MSU Authorized User Campus Access Procedure, Campus VPN

This document provides the requirements and procedures for access to the Campus Network for MSU Authorized Users. Access to the Campus Network is provided by a connection to the Campus VPN through the MSU VPN Service web site or the Cisco AnyConnect client.

Please refer to the MSU IT Data Center and Campus Network Remote Access Policy for more information.

Requirements

Access to the Campus Network via VPN requires:

- An MSU NetID
- Enrollment in Duo for Two-Factor Authentication (2FA)
- Utilizing the MSU VPN Service web interface or installing and utilizing the Cisco AnyConnect client

Process Overview

To obtain access to the VPN:

1. Submit a request to the ISIM group via an incident in ServiceNow using the **Data Center and Campus Network Access Request** template.
2. If you have not yet enrolled in Duo for Two-Factor Authentication, do so upon receiving the enrollment email.
3. Decide on your preferred connection method detailed below and proceed to follow the instructions.

Enrollment for Duo for Two-Factor Authentication (2FA)

All logins to the Campus VPN require the use of an additional factor of authentication from the user. IT provides users with a Duo account to accomplish this. Two-factor authentication increases security for both the campus network and the user's account by ensuring that a potentially compromised NetID and password combination alone cannot be used to access two-factor protected resources such as the campus VPN.

Refer to the document Duo Enrollment for Two-Factor Authentication (2FA). Upon receiving a VPN provisioning request, ISIM will also provision your MSU NetID into Duo if not previously enrolled, and you will receive an enrollment email. Follow the steps in the above document to enroll your mobile device for use with Duo.

Connection methods

There are two methods to connect to the campus VPN.

The **Cisco AnyConnect client** provides a full service VPN connection to a computer. Once connected, the computer is essentially on the campus network. Generally, any service you would use from a computer directly attached to the campus network is reachable from a remote location.

The **SSL VPN Web Interface** provides the ability to connect to web sites only. This is useful when you must reach a campus web service that is not available externally but you are not on a computer that you can install the Cisco AnyConnect client on (i.e. kiosk, public computer, managed computer, etc.)

Connecting to the VPN with Cisco AnyConnect

The Cisco AnyConnect client **comes pre-installed on University provided computers that are running the latest IT Secured/Managed image**. If the client is not installed on your University provided computer, contact the IT Service Desk at (973)655-7971, opt. 1 or your local College technical team for installation assistance.

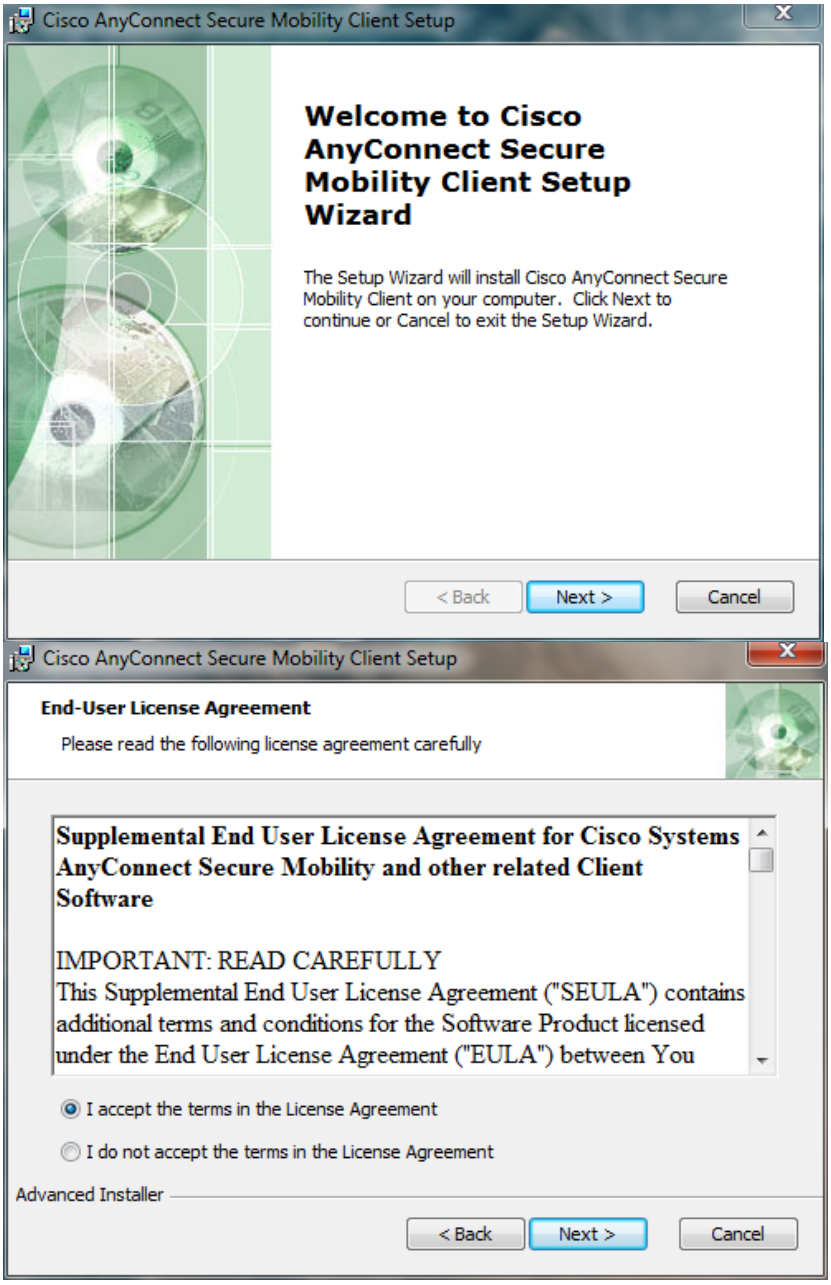
For installation on non-University provided (personally owned) computers, you may also download it directly from the following links:

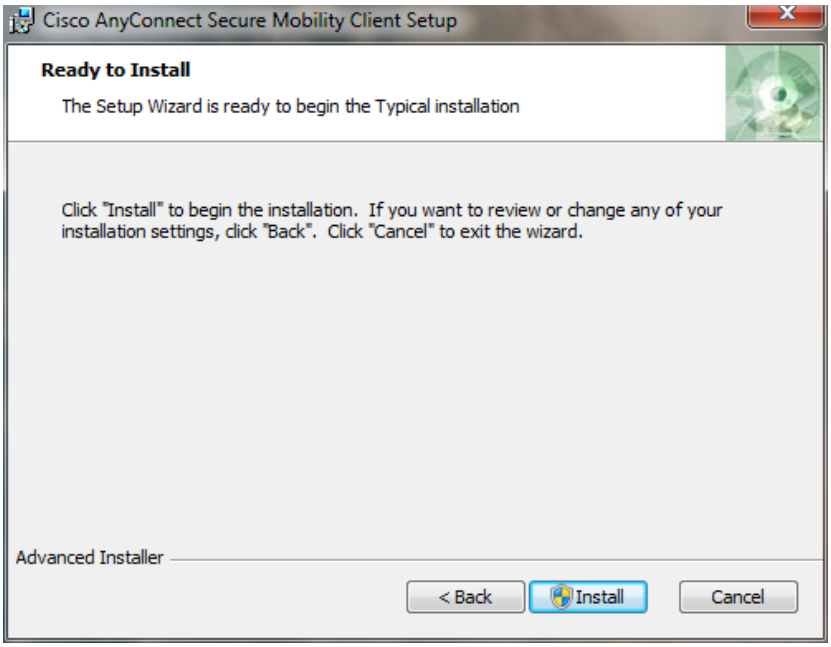
Windows
Mac OS X

Installing the AnyConnect Client

Windows

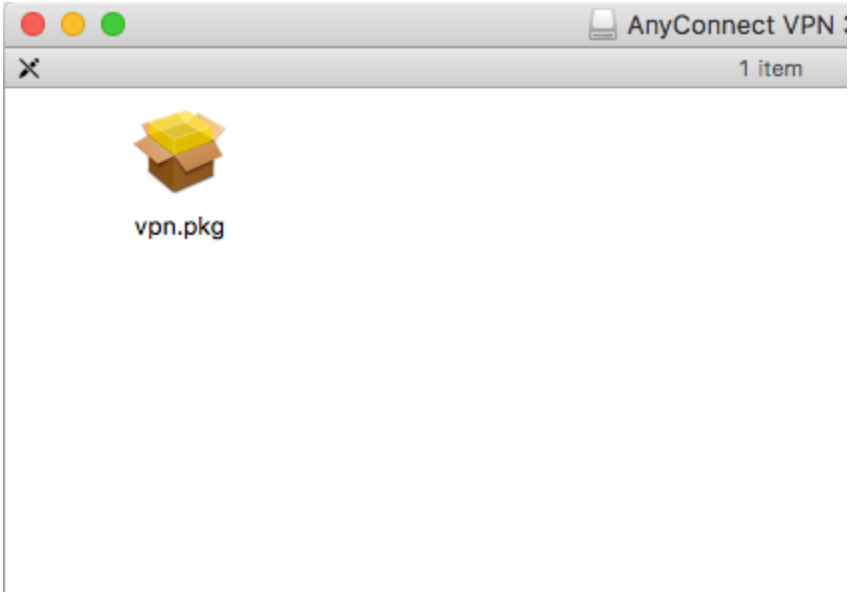
Download the installer from the link above, and double click it to run**.** Follow the dialog boxes to install the software, clicking Next.

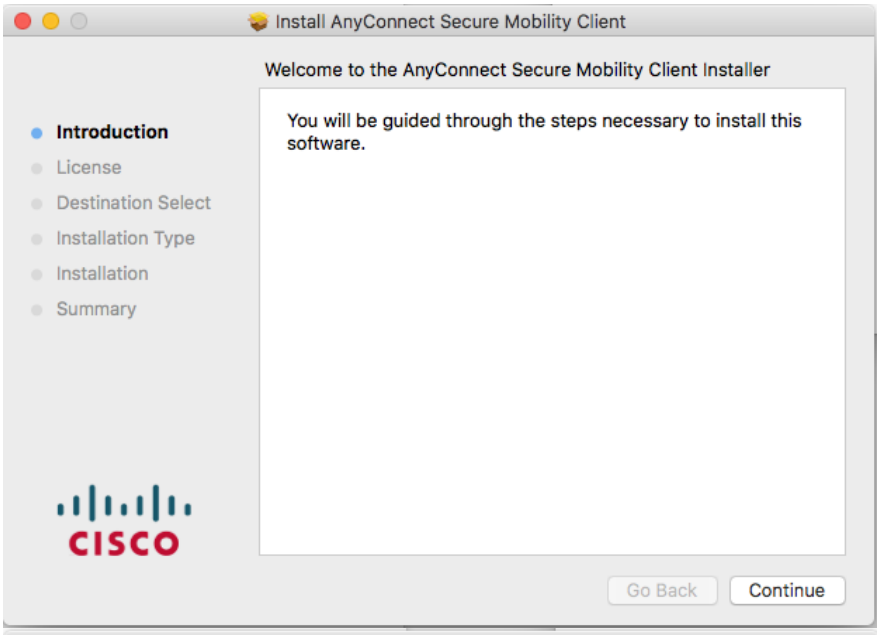

Cisco AnyConnect Secure Mobility Client Setup
Welcome to Cisco AnyConnect Secure Mobility Client Setup Wizard
The Setup Wizard will install Cisco AnyConnect Secure Mobility Client on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
< Back
Next >
Cancel
Cisco AnyConnect Secure Mobility Client Setup
End-User License Agreement
Please read the following license agreement carefully
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
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
Advanced Installer
< Back
Next >
Cancel

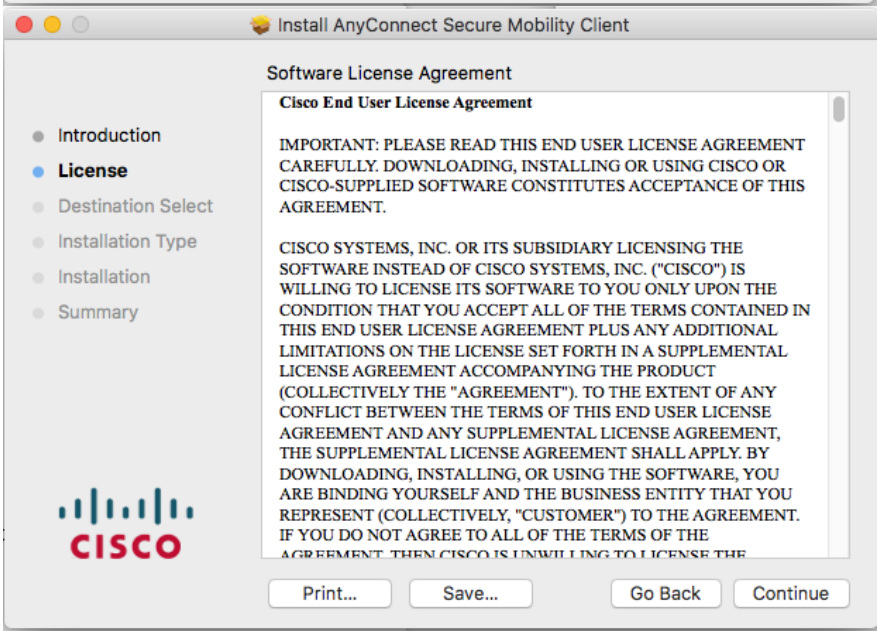


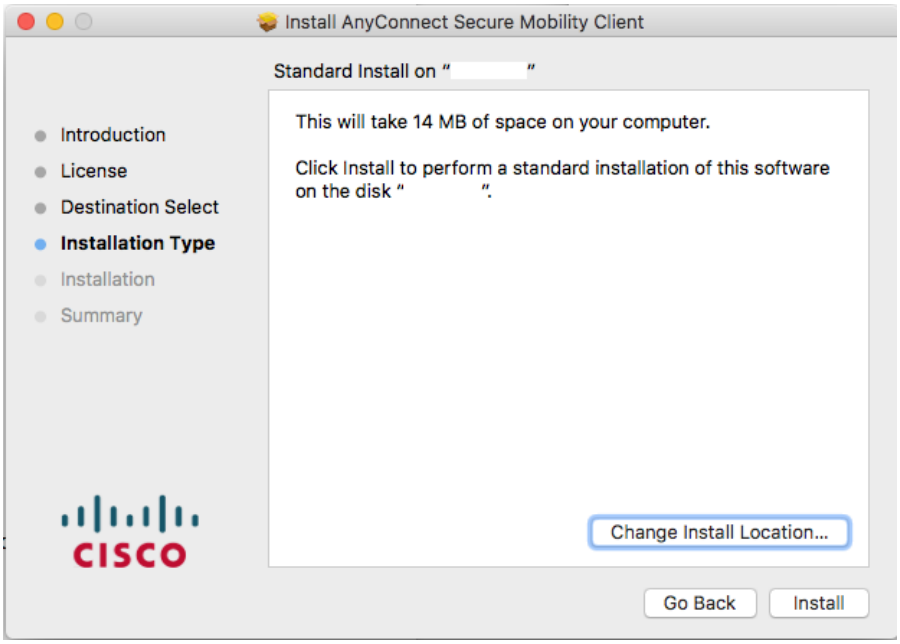
Mac OS X

Download the disk image from the link above and double-click to open it. Double-click the "vpn.pkg" file to run it. Follow the dialog boxes to install the software, clicking Continue, Agree, or Install on each screen to proceed.




Install AnyConnect Secure Mobility Client
Welcome to the AnyConnect Secure Mobility Client Installer
Introduction
License
Destination Select
Installation Type
Installation
Summary
You will be guided through the steps necessary to install this software.
Go Back
Continue

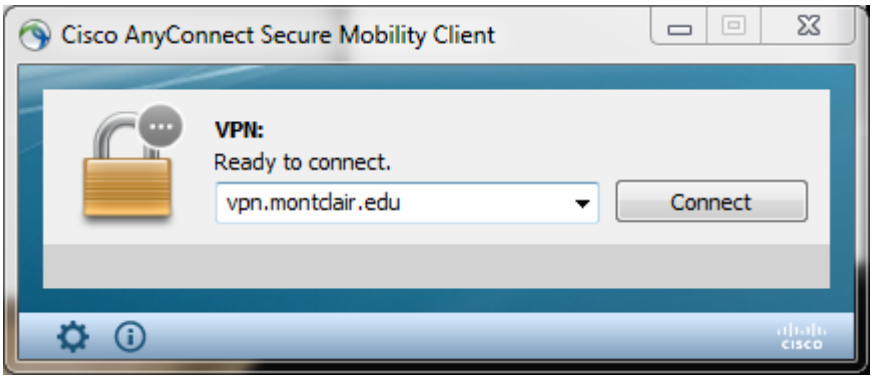

Install AnyConnect Secure Mobility Client
Software License Agreement
Introduction
License
Destination Select
Installation Type
Installation
Summary
Cisco End User License Agreement
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, 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
Print...
Save...
Go Back
Continue



Using the AnyConnect Client

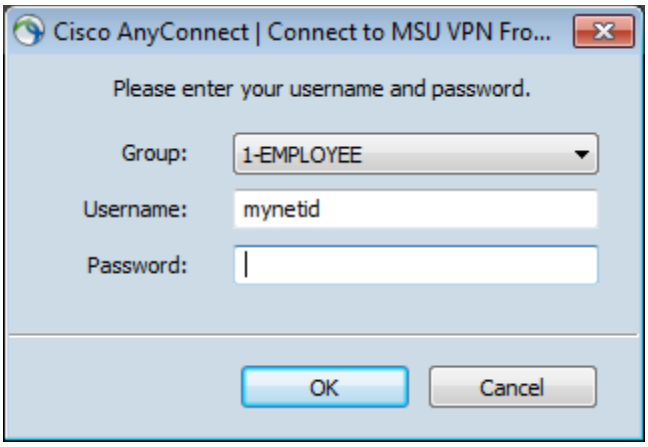
(Note: These screenshots are from the Windows version but the macOS version is very similar.)

Enter **vpn.montclair.edu** in the dialog box and click Connect



When prompted, select the Employee profile “1-EMPLOYEE”.

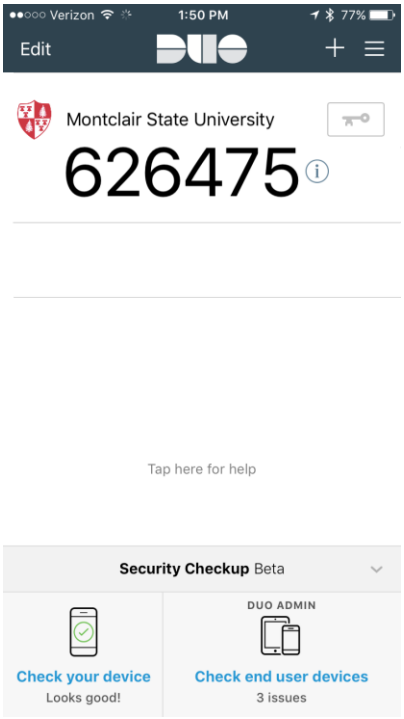
In the fields labeled *Username* and *Password*, enter your MSU NetID and password.



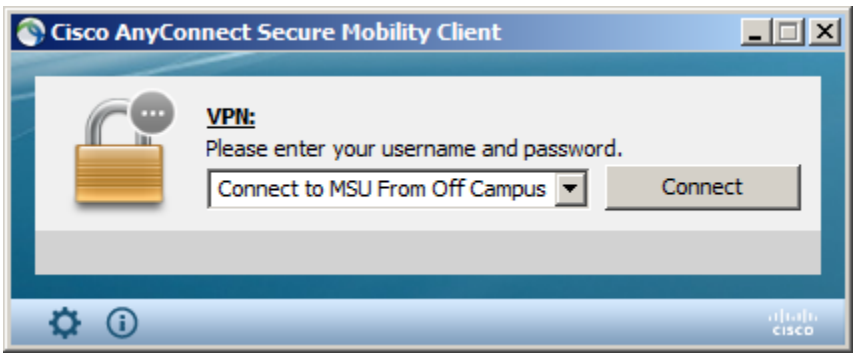
In the field labeled *Second Password* you can type one of the following words:

push Duo will send a push notification to your phone with Duo Mobile installed
sms Duo will send an SMS to your registered cell phone
phone Duo will call your registered cell phone

Alternatively, you can enter the token generated by Duo Mobile in the field labeled *Second Password*. To reveal this token, open Duo Mobile and tap **Montclair State University**.



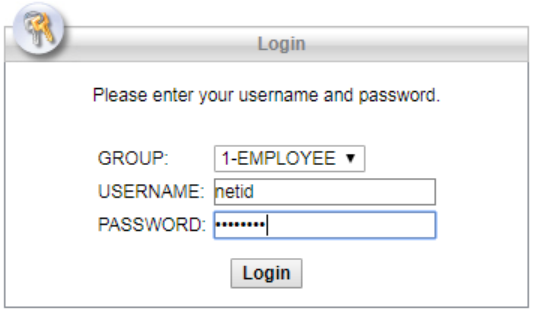
After you connect for the first time, the Cisco AnyConnect client will present an option dropdown box for “Connect to MSU from Off Campus”. For subsequent connections to the VPN, simply select this option from the drop-down box and click Connect.



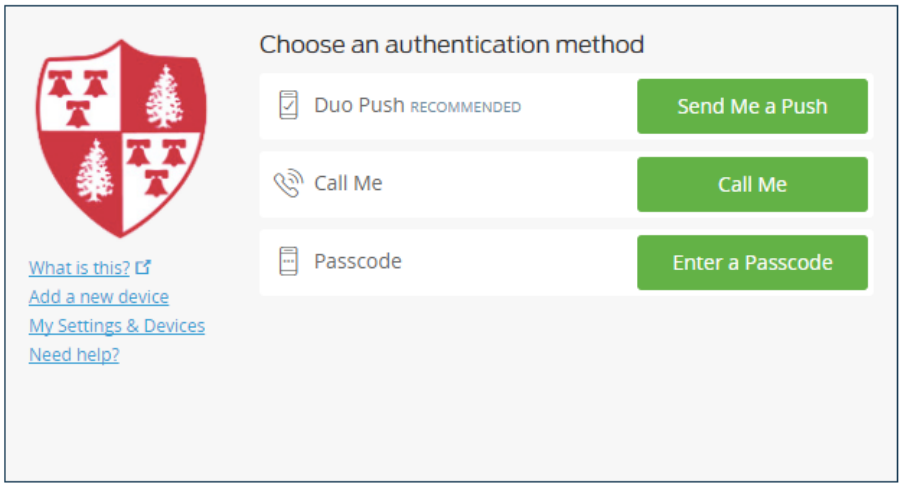
Connecting to the VPN via web interface

Browse to: https://vpn.montclair.edu

Select "**1-EMPLOYEE**" from the GROUP drop-down box, and enter your MSU NetID and Password.



Once you log in, you will be presented with the Duo second authentication page.

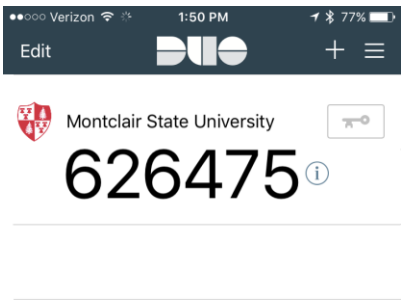


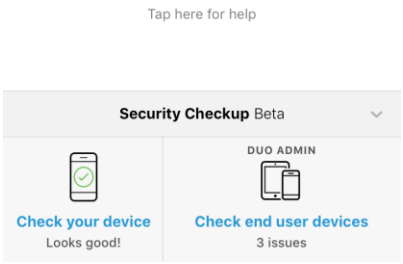
Choose a second authentication method from the following

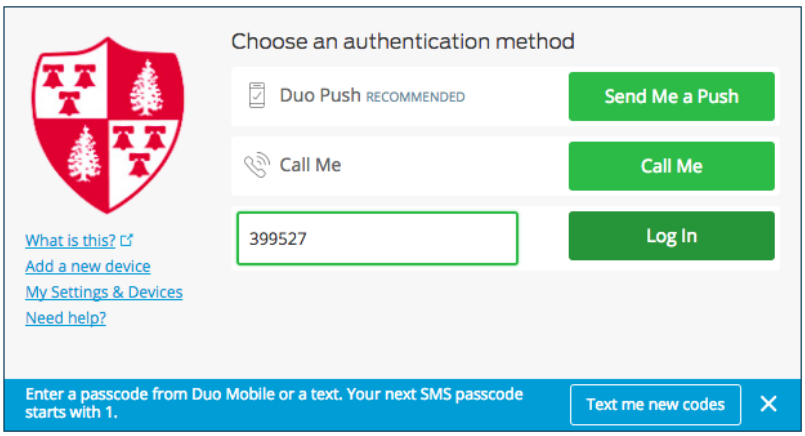
Duo Push
Will send a push request to the Duo Mobile application on your enrolled device.

Call Me
Will call the phone number that you have registered during Duo Mobile enrollment

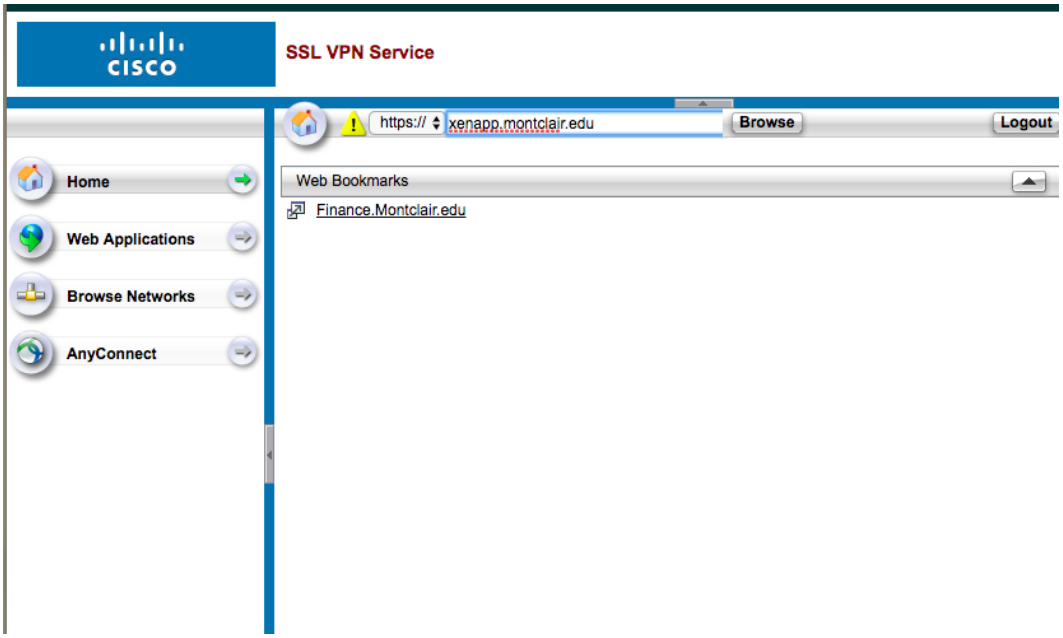
Passcode
In Duo Mobile on your enrolled device, select the Key icon next to Montclair State University to reveal a six digit passcode. Enter this code into the dialog box on the web site.







Once logged into the SSL VPN Web Interface, you can browse to .montclair.edu web pages that would typically be available from on campus. Enter the URL in the dialog box at the top, select http:// or https:// from the drop-down box, then hit **Browse**.



You will be redirected through the SSL VPN interface to the website that you've requested. The URL in your browser will still display **vpn.montclair.edu** instead of the resource you've requested