

# MSU Authorized IT User Data Center Access Procedure, Campus VPN

This document provides the requirements and procedures for access to the Data Center Network for MSU Authorized IT Users. MSU Authorized IT Users are IT employees authorized to access data center resources. Access to the Data Center Network is provided by a connection to the Campus VPN with the Cisco AnyConnect client.

## Requirements

Access to the Data Center Network requires:

- An MSU Privileged Account
- A MSU Managed Secure Desktop
- Enrollment in Duo for Two-Factor Authentication (2FA)
- The Cisco AnyConnect client

## MSU Privileged Account

Your MSU Privileged Account is a secondary account that is only to be used for access to privileged resources, such as access to the Data Center Network. This account is usually named *netid\_adm* or *netid\_prv*, depending upon when you were provisioned the account. If you do not know the password to your MSU Privileged Account, contact ISIM to ask for a password reset. For more information regarding Privileged Accounts, reference the [IT Privileged Account Policy](#).

## Obtain a MSU Managed Secure Desktop

New users in MSU IT are provided a Secure Desktop by default. If you are unsure whether or not your MSU provided workstation is running the Secure Desktop image, provide ISIM with your machine name to verify. If you do not have an MSU Managed Secure Desktop, have your manager contact Technology Solutions so that they can provision you a new machine with the Secure Desktop image.

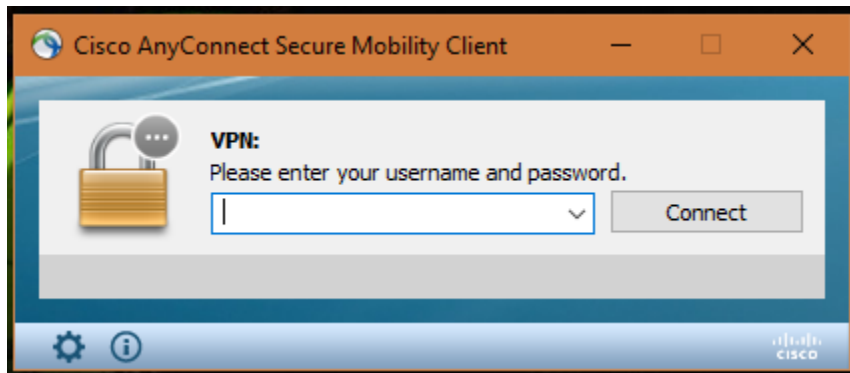
## Enroll in Duo for Two-Factor Authentication (2FA)

Logins to the Campus VPN require Two-Factor Authentication, which is provided to the University through Duo. Reference the document [Duo Enrollment for Two-Factor Authentication \(2FA\)](#). Upon receiving a provisioning request, ISIM will provision your MSU Privileged Account into Duo, and you will receive an enrollment email. Follow the steps in the document to enroll your mobile devices for use with Duo.

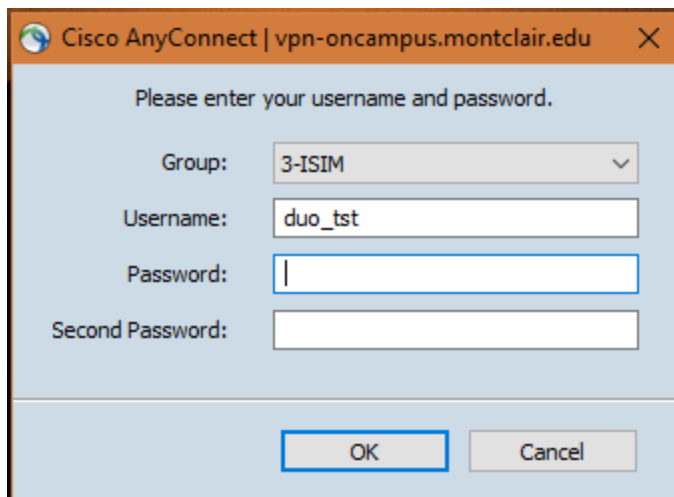
## Connecting to a Duo-protected VPN account with Cisco AnyConnect

The Cisco AnyConnect client comes pre-installed on University-provided workstations that are running the latest secure image.

1. If you are currently on campus, enter **vpn-oncampus.montclair.edu** in the text box
2. If you are currently off campus, enter **vpn-offcampus.montclair.edu** in the text box



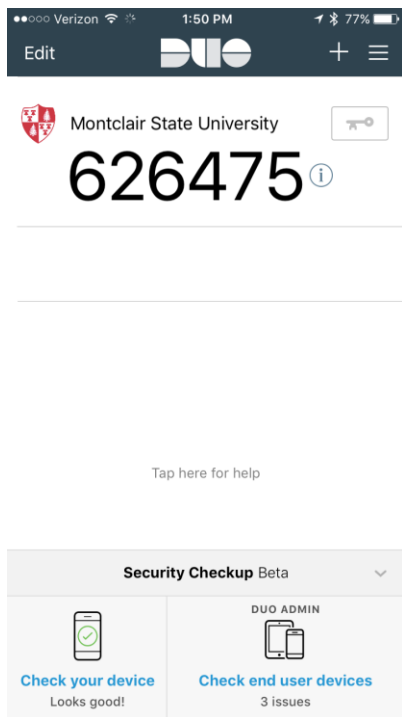
When prompted, select the profile of the group you belong to. For example, if you are a member of EAS, select "4 - EAS". In the fields labeled *Username* and *Password*, enter your MSU Privileged Account and password.



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 options in the dropdown box for “Connect to MSU from On Campus” and “Connect to MSU From Off Campus”. Use the appropriate option on subsequent connections.

