an app. While there are a variety of apps which can effectively connect to the UNT System Campus VPN, this guide continues to use Cisco AnyConnect.

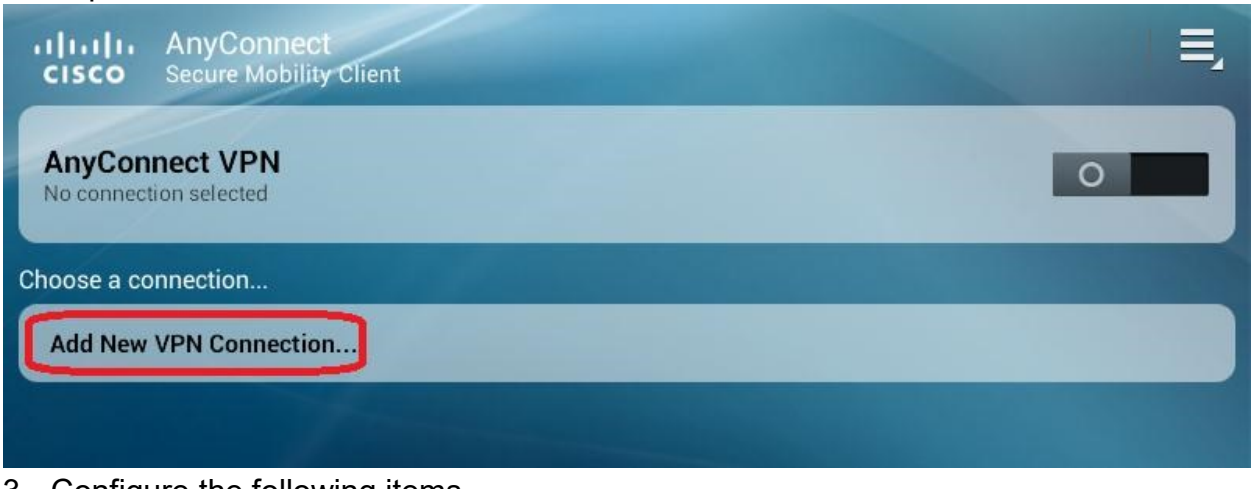
To download and install the Cisco AnyConnect app, go to the Google Play Store and find the appropriate app for the device.

https://play.google.com/store/apps/details?id=com.cisco.anyconnect.vpn.android.avf&hl=en

Cisco AnyConnect ICS is a free app and requires Android 4.0.3 or later. Not all manufactures of Android devices support ICS. Cisco offers alternative versions for some Samsung devices and rooted devices.

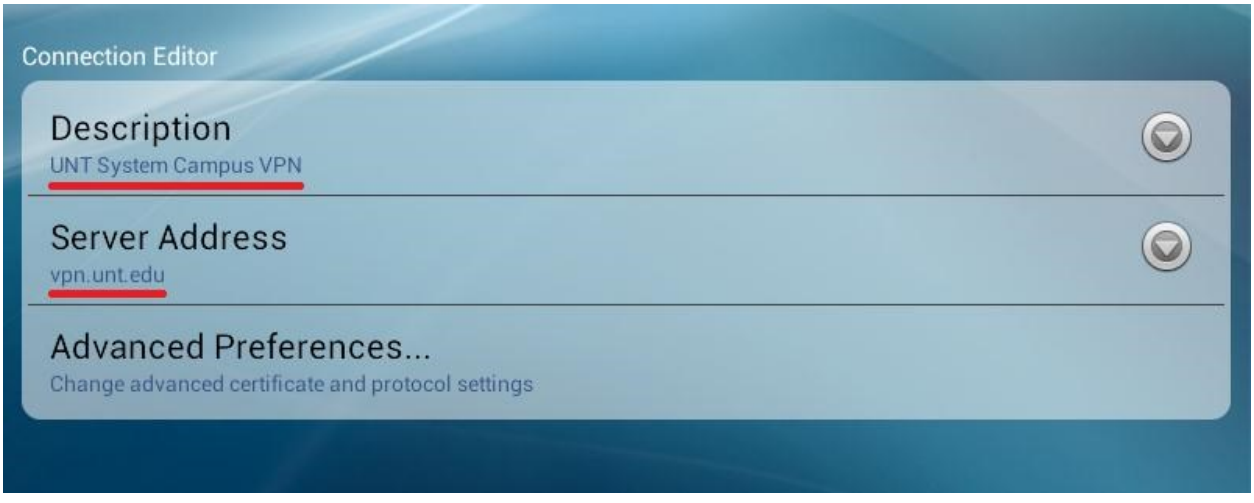
1. Launch the Cisco AnyConnect Secure Mobility Client app.

2. Tap **Add New VPN Connection.**



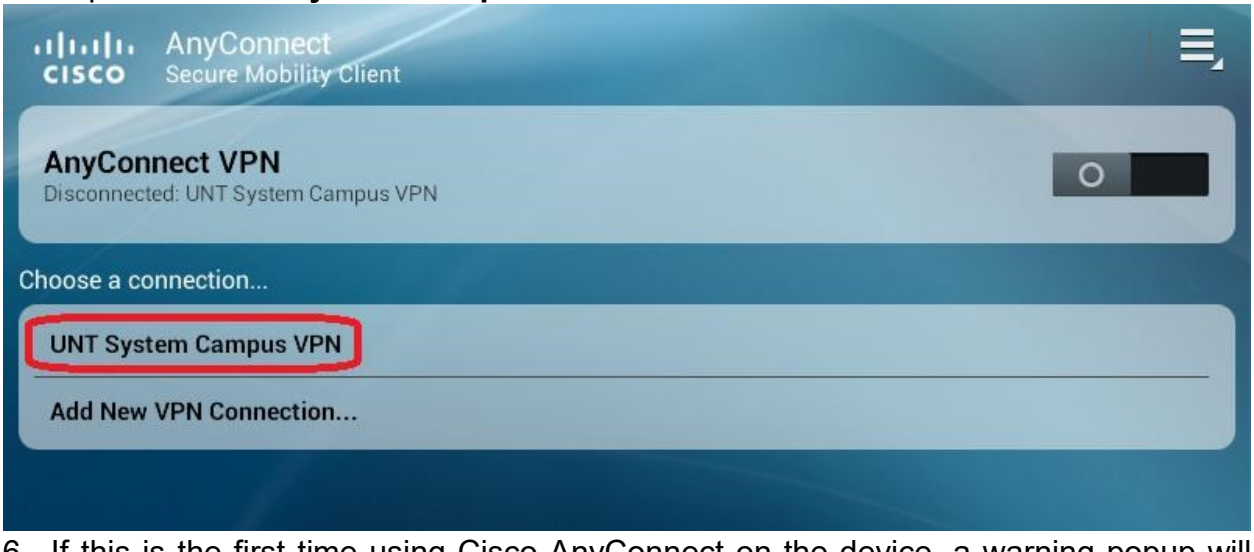
3. Configure the following items.

   Description: **UNT System Campus VPN** Server
   Address: **vpn.unt.edu**

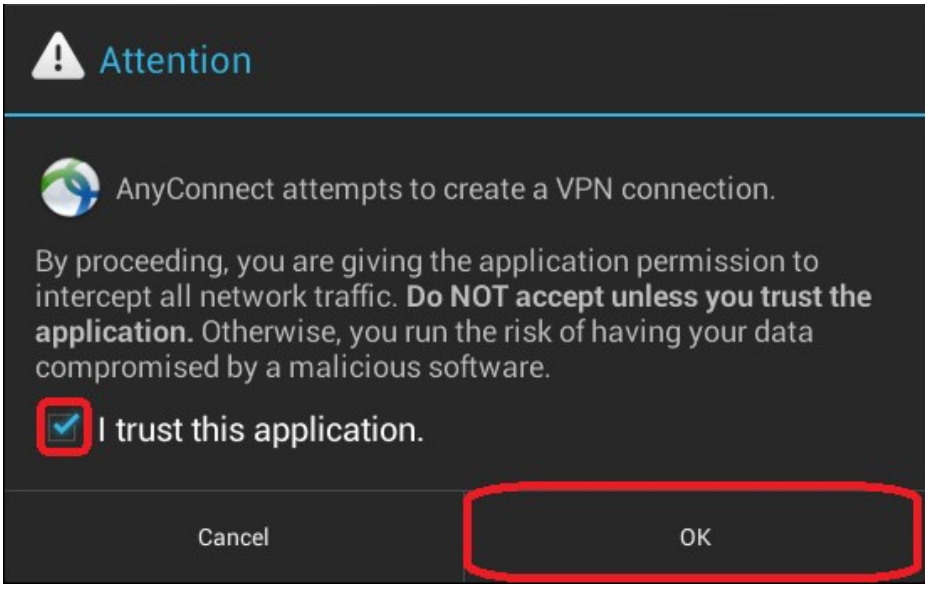


4. Tap **Done** at the bottom of the screen.

5. Tap on the **UNT System Campus VPN** button.

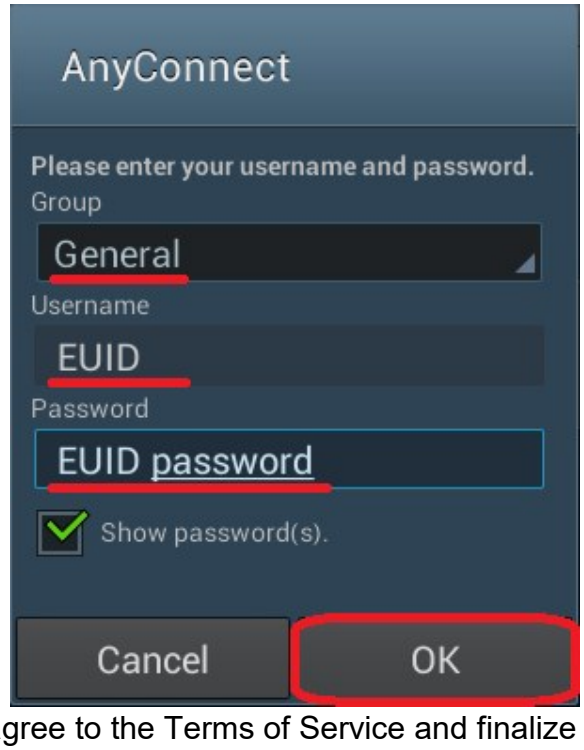


6. If this is the first time using Cisco AnyConnect on the device, a warning popup will appear. Check the box **I trust this application** and select **OK.**

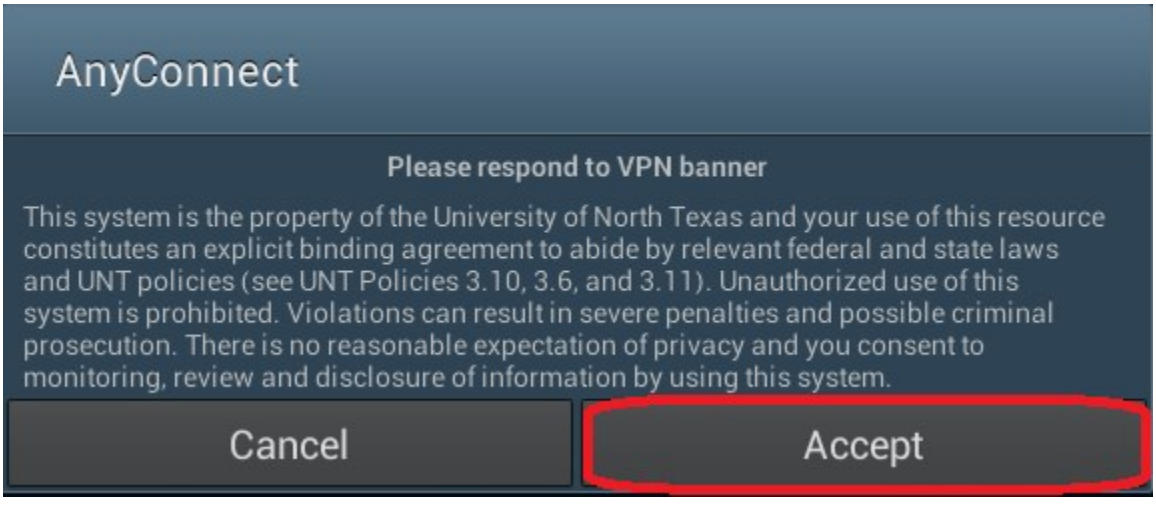


7. Configure the following items in the new prompt. Then, click **OK**.

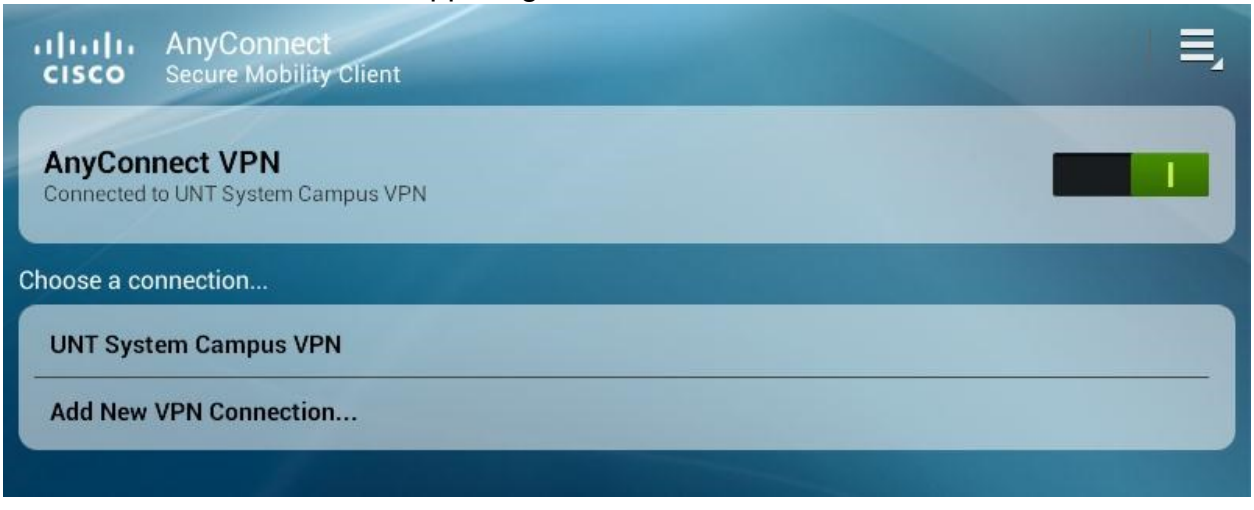
   User Group: **General** Username: **EUID**
   Password: **EUID Password**



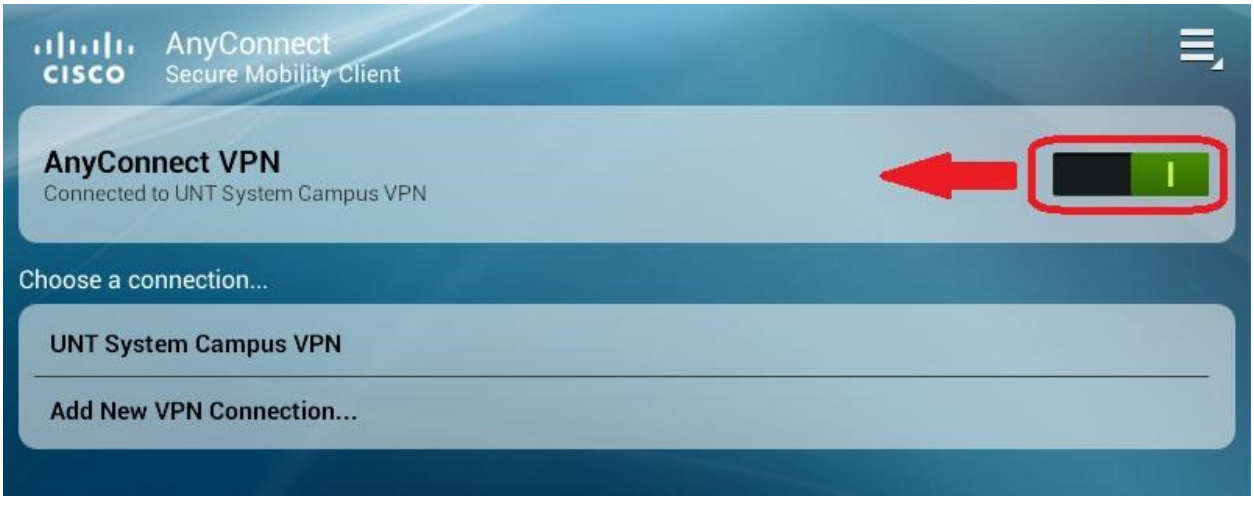
8. Tap **Accept** if you agree to the Terms of Service and finalize your VPN connection.



9. The main button will now appear green to confirm an active VPN connection.



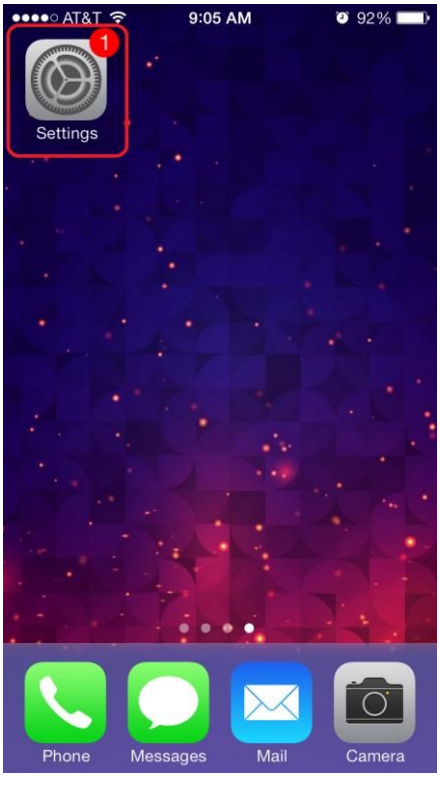
10. To close the connection, swipe the green tab to the left.



Apple iOS Configuration

This guide details setting up the UNT System Campus VPN using the built in iOS VPN functionality. Alternatively, you may use the Cisco AnyConnect Secure Mobility Client app available for free in the Apple App Store.

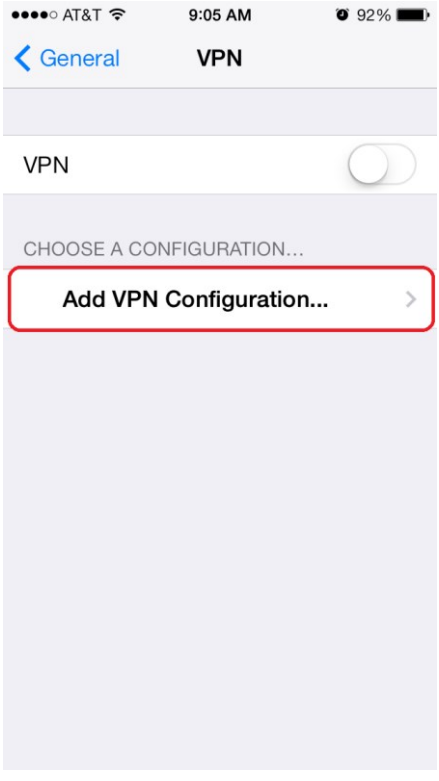
1. Tap **Settings** on your iPhone / iPad / iPod Touch.



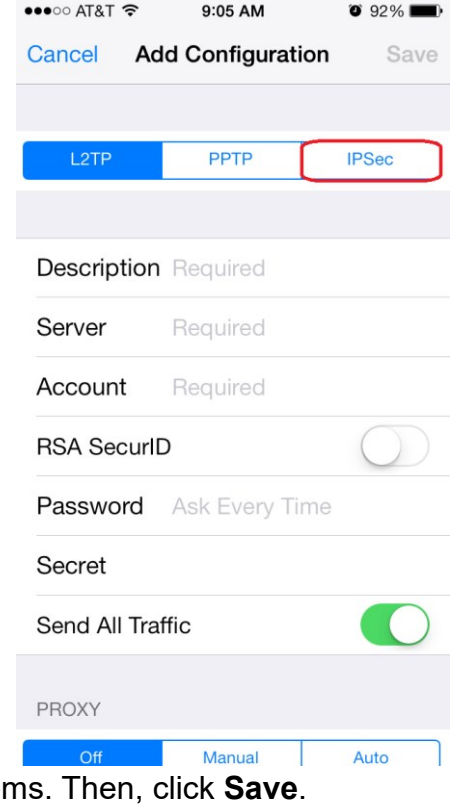
2. Tap **General**

3. Tap **VPN** (some devices will have **Network** listed in the General menu, then tap **VPN**).

4. Tap **Add VPN Configuration…**

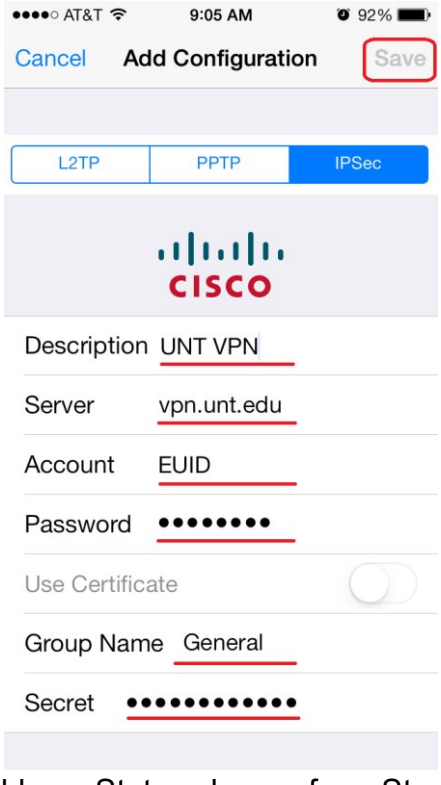


5. Select **IPSec** from the options at the top of the screen.



6. Configure the following items. Then, click **Save**.

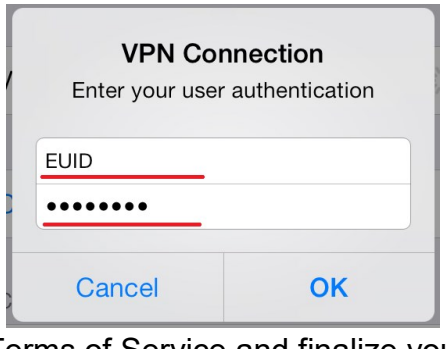
Description: **UNT VPN**
Server: **vpn.unt.edu** Account:
EUID
Password: **EUID Password**
Group Name (case sensitive): **General**
Secret (case sensitive): **untvpnaccess**



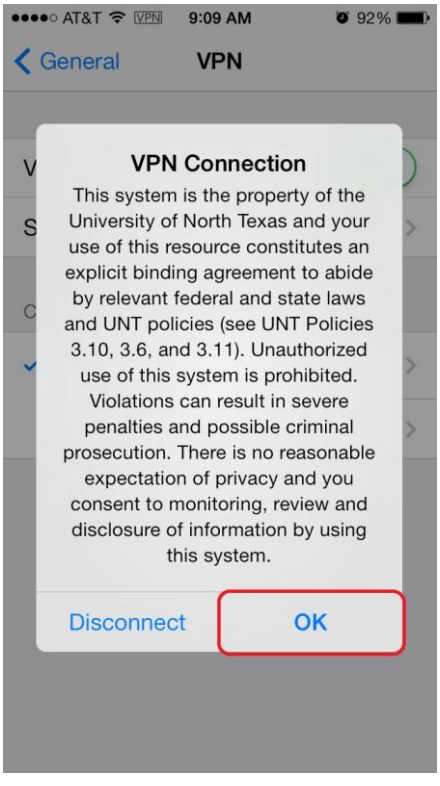
7. Swipe **VPN** to **On**. You should see Status change from Starting to Connecting.

8. A prompt will appear. Configure the following items. Then, click **OK**.

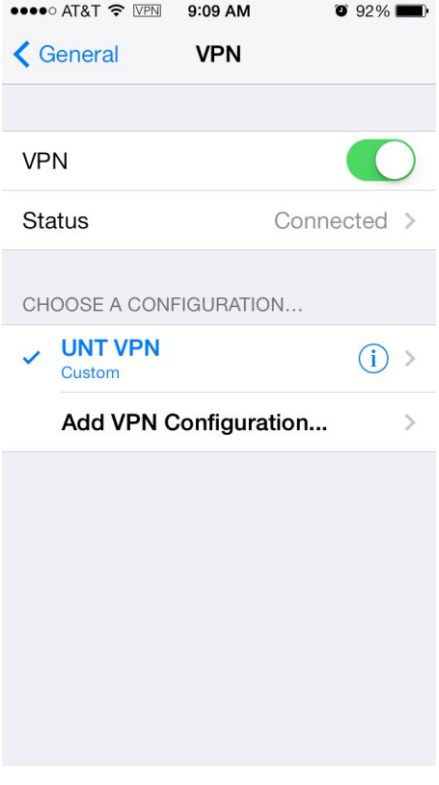
   Account Name: **EUID**
   Password: **EUID Password**



9. Tap **OK** if you agree to the Terms of Service and finalize your VPN connection.



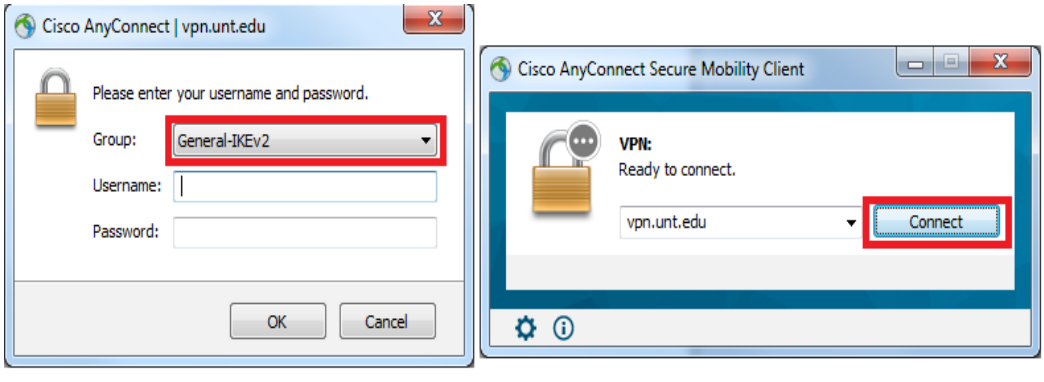
10. You should now see Status: **Connected**



IKEv2(Internet Key Exchange Version 2)

AnyConnect has been configured to use IKEv2 encryption protocol to connect to the VPN appliance securely. IKEv2 use UDP port 500 for connectivity. This protocol is good at automatically reestablishing a VPN connection when users temporarily lose their internet connections. In order to use this feature, a user has to select the “General-IKEv2” Group from the drop down box and connect to the VPN. When a user use the General-IKEv2 Group and connect to the VPN for the first time, the system will push an XML profile to the users PC. The AnyConnect will use the XML profile pushed to the users PC for all future VPN connections. There are 2 step to use the IKEv2 .

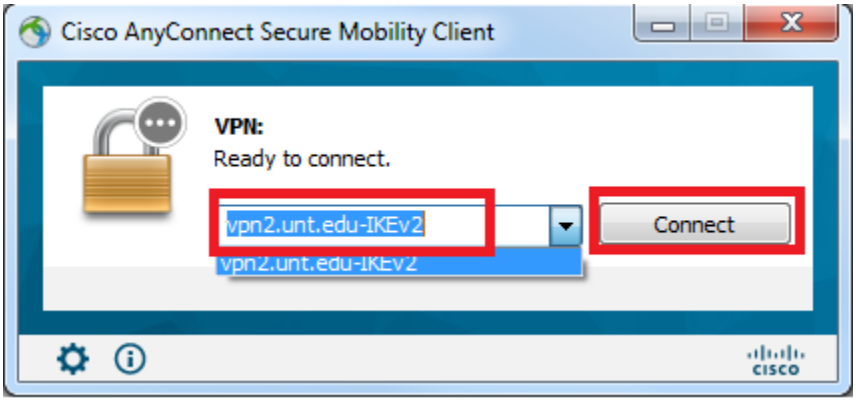
1)The first step is to push the XML profile.



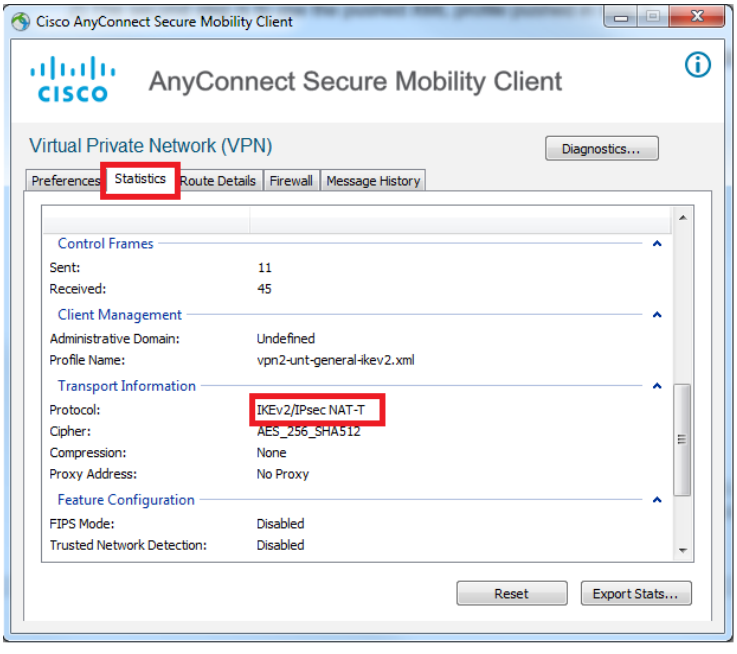
Once connected to the group “General-IKEv2”, the XML profile is pushed to the PC but still connected to the VPN using SSL protocol because the IKEv2 profile is only pushed but not used.

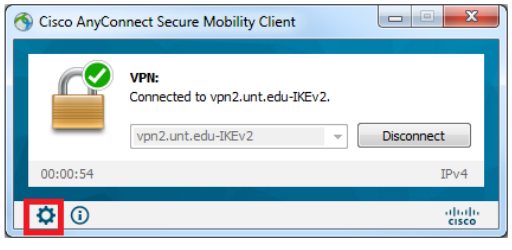
2) The second step is to use the pushed XML profile pushed in step 1

Once the XML profile is pushed, you will be able to see and select from the drop down box as bellow before you login with your EUID and password



Checking if the connection use IKEv2



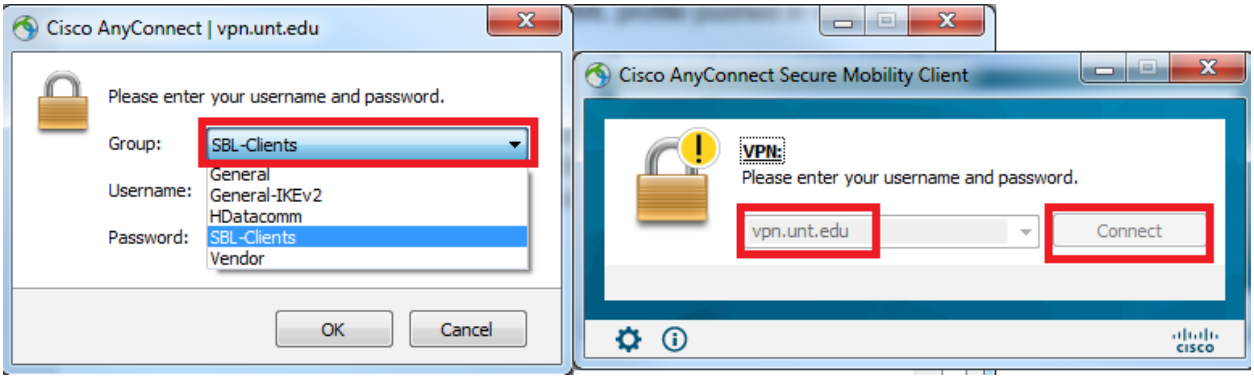


SBL(Start Before Logon)

Start Before Logon feature is added to the AnyConnect to allow users to connect to the VPN before login to Windows (Windows only feature). This feature help the user to access mapped network drives once connected to VPN and login to the windows.

There are 2 steps in using the SBL feature. The first one is to download the SBL XML profile and the 2nd step to use the SBL feature.

1) The user has to select the Group “SBL-Clients” from the drop down box before login to the AnyConnect . once connected, the XML profile is pushed to the users PC



2) Once the XML profile is pushed to the user's PC. The user has to restart the PC. Once the PC is rebooted, the user will be able to see the following icon on the Widows login screen when you press Alt+ Ctrl (or Alt +ctrl + del) . The user has to click on the network icon and login to the VPN first and then login to the Windows.