

Henry Ford College - Advanced Authentication Enrollment

Table of Contents

Introduction	1
Update or Verify your Mobile Phone Number	1
Download NetIQ Advanced Authentication App	3
Enrolling Your Device Using Your Desktop Browser.....	5
Enrolling Your Device From Your Device	12
Testing Your Enrolled Device	13
Authentication Example.....	16
Frequently Asked Questions.....	18

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 and not while connected to the VPN).¹ Enrollment requires installing the NetIQ Advanced Authentication application on your phone and accessing the HFC Advanced Authentication enrollment portal from your desktop browser or by accessing an enrollment link directly on your mobile device (choose one enrollment method, NOT BOTH). 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 device. Please verify your profile information in the employee portal prior to attempting enrollment.

Update or Verify your Mobile Phone Number

You will not be able to login to the enrollment portal if you mobile/cellular phone number is in correct in the HFC system. To update and/or verify your mobile number, please complete the following steps.

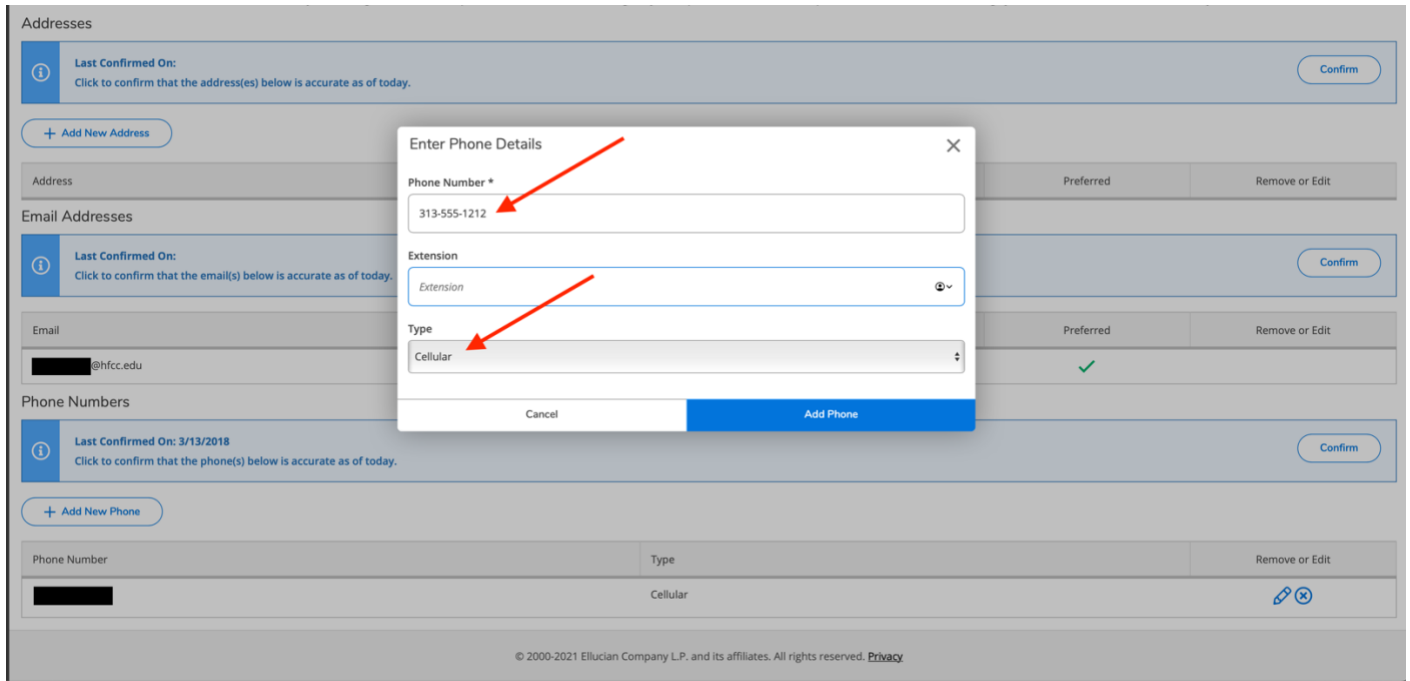
First, login to the Employee Portal (<https://my.hfcc.edu/faculty-and-staff>).

Next, select update profile information.

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

If your cell phone number is listed as type “Cellular”, and is correct, then this step is complete and you may proceed to the next section, *Download NetIQ Advanced Authentication App*.

If your cellular number is not listed, click “Add New Phone” and then add your ten-digit mobile phone number with no spaces or dashes. The system will add the appropriate formatting. If your cellular number is wrong, click the pencil icon on the right to edit and update your mobile number.



Click “Add Phone”

Your cell phone number is now correctly added into the system. Please wait at least 30 minutes before proceeding with enrollment to ensure this update has synchronized to all HFC systems.

Download NetIQ Advanced Authentication App

The application can be downloaded by scanning one of the following QR Codes:

For Android Devices:



For iOS Devices:



If you have a problem scanning the QR code, you can also install the application during enrollment if you follow the *Enroll Your Device From Your Device* instructions later in this document. Enrolling using that process provides a link to the appropriate application for your device. The applications can also be found at the following URLs:

For iOS:

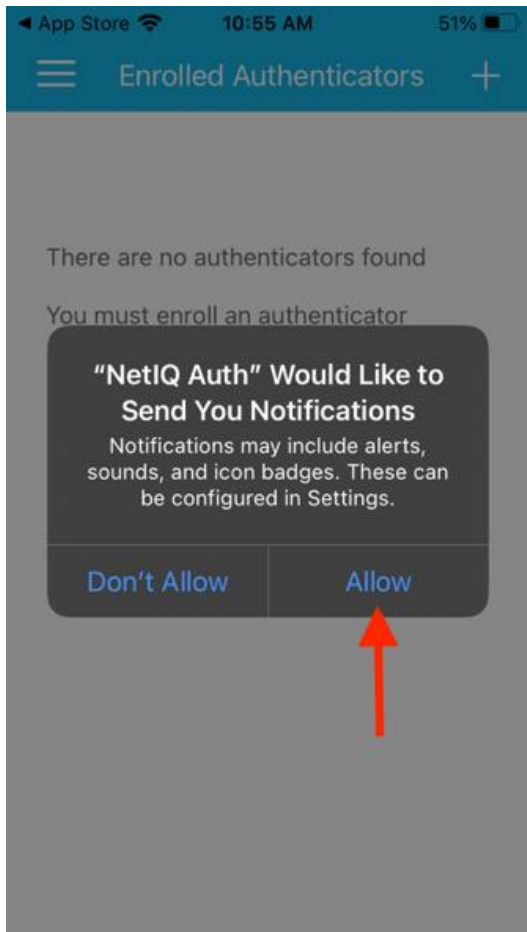
<https://apps.apple.com/us/app/netiq-advanced-authentication/id843545585>

For Android:

https://play.google.com/store/apps/details?id=com.netiq.oathtoken&hl=en_US&gl=US

The first time the application is launched, you will be required to set a PIN. This is required to unlock the application if other methods (e.g. fingerprint, face) are not available.

On iOS, be sure to Allow notifications from this application:



Enrolling Your Device Using Your Desktop Browser

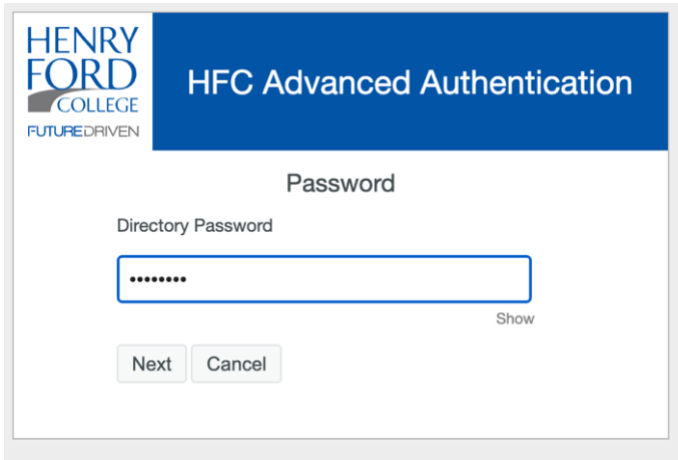
Access the Henry Ford College Advanced Authentication Enrollment Portal from your desktop web browser:

<https://advauth.hfcc.edu/>

Enter your Username:

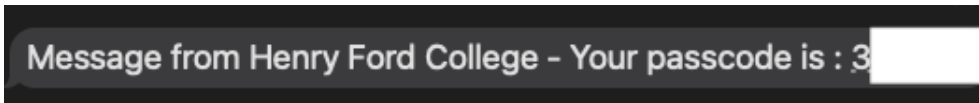
A screenshot of the 'HENRY FORD COLLEGE FUTUREDRIVEN' logo on the left and a blue header with 'HFC Advanced Authentication' on the right. Below the header is a text input field containing 'jdoe99' and a 'Next' button.

Enter your HFC password:

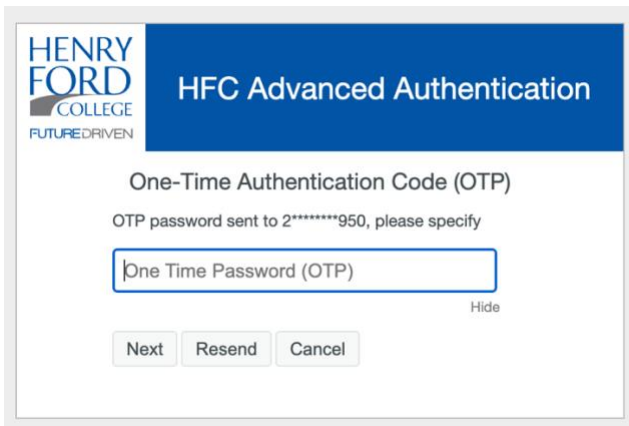


The screenshot shows the 'HFC Advanced Authentication' interface. At the top left is the Henry Ford College logo with the tagline 'FUTUREDRIVEN'. The main title is 'HFC Advanced Authentication'. Below this, the word 'Password' is centered. Underneath, it says 'Directory Password'. There is a text input field containing seven asterisks. To the right of the input field is a 'Show' link. At the bottom, there are two buttons: 'Next' and 'Cancel'.

Next, HFC AdvAuth will send an SMS One-Time-Password (OTP) to your phone:



Enter that value in the next box:



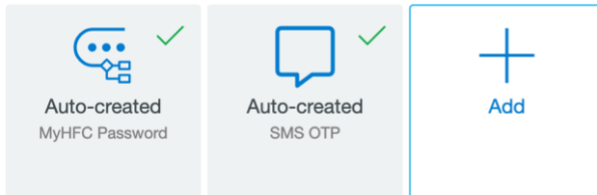
The screenshot shows the 'HFC Advanced Authentication' interface for entering a One-Time Authentication Code (OTP). At the top left is the Henry Ford College logo with the tagline 'FUTUREDRIVEN'. The main title is 'HFC Advanced Authentication'. Below this, it says 'One-Time Authentication Code (OTP)'. Underneath, it says 'OTP password sent to 2*****950, please specify'. There is a text input field containing the text 'One Time Password (OTP)'. To the right of the input field is a 'Hide' link. At the bottom, there are three buttons: 'Next', 'Resend', and 'Cancel'.

At this point, you will be at the main Enrollment Portal screen. Here click the box that says "Add" with a plus (+) sign to enroll your phone:

Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

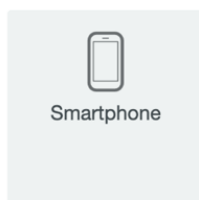
Your Enrolled Single Methods for sign in



On the next screen, select Smartphone (should be the only choice at this time):

Available Methods for Enrollment

Select an authentication method for enrollment. Once enrolled, the method can be used for sign in. OTP methods are one-time password authenticators.



You may give the method a custom name or simply accept “My Smartphone”. Next, click “Get QR Code”:



Smartphone

The Smartphone method allows authentication with your smartphone. It is an out-of-band authentication. The NetIQ Advanced Authentication application sends a push message to your smartphone, which you can accept or reject. Installing the NetIQ Advanced Authentication mobile app on your smartphone is required.

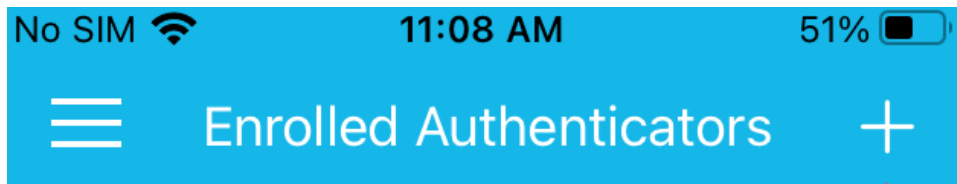
Display Name

To enroll, get a QR code and scan it using the Advanced Authentication mobile app:



- As a backup method, the AdvAuth mobile app provides an OTP code if internet connection is not available on your smartphone.

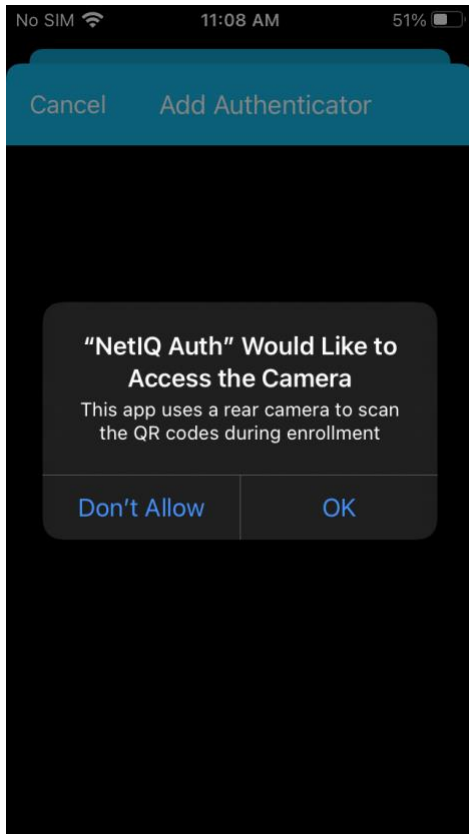
A QR Code will be displayed. Scan the QR code using the NetIQ Authentication App on your Smartphone. Open the NetIQ Authentication App on your phone and click the “+” on the top right:



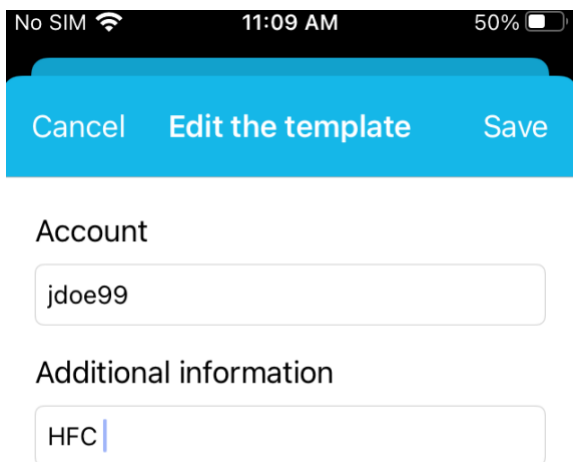
There are no authenticators found

You must enroll an authenticator

If your phone asks, allow NetIQ Auth to access your camera:

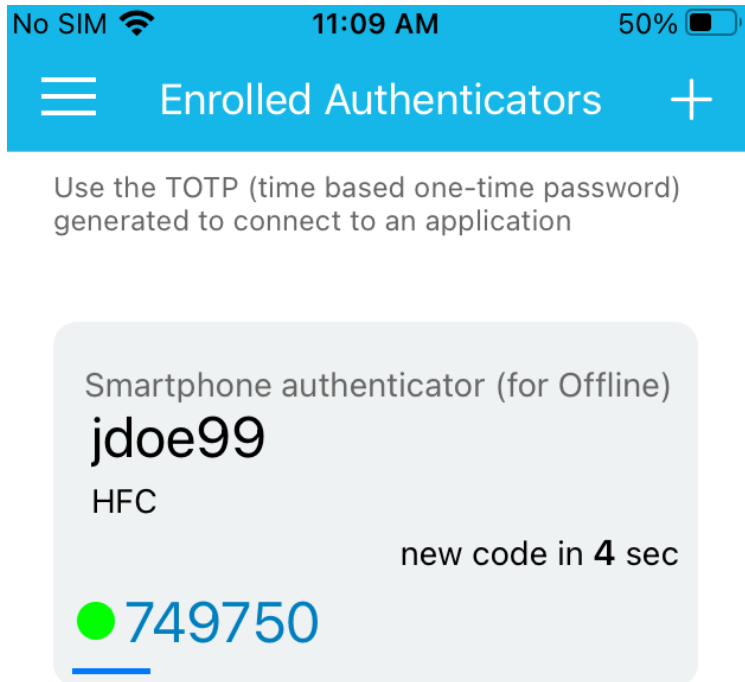


At this point, aim your phone camera at the QR code on your computer screen. The application should identify the QR code and then allow you to enter additional data about the authenticator:



You can enter information here to identify the authenticator, such as your User ID. This information is purely for your viewing only and has no impact on functionality of the authenticator.

At this point, you have enrolled your phone with the HFC Advanced Authentication system. You should see a screen like this on your phone:



Your phone is also enrolled for Time-Based One-Time Passwords (TOTP). This can be used to allow you to login in situations where your phone has no Internet access.

On the enrollment portal, you should see a screen similar to the following that shows "Enrollment is complete." Be sure to click "Save" to save the authenticator!

Smartphone

The Smartphone method allows authentication with your smartphone. It is an out-of-band authentication. The NetIQ Advanced Authentication application sends a push message to your smartphone, which you can accept or reject. Installing the NetIQ Advanced Authentication mobile app on your smartphone is required.

Display Name

My Smartphone

 Enrollment is complete

To enroll, get a QR code and scan it using the Advanced Authentication mobile app:

Get QR Code



- As a backup method, the AdvAuth mobile app provides an OTP code if internet connection is not available on your smartphone.

Save

Cancel







After clicking save, you should see that the Smartphone method is now enrolled:

Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in

 ✓ Auto-created MyHFC Password	 ✓ My Smartphone Smartphone	 ✓ Auto-created SMS OTP	 Add
---	--	--	--

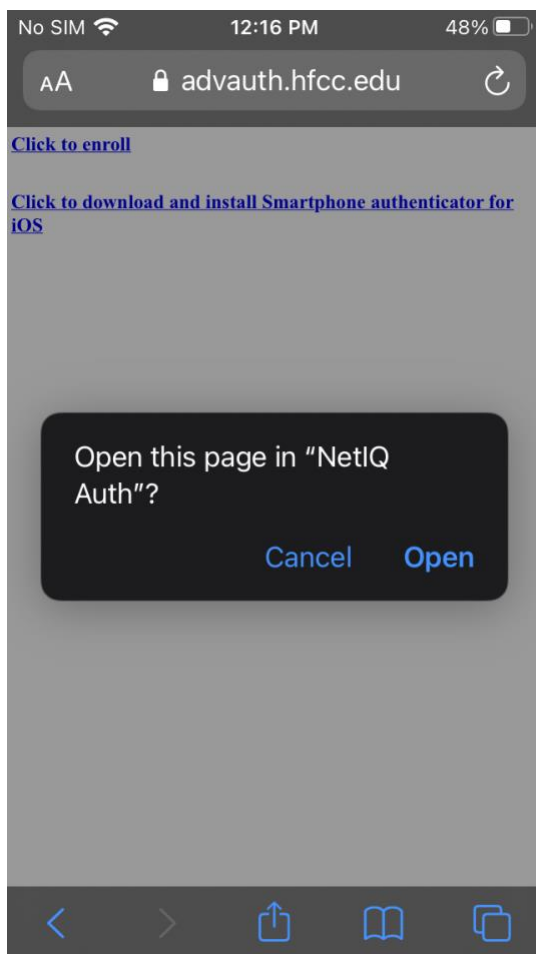
This completes the enrollment process.

Enrolling Your Device From Your Device

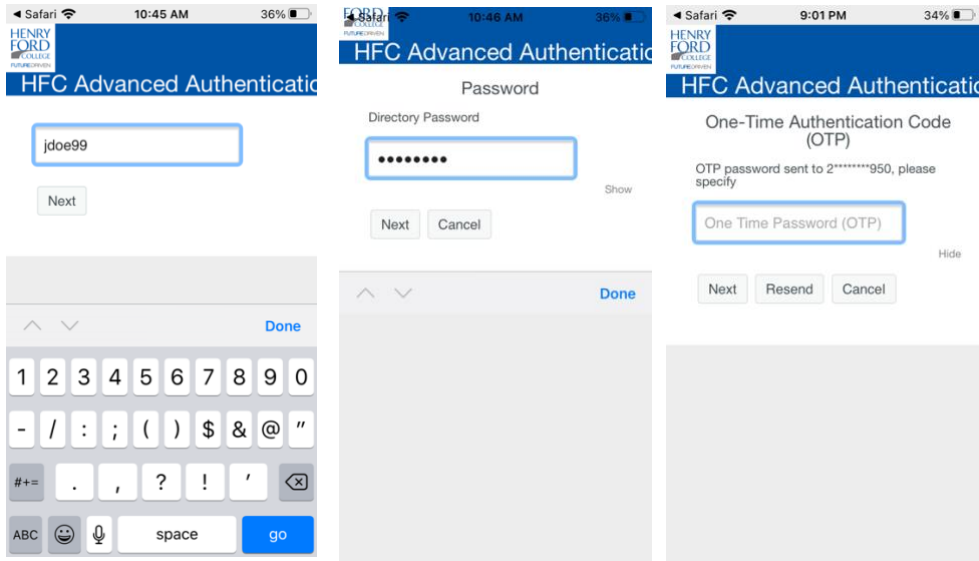
You can enroll your device directly from your device without using the Enrollment Portal from your desktop. To do this, first install the NetIQ Authentication App as described in the first section (if you do not have it previously installed, you will be presented with a link to install the App, see image below) and then open the following URL in a browser directly on your phone:

<https://advauth.hfcc.edu/smartphone/enroll>

This will ask to open the NetIQ Authenticator App.



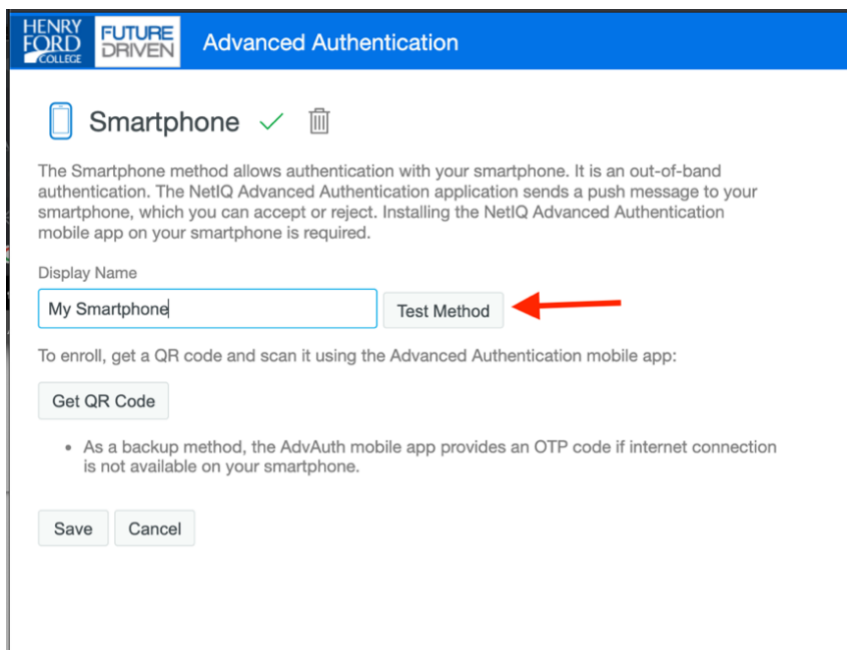
Click Open. Once opened, you will be prompted to login on your phone. Enter your user ID, followed by your password and then the one-time use code sent to your phone via SMS:



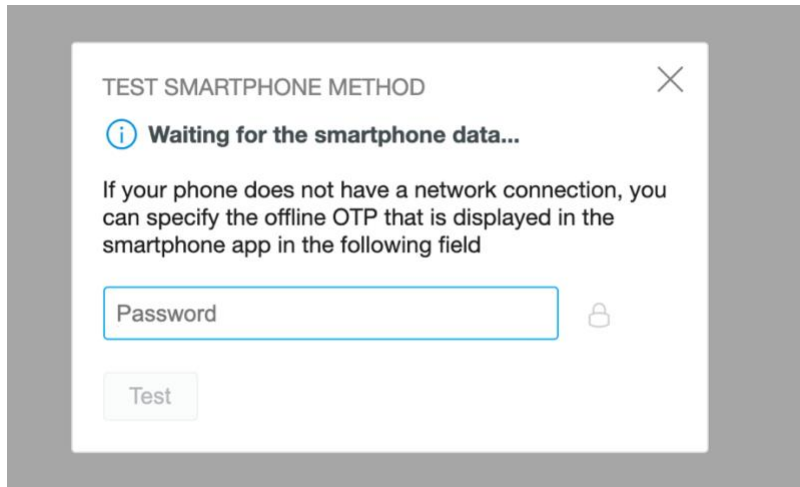
After this, your phone will be enrolled without the need to scan a QR code. You can still login to the Enrollment Portal from your desktop to test the authentication if you like (see below).

Testing Your Enrolled Device

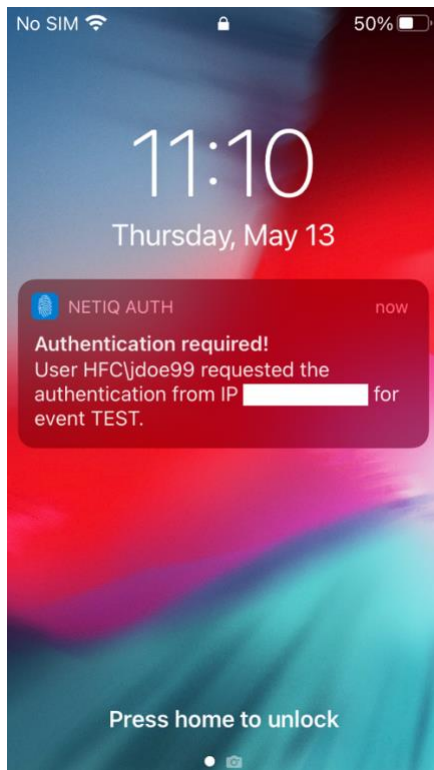
You can test your enrolled device form the Enrollment Portal. Once logged into the Enrollment Portal, Click “My Smartphone” (or whatever you labeled the enrollment as). Then click the “Test Method” button:



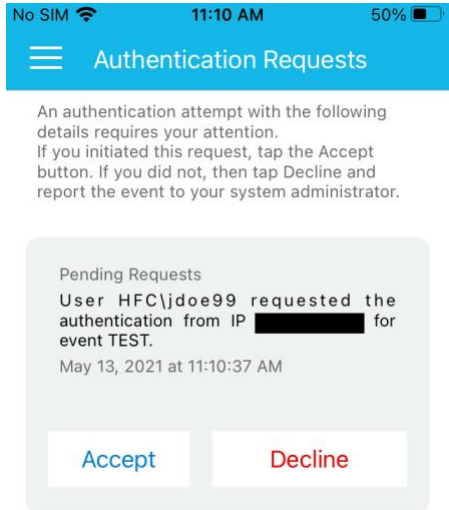
A screen like the following will come up:



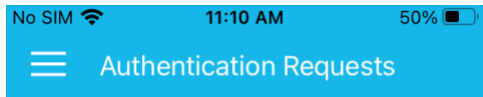
If your phone is locked or not in the NetIQ Auth App, you should see a notification like this:



On iOS, NetIQ Auth App MUST be allowed to send notifications, or this will NOT be seen. Tap the notification and unlock your device. You should be presented with a screen like the following:

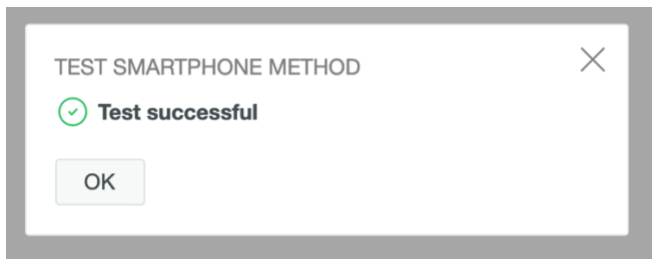


Tap "Accept". This should result in the following:



Accepted

And on your desktop, you should see:



This completes the test. You may now login to HFC services using Two-Factor Authentication.

Authentication Example

With 2FA enabled, when accessing HFC protected resources from untrusted networks, the following is the login sequence to expect.

First, you will see the normal login screen, enter your user ID and password like normal:

HENRY FORD COLLEGE
FUTUREDRIVEN

HFC Websites Login

Please log in to continue.

Username:
jdoe99

Password:
.....

LOG IN

I can't log in

Problem with your username and/or password? Please visit [HFC Universal Username and Password Help.](#)

Henry Ford College | 5101 Evergreen Road | Dearborn, MI 48128 | 800-585-4322
[terms](#) | [privacy](#)

Next, you will see the following:

HENRY FORD COLLEGE
FUTUREDRIVEN

HFC Advanced Authentication

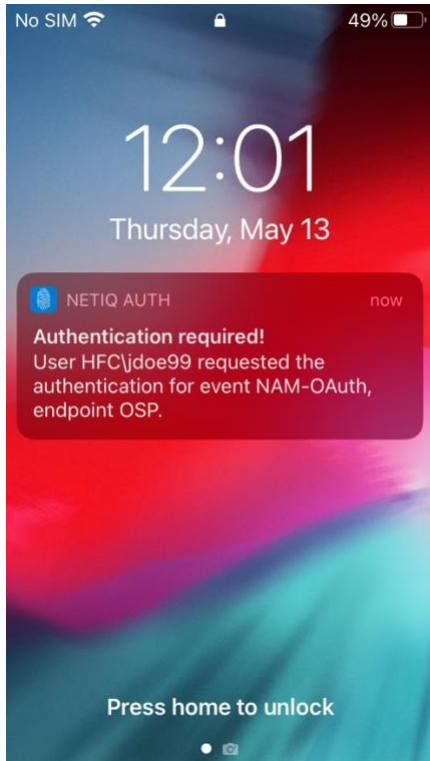
Advanced Authentication Application

Waiting for you to accept the authentication request in the Advanced Authentication app...

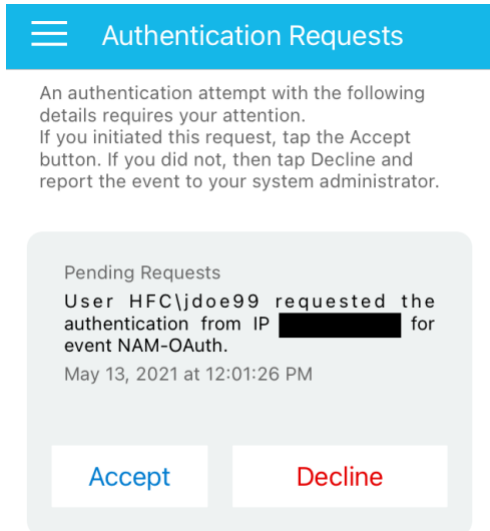
You may instead use an OTP code from your Advanced Authentication App

Cancel

The browser is now waiting for you to approve this authentication on your phone. On your phone, you should see a notification like the following:



Click the notification and unlock your device. NetIQ Auth will prompt you to Accept or Decline the request:



Tap “Accept” and you should be allowed access to the protected resource.

Frequently Asked Questions

Q. Can I enroll multiple devices?

A. Currently, you can only enroll one device (this may change in the future).

Q. I got a new phone, now what do I do?

A. Login to the enrollment portal (<https://advauth.hfcc.edu>) and remove/delete your old/existing Smartphone enrollment. Once done, you will be able to re-enroll with your new phone/device.

Q. I forgot my password and cannot login to the enrollment portal, what do I do?

A. Following the forgotten password instructions at <https://www.hfcc.edu/password> .

Q. I'm not getting push notifications for some reason, can I still login from untrusted networks?

A. Yes, you can use the Time-based One Time Password (TOTP) backup as your second factor.