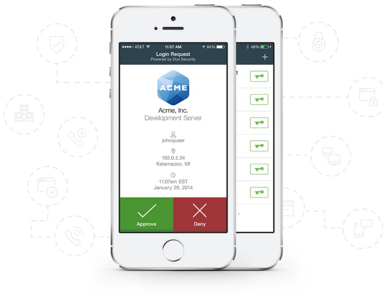
VPN & MFA

Overview



The **Central Authentication System (CAS)**, **Virtual Private Network (VPN)** and **Multi-Factor Authentication (MFA)** systems are important tools that allow you to access University resources in a secure manner. Depending on the resource you are trying to access, you may be required to utilize one or more of these systems.

It's also helpful to note that MFA is a way of authenticating that can be used by the both the CAS and VPN systems (but usually just one at a time).

For example:

- Web applications (e.g. Gmail, Tableau Server, SAS Visual Analytics) generally enforce MFA through CAS. When you go to these sites, if you're not already logged-in to CAS, you can expect to see a CAS prompt, followed by an MFA prompt.
- Desktop applications (e.g. Tableau Desktop, SAS Enterprise Guide) generally enforce MFA through a specific VPN group that requires MFA (i.e. UMaccess-MFA). To use these desktop applications, you generally will connect to the VPN first, complete the MFA prompt, then enter your Directory ID and password directly into the application.
- When you are off-campus, you may be required to connect to the VPN, even when accessing web applications. For Tableau Server and SAS Visual Analytics, you can connect to any VPN group, even if it does not include MFA, because MFA is guaranteed to be enforced through the CAS log-in to those web applications. However, if you happened to select the UMaccess-MFA group, you would need to complete the MFA prompt twice: once for the VPN connection, and once for the CAS log-in.

Table of Contents

Using MFA to log-in to the VPN

The Multi-Factor Authentication (MFA) system is a layer of security that is used in conjunction with other security systems. Even if you log-in to a system that requires you to use MFA with the Central Authentication System (CAS), such as Gmail for example, you may still need to use MFA again with the VPN system, depending on which VPN Group you select. Most staff and faculty were required to use MFA with the CAS system on or before March 5, 2018.

Summary

- **Step 1:** Open the VPN program.
- **Step 2:** Select a VPN group and enter your credentials. Some systems require a specific VPN group, others do not.
- **Step 3:** Approve the "push" via your phone, or manually enter your MFA code in the "Second Password" field.

Step-by-step Instructions

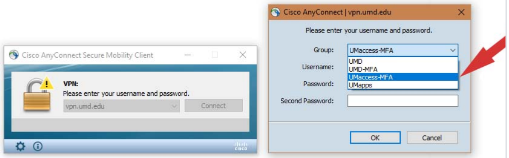
If you have **NEVER** used MFA, please see the instructions to enroll here: Obtaining MFA for the first time. Otherwise, please proceed to the instructions to connect below.

Step 1: Load the computer program called **Cisco Anywhere Connect**, and connect to the address **vpn.umd.edu**

? Unknown Attachment

Tip: Cisco Anywhere Connect is installed on most university machines, but you can also download it from Terpware (links)

Step 2: Select a "Group" choice from the drop down box and enter your information. Some systems require a specific VPN group, others do not.



Cisco AnyConnect Secure Mobility Client

VPN:
Please enter your username and password.
vpn.umd.edu
Connect

Cisco AnyConnect | vpn.umd.edu

Please enter your username and password.

Group: UMaccess-MFA
UMD
UMD-MFA
UMaccess-MFA
UMapps
Username:
Password:
Second Password:

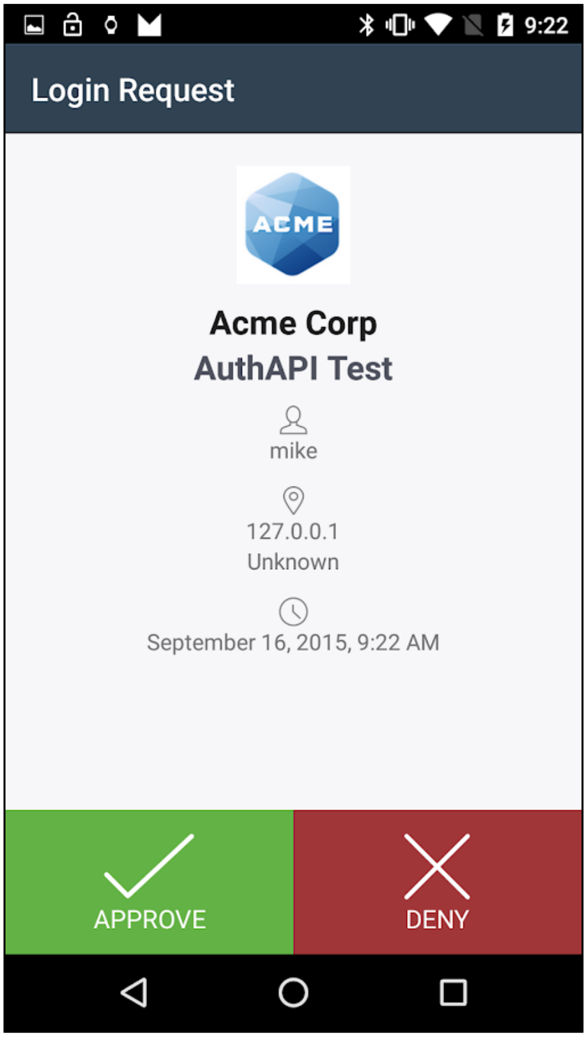
OK
Cancel

(Click to enlarge)

? Unknown Attachment

- Your **Username** is your Directory ID (i.e. your ema
- Your **Password** is your normal UMD Password (i. gmail or timesheets)
- If prompted for a **Second Password**, type "push"

Step 3: You will receive a "push" notification on your phone asking you to confirm your log-in.



Login Request

Acme Corp

AuthAPI Test

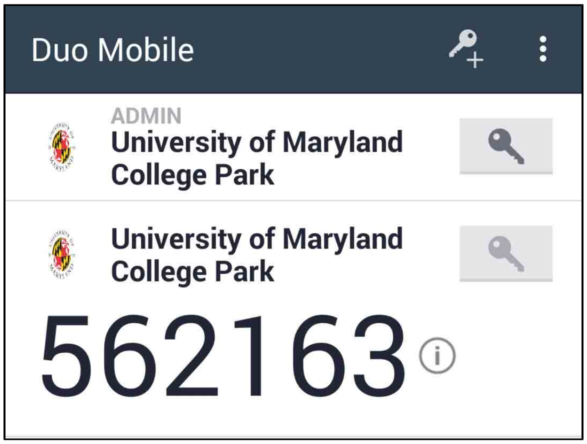
mike

127.0.0.1
Unknown

September 16, 2015, 9:22 AM

If you do not receive a push on your phone

Step 4: Open your **Duo Mobile** app and click the key icon next to the account you are using to generate a passcode



Duo Mobile

ADMIN
University of Maryland College Park

University of Maryland College Park

562163

Step 5: You should already have **Cisco Anywhere Connect** open from Step 1 above, select any "Group" connection from the drop down box

Instead of entering the word "push" in the **Second Password** field, you will enter the code generated by your phone app

? Unknown Attachment

-
    - Your **Username** is your Directory ID (i.e. your email without the "@umd.edu" part)
    - Your **Password** is your normal UMD Password (i.e. the one you would use to sign into gmail or timesheets)
    - Your **Second Password** is the MFA code generated by your DuoMobile phone app or your token

You should now be logged in to the VPN/MFA system. You can now proceed to log-in normally to MFA-protected systems such as report.umd.edu/campus.

FAQ for VPN & MFA

What is MFA?

Multi-Factor Authentication (MFA) is a method to confirm that "you are who you say you are" when accessing a system, using something ***other*** than your password to authenticate you. Your password is generally the first factor, and this "other thing" becomes the second factor. Using both makes it "multi-factor". In addition to passwords, "factors" can include:

- "something you know" (for example, your mother's maiden name),
- "something you have" (like your phone or a "token"),
- or "something you are" (i.e. biometrics, which the University does not currently use).

MFA is used for the Central Authentication System (CAS) as well as certain Groups on the VPN system.   As a result, you may encounter the MFA prompt multiple times (for example, if you log-in to both Gmail and the VPN).

What is VPN?

Virtual Private Networking (VPN) is a tool that encrypts data as they travel from a system to your computer, and back. Data are only sent to you after you have confirmed that "you are who you say you are." This is why MFA is required first, in order to access the VPN system. As noted above, MFA is not only required for the VPN system. Even if you have logged-in to the VPN, you may encounter the MFA prompt again when logging-in to Gmail and other campus systems. Links to download the VPN client are located below.

How do I get the Cisco AnyConnect VPN tool?

- TerpWare for Windows
- TerpWare for Mac
- TerpWare for Linux

VPN Tips

- Once connected to the VPN, your connection should hold for at least 24 hours unless you turn off your computer or put it to sleep.
- To make access to Tableau and other systems more convenient, consider logging-in to the VPN as part of your morning routine when you log-in to your computer.

More Resources

ⓘ These links repeat some information that is summarized in the previous sections.

- How to Add **Additional** Devices for use with DUO Multi Factor Authentication
- How to Enable Multi-Factor Authentication (MFA) for **all** CAS Authenticated Webpages
- **Bypass (i.e. backup) codes**
  - Multi-Factor Authentication Bypass Codes
  - How To Print Multi-Factor Authentication Bypass Codes
- **Hardware tokens**
  - How To Register a Multi-Factor Authentication Hardware Token
  - Multi-Factor Authentication Hardware Token Frequently Asked Questions (FAQ)
- Overview of Multi-Factor Authentication and Login Methods
- How to Enroll Your Mobile Device in Multi-Factor Authentication at University of Maryland
- University of Maryland Multi-Factor Authentication Frequently Asked Questions (FAQ)
- How to Use Multi-Factor Authentication with the Cisco AnyConnect Virtual Private Network (VPN) Client