VCU Two-Factor Authentication

Setup Walkthrough

Step 1: Configure DUO Authentication

- Read detailed instructions (highly recommended)
- In a hurry?
  - If you arrived at a DUO enrollment prompt through a CAS-enabled application, simply click "Start" and follow the prompts.
  - Otherwise, click here to set up DUO for the first time, or to manage your devices.

Step 2: Check the Instructions for a
DUO-Enabled Service

VCU Services for which DUO is Mandatory:
- VPN Access
- Central Authentication Service ("CAS")
  - Phased roll-out of DUO to CAS is currently in progress. Contact infosec@vcu.edu for details.

VCU Services for which DUO is Available (at a
system owner’s discretion):
- Windows Remote Desktop
- Secure Shell (SSH) on UNIX / Linux / Mac OS X

Step 3: Log In to the Chosen Service in
accordance with the Instructions

Quick Start Setup Instructions and
Videos

Step 1:

Go to https://duo.vcu.edu to register your device in preparation for two-factor authentication and come back to this page when you are done. Please see walk through video below.

<p></p>

Step 2:

The following video shows the activation process for Duo Mobile / DUO Push (Optional but highly recommended)

<p></p>

Step 3:

Select one of the following use cases to start using your new Two Factor authentication

- 2 Factor VPN access
  Required for faculty / staff remote access into VCU networks from remote locations.

- 2 Factor Windows Remote Desktop (RDP) Access
  Can help to enhance your windows remote access security.

- 2 Factor Secure Shell (SSH) on Unix / Linux / MacOSX access
  Can help to enhance your SSH remote access security.

Two-Factor Authentication at VCU

DUO is a two-factor software product by Duo Security. It is made available as a series of modules, or plug-ins, that can be integrated into various other software products.

When you’re using a VCU application or system that has been configured to require two-factor authentication, you will open the application or connect to the system just as you normally would. You’ll verify your first factor (often a password) just as you have in the past. You will then be presented with a DUO interface to verify your second factor (or to enroll in DUO if you have not already done so).

In order to utilize two-factor authentication, you have to configure DUO so that it knows how to authenticate you, just like you’d have to establish a password for the first time on a new account.

Please see the links to the right to get started with the different options for DUO.
"What is Two-Factor Authentication?"

In a traditional authentication model, you are asked to verify your alleged identity (often a username) by providing something that only you should know (often a password). In this model, the password would be your first and only authentication factor.

Unfortunately, this model has some serious weaknesses when it comes to technology in the twenty-first century. For the first few decades of computing history, a single factor was considered adequate to prove a person's identity- computers were often so slow that guessing somebody's password randomly (called brute forcing in industry parlance) was too time-consuming to be feasible. Now, with the advent of faster computers, to say nothing of the increased impact of programming errors, social engineering attacks, et cetera as computers have become a part of most people's daily lives, this single factor system has become woefully inadequate.

The reasonable solution, then, is to require additional authenticating factors on top of the first, in order to prove your identity. You've likely already been doing this for years without realizing it: at the bank, when you start a new job, when you apply for a passport or a driver's license, and in many other situations besides. In those cases, you're simply asked to provide multiple forms of validation for your identity. Two-factor authentication, in a technology context, is no different. In addition to the thing that only you should know- your first factor such as a password- you will also be asked to provide something that only you should have, like access to your cell phone or key ring. This second thing is your second factor.

So, in short, two-factor authentication is a way of proving your identity where you're required to provide something that only you should have, in addition to something that only you should know.