Henry Ford College – Multi-Factor Authentication Enrollment

Table of Contents

Introduction

Once enrolled for 2FA (Two Factor Authentication), you will be required to approve any logins to HFC protected web services when accessing them from non-HFC networks (e.g., not onsite).[1] This will not be required for every external authentication attempt. HFC currently supports the following methods of 2FA:

- SMS Message (also known as a "One Time Password" or OTP)
- Smartphone Push Notification (Requires iOS or Android App)
- Fast Identity Online (FIDO) Hardware Tokens (e.g. Yubikeys)

All users with valid mobile numbers are already pre-enrolled (see *Update or Verify Your Mobile Phone Number* below) for SMS. Each unique device/browser combination will be tracked so that the second factor is only required once every five days. Clearing browser history or using a private or incognito window will result in the second factor requirement on next login. Smartphone enrollment requires installing the NetIQ Advanced Authentication application on your phone and accessing the HFC Advanced Authentication enrollment portal from your desktop browser. Please note, your cell/mobile phone number MUST be accurate in the HFC system, otherwise you will NOT be able to access the enrollment portal or enroll your phone or hardware token. Please verify your profile information in the employee portal prior to attempting enrollment.

[1] Enforcement of 2FA for non-trusted networks has not yet been enabled for all users.