Using YubiKey as a One-Time-Password Token

Purpose

This document provides directions to program a YubiKey as a one-time-password token for use with Duo Two-Factor Authentication (2FA) at the University of Washington.

Prerequisites

- Eligibility to use Duo two-factor authentication (2FA)
- YubiKey Personalization Tool (https://www.yubico.com/products/services-software/personalization-tools/use/) installed
- Possession of a compatible YubiKey (cannot program the Security Key, which only uses FIDO U2F and directions will be different with a YubiKey VIP key)

First Steps

- Decide which algorithm to use. Duo supports YubiKey AES and OATH-HOTP. A helpful comparison between YubiKey AES and OATH-HOTP is here.
- Note: The mainframe system (Keynes) cannot support longer than 8 character passcodes. If you plan on using your YubiKey to sign in to the mainframe (Keynes) you'll need to use the OATH-HOTP algorithm and configuration directions.
- If you're planning on using the same secrets for other external services that rely on Yubico's validation servers you'll need to use the YubiKey AES Configuration algorithm and configuration directions.

Directions

- YubiKey OATH-HOTP Configuration
- YubiKey AES Configuration