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.

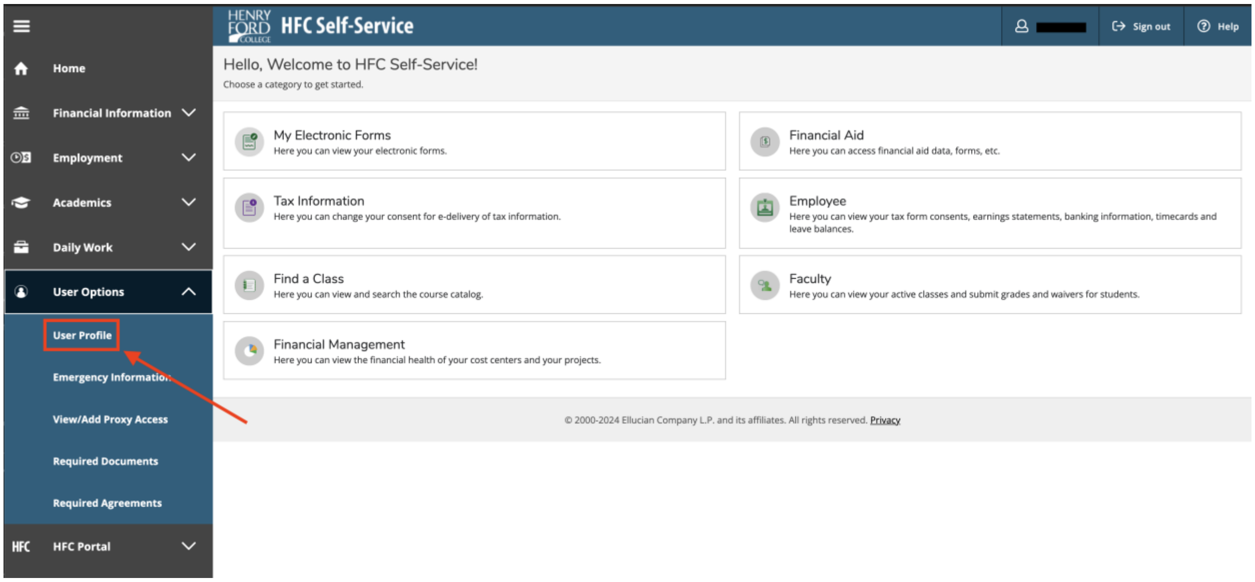
[1] Enforcement of 2FA for non-trusted networks has not yet been enabled for all users.

Update or Verify Your Mobile Phone Number

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

First, login HFC Self Service (https://sss.hfcc.edu).

Next, select "User Options" on the left and then "User Profile".



Hello, Welcome to HFC Self-Service!

Choose a category to get started.

My Electronic Forms
Here you can view your electronic forms.

Financial Aid
Here you can access financial aid data, forms, etc.

Tax Information
Here you can change your consent for e-delivery of tax information.

Employee
Here you can view your tax form consents, earnings statements, banking information, timecards and leave balances.

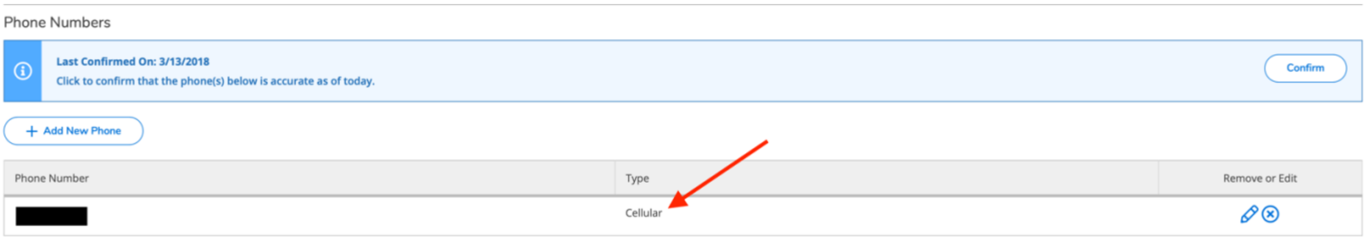
Find a Class
Here you can view and search the course catalog.

Faculty
Here you can view your active classes and submit grades and waivers for students.

Financial Management
Here you can view the financial health of your cost centers and your projects.

© 2000-2024 Ellucian Company L.P. and its affiliates. All rights reserved. Privacy

Scroll down to "Phone Numbers." 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*.

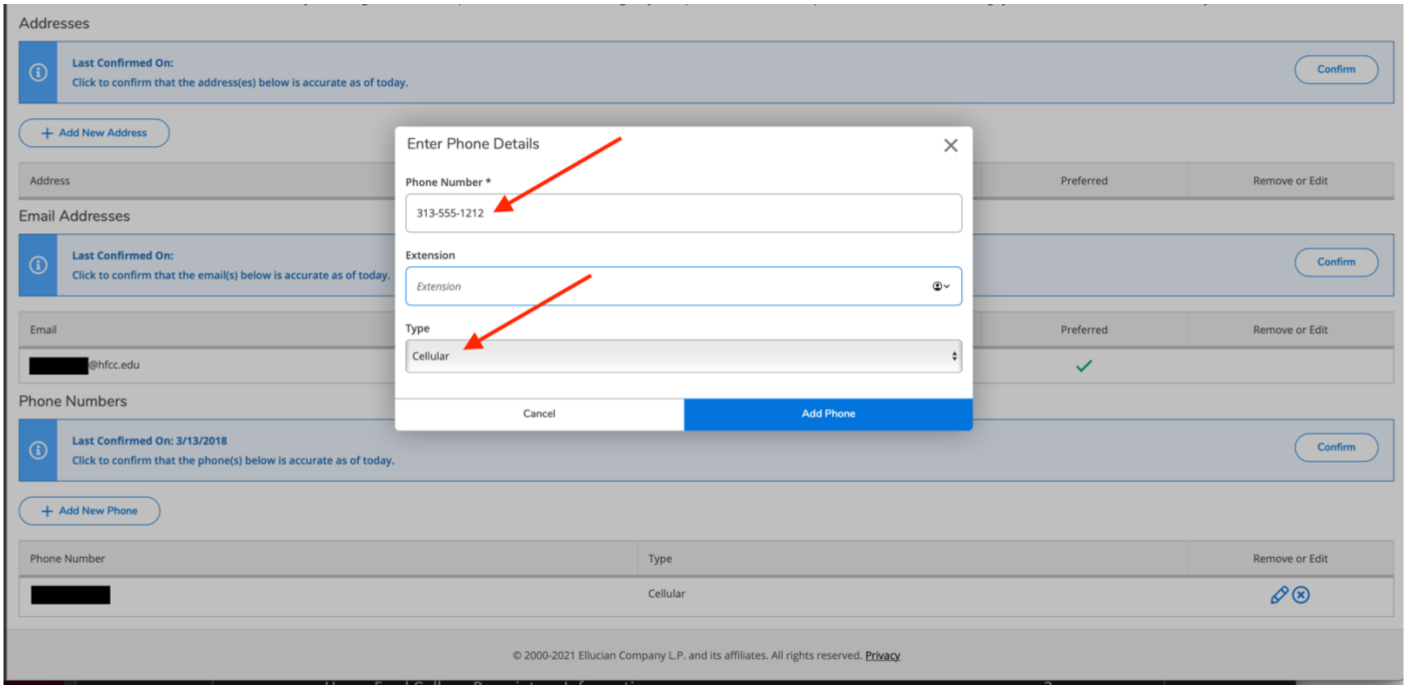


Phone Numbers

Last Confirmed On: 3/13/2018
Click to confirm that the phone(s) below is accurate as of today.

Phone Number	Type	Remove or Edit
[redacted]	Cellular	✎ ⊗

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.



Addresses

Last Confirmed On:
Click to confirm that the address(es) below is accurate as of today.
Confirm

+ Add New Address

Address	Preferred	Remove or Edit

Email Addresses

Last Confirmed On:
Click to confirm that the email(s) below is accurate as of today.
Confirm

Email	Preferred	Remove or Edit
[redacted]@hfcc.edu	✓	

Phone Numbers

Last Confirmed On: 3/13/2018
Click to confirm that the phone(s) below is accurate as of today.
Confirm

+ Add New Phone

Phone Number	Type	Remove or Edit
[redacted]	Cellular	✎ ⊗

Enter Phone Details

Phone Number *
313-555-1212

Extension
Extension

Type
Cellular

Cancel
Add Phone

© 2000-2021 Ellucian Company L.P. and its affiliates. All rights reserved. Privacy

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

If you plan on using the Smartphone “Push” Notification for 2FA, then you must first install the NetIQ Advanced Authentication App on your device. If you do not plan on using Smartphone “Push” Notification, then you may skip installing this application.

The application can be downloaded by scanning one of the following QR Codes using your phone’s camera:

For Android Devices:

For iOS Devices:

If you have a problem scanning the QR code, you can also install the application using the following links:

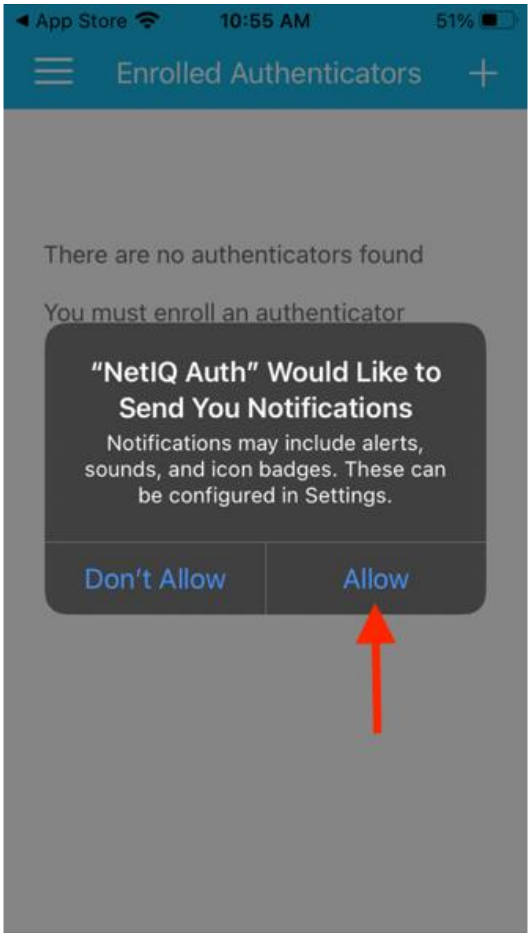
Android:

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

iOS:

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

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, facial recognition) are not available. On iOS, be sure to **allow notifications** from this application. It is very important that you allow these notifications, otherwise you will NOT get notified to approve logins:



◀ App Store 10:55 AM 51%

Enrolled Authenticators

There are no authenticators found

You must enroll an authenticator

"NetIQ Auth" Would Like to Send You Notifications

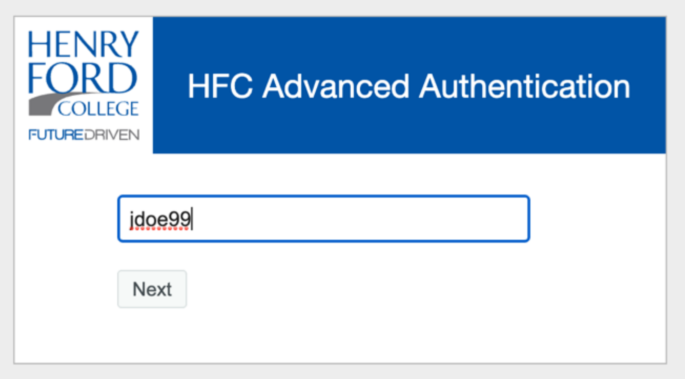
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Enrolling a Smartphone

After installing the NetIQ Advanced Authentication App on your device, access the Henry Ford College Advanced Authentication Enrollment Portal from your desktop web browser (this can be done on or off campus):

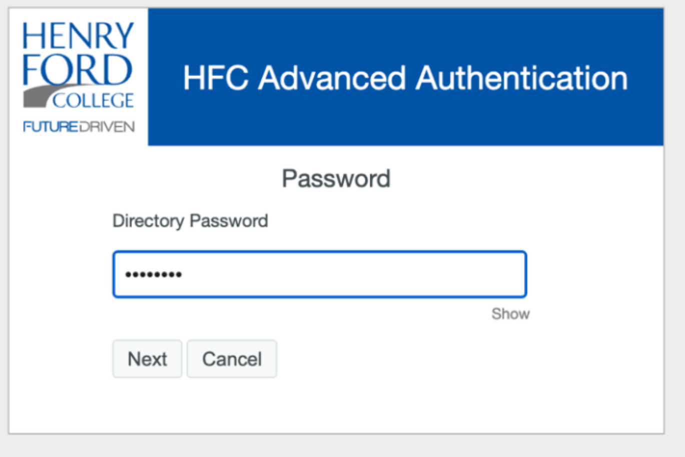
https://advauth.hfcc.edu/

Enter your Username:



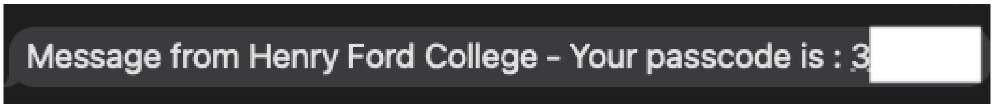
jdoe99

Enter your HFC password:



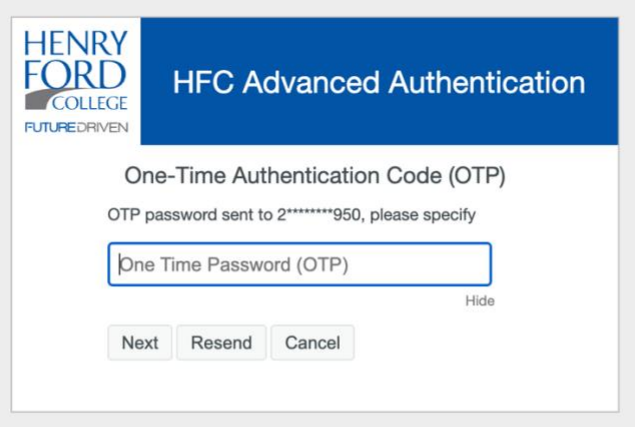
••••••••

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



Message from Henry Ford College - Your passcode is : 3[redacted]

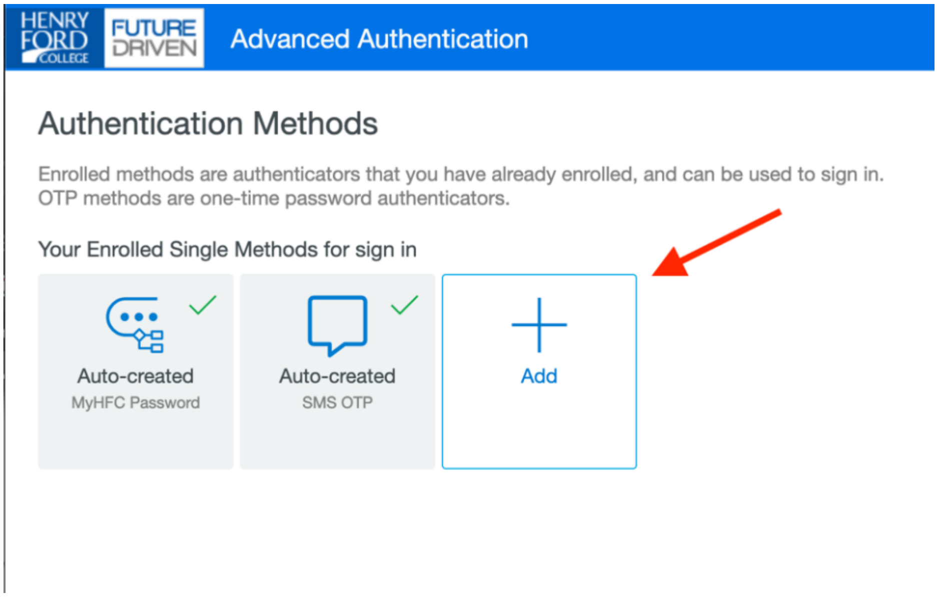
Enter that value in the next box:


HFC Advanced Authentication

One-Time Authentication Code (OTP)

OTP password sent to 2********950, please specify

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:

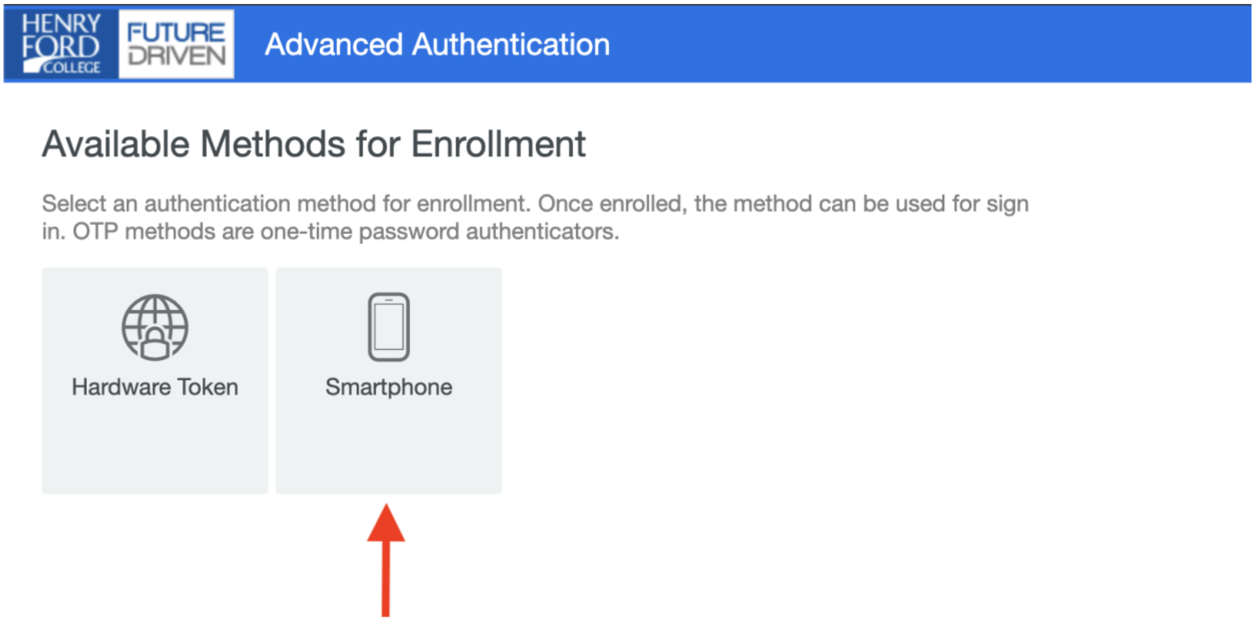

Advanced Authentication

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:

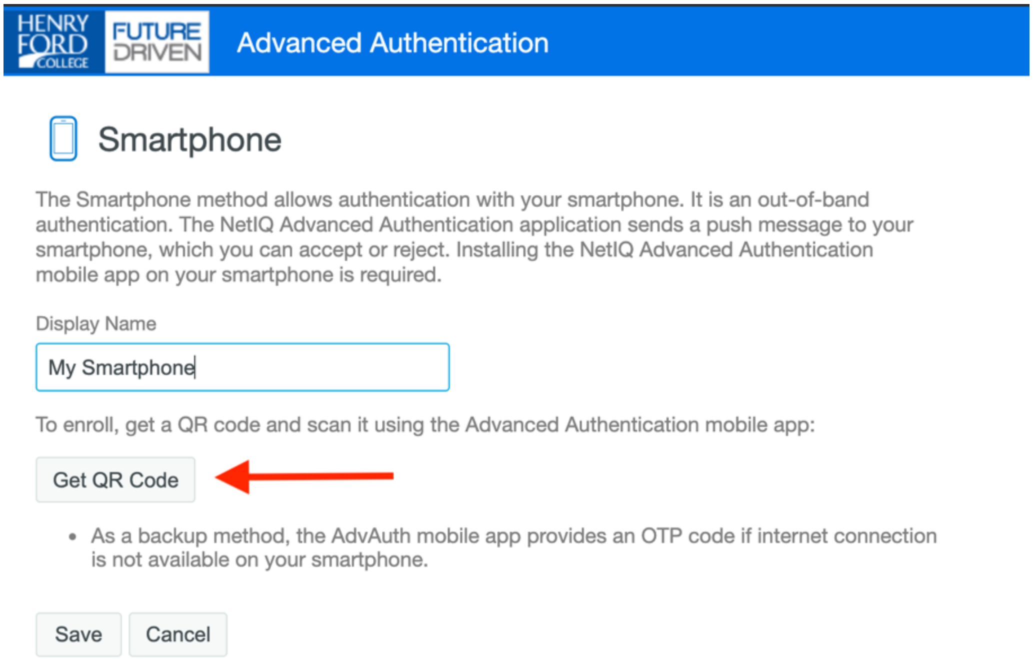


Advanced Authentication

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":



Advanced Authentication

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.

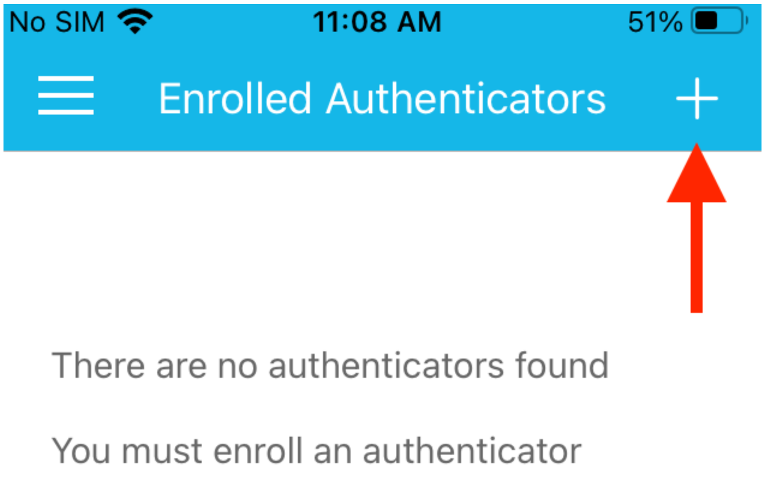
Display Name

My Smartphone

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.

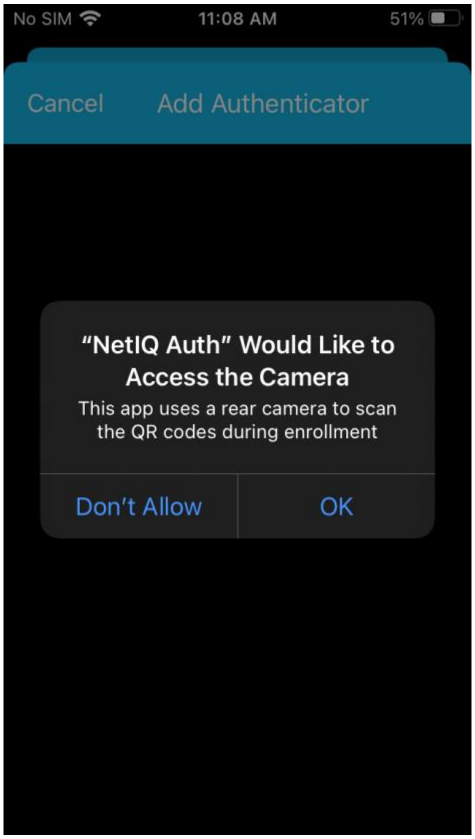
A QR Code will be displayed. Scan the QR code using the NetIQ Authentication App on your Smartphone. Open the NetIQ Authentication App on your phone and click the “+” on the top right:



There are no authenticators found

You must enroll an authenticator

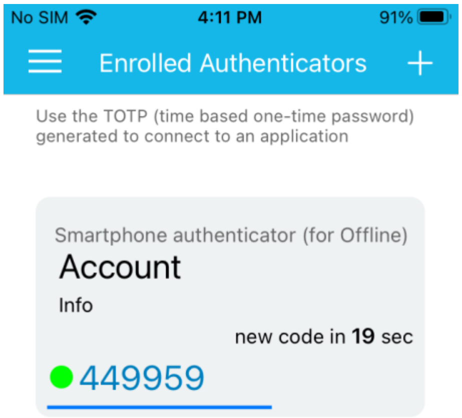
If your phone asks, allow NetIQ Authentication App to access your camera:



“NetIQ Auth” Would Like to Access the Camera

This app uses a rear camera to scan the QR codes during enrollment

At this point, aim your phone camera at the QR code on your computer screen. The application should identify the QR code and display a screen like the one shown below:



Enrolled Authenticators

Use the TOTP (time based one-time password) generated to connect to an application

Smartphone authenticator (for Offline)

Account

Info

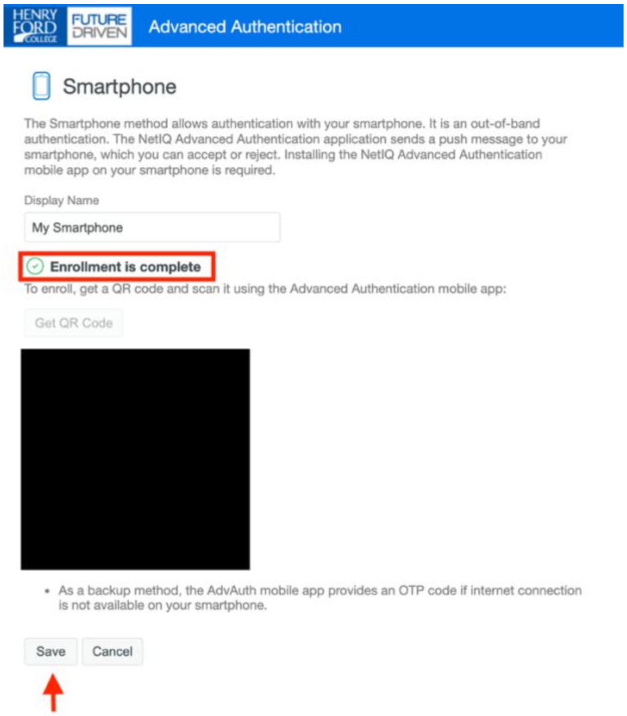
new code in **19** sec

● 449959

After the first successful authentication, your user ID information will appear in place of "Account" (on Android this area is blank until the first authentication).

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 like the following that shows "Enrollment is complete." Be sure to click "Save" to save the authenticator!



Advanced Authentication

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

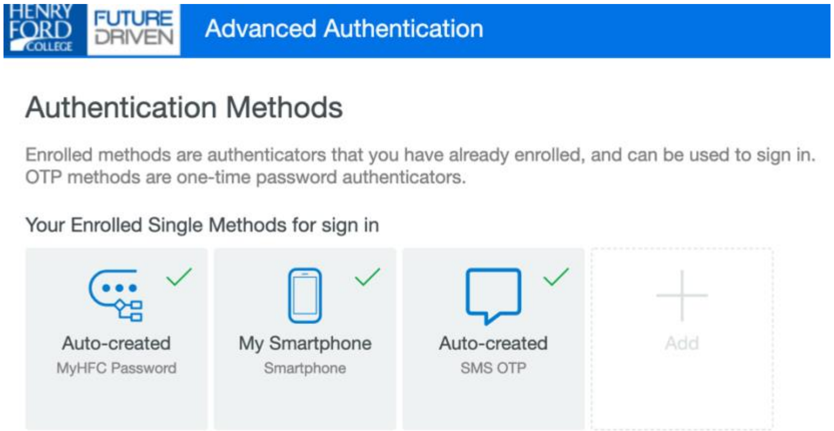
✓ **Enrollment is complete**

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

[redacted]

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

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



Authentication Methods

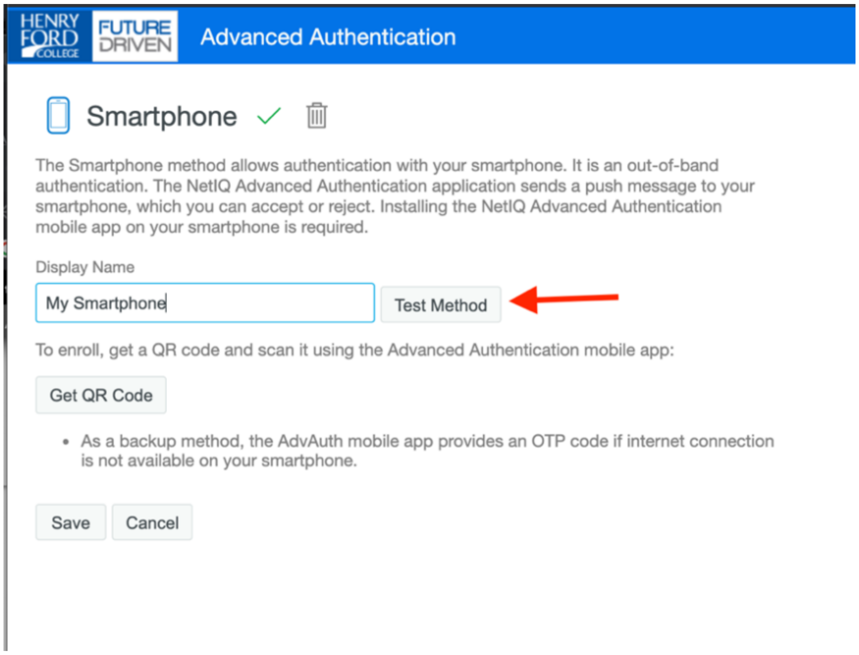
Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in

This completes the enrollment process.

Testing Your Enrolled Smartphone

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



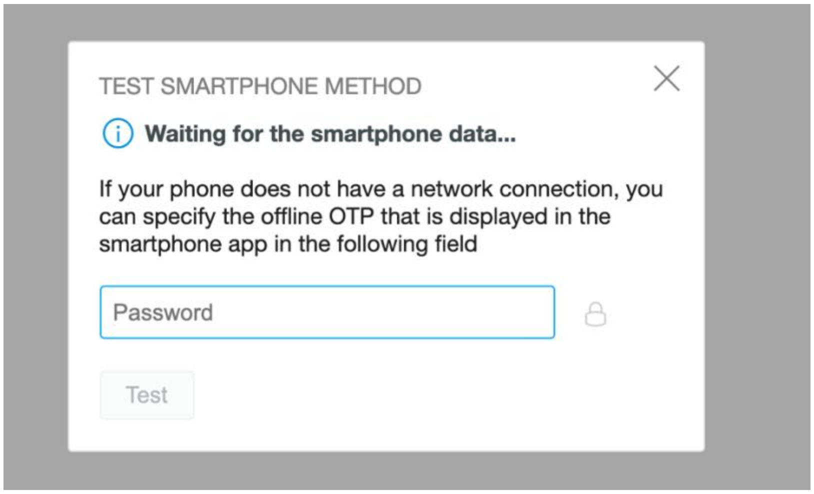
The Smartphone method allows authentication with your smartphone. It is an out-of-band authentication. The NetIQ Advanced Authentication application sends a push message to your smartphone, which you can accept or reject. Installing the NetIQ Advanced Authentication mobile app on your smartphone is required.

Display Name: My Smartphone

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.

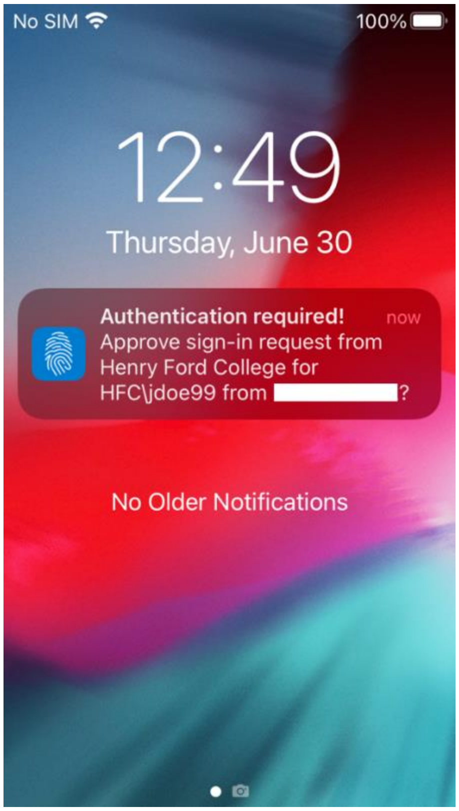
A screen like the following will come up:



Waiting for the smartphone data...

If your phone does not have a network connection, you can specify the offline OTP that is displayed in the smartphone app in the following field

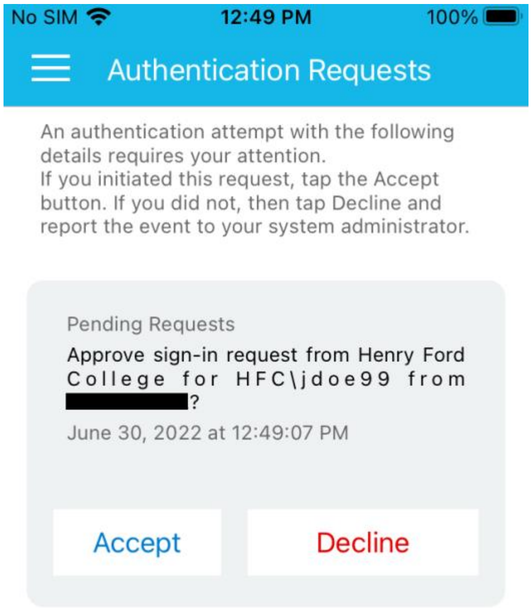
If your phone is locked, you should see a notification like this on iOS:



Authentication required!
Approve sign-in request from Henry Ford College for HFC\jdoe99 from [redacted]?

No Older Notifications

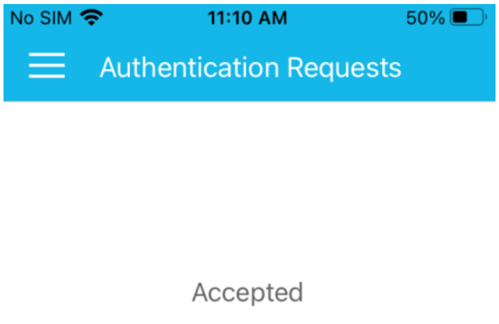
The NetIQ Authentication App MUST be allowed to send notifications, or this will NOT be seen. Tap the notification and unlock your device. You should be presented with a screen like the following:



An authentication attempt with the following details requires your attention.
If you initiated this request, tap the Accept button. If you did not, then tap Decline and report the event to your system administrator.

Pending Requests
Approve sign-in request from Henry Ford College for HFC\jdoe99 from [redacted]?
June 30, 2022 at 12:49:07 PM

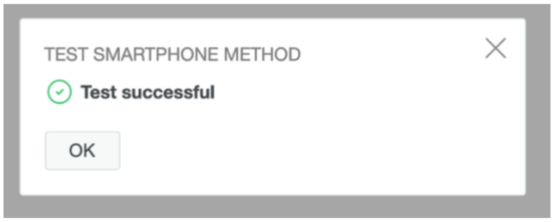
Tap “Accept”. This should result in the following:



Authentication Requests

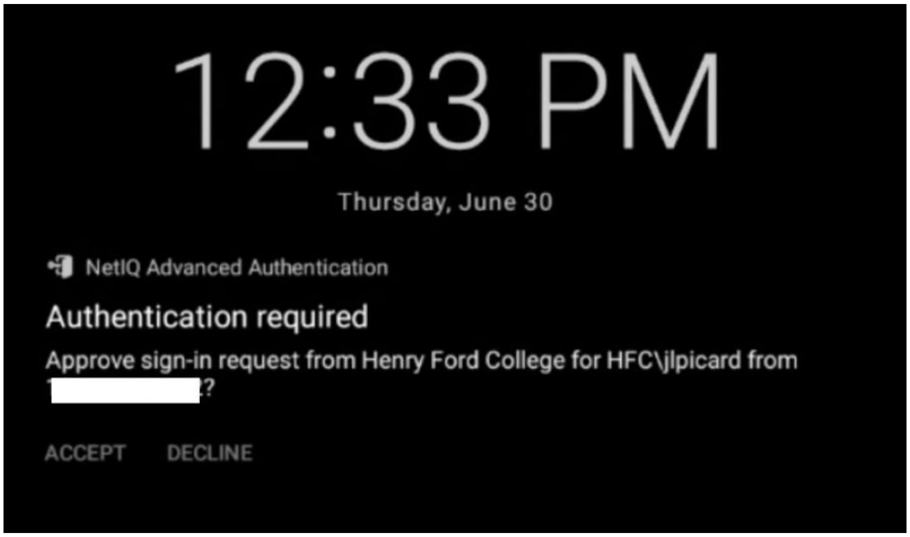
Accepted

And on your desktop, you should see:


TEST SMARTPHONE METHOD

✓ Test successful

On a device running Android, you can Accept or Decline the authentication request directly from the lock screen or notification message itself (this is not possible on iOS). The notification will look like this on the Android lock screen:


12:33 PM

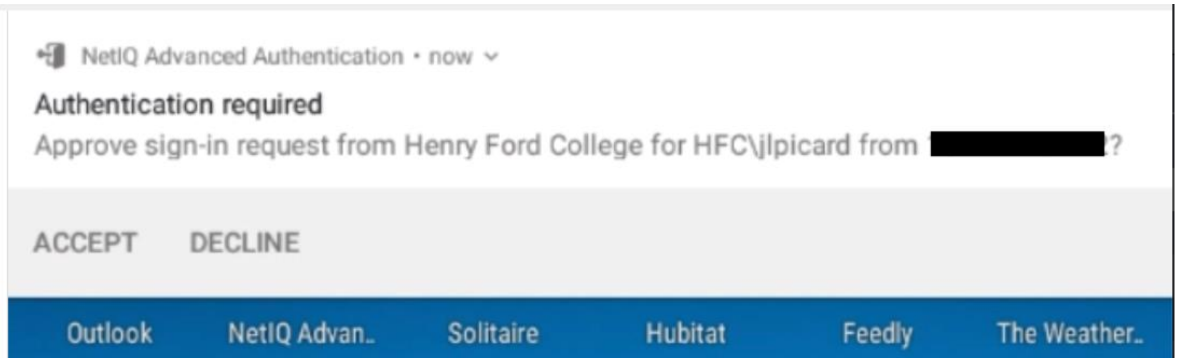
Thursday, June 30

NetIQ Advanced Authentication

Authentication required

Approve sign-in request from Henry Ford College for HFC\jlpicard from [redacted]?

Or like this from the notification pop-up on an unlocked device:



NetIQ Advanced Authentication • now

Authentication required

Approve sign-in request from Henry Ford College for HFC\jlpicard from [redacted]?

Tapping “Accept” on either notification should also result in the “Test Successful” message appearing on your desktop.

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

Enrolling a Hardware Token

Any FIDO compliant hardware token can be used with the HFC authentication system. HFC recommends using FIDO tokens from Yubico, specifically the “Security Key NFC”, which can be purchased directly from Yubico here:

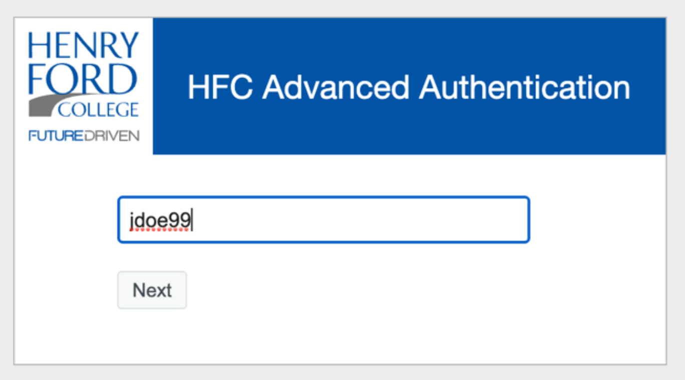
https://www.yubico.com/product/security-key-series/security-key-nfc-by-yubico-black/

Both a USB-A and USB-C version are available and both support Near Field Communication (NFC) as well.

To enroll the token, access the Henry Ford College Advanced Authentication Enrollment Portal from your desktop web browser (this can be done on or off campus):

https://advauth.hfcc.edu/

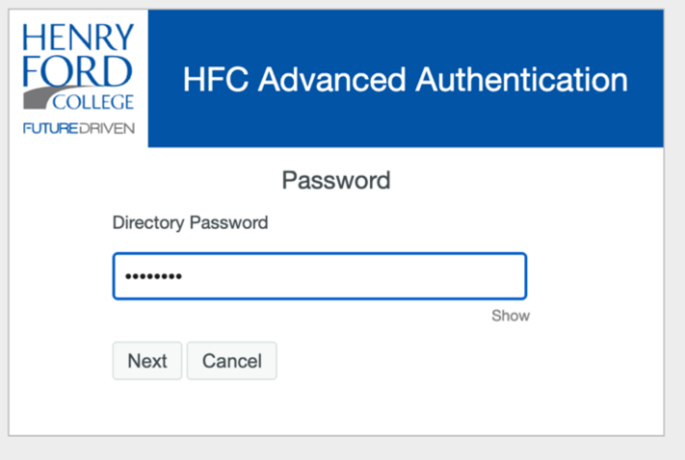
Enter your Username:



HFC Advanced Authentication

jdoe99

Enter your HFC password:

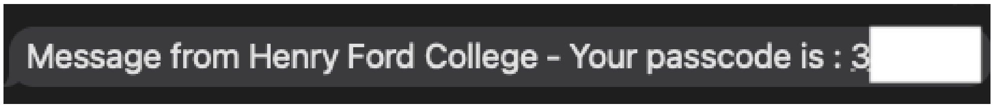


HFC Advanced Authentication

Password

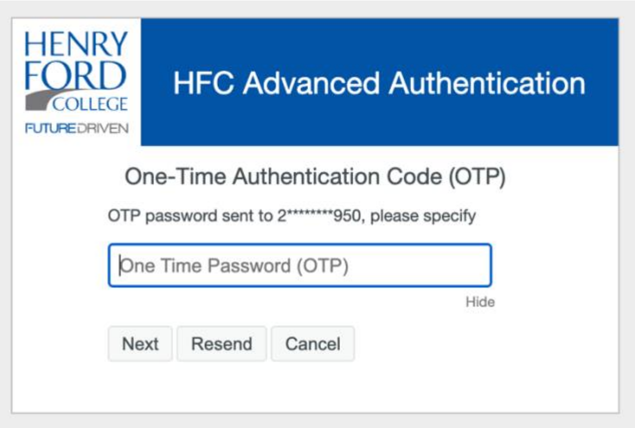
Directory Password: ••••••••

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



Message from Henry Ford College - Your passcode is : [redacted]

Enter that value in the next box:

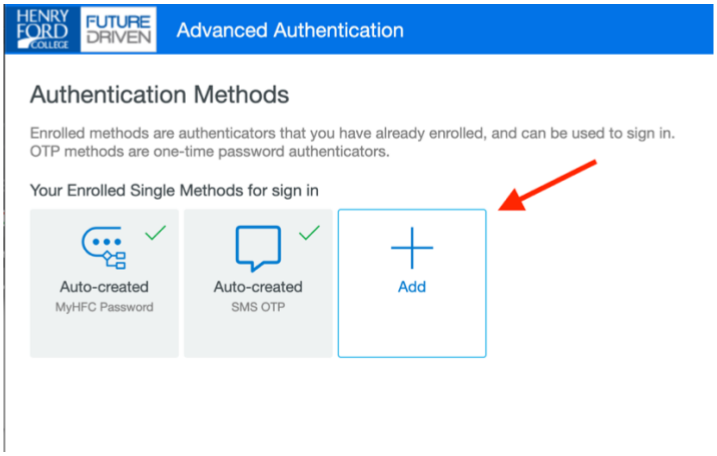


HFC Advanced Authentication

One-Time Authentication Code (OTP)

OTP password sent to 2********950, please specify

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:



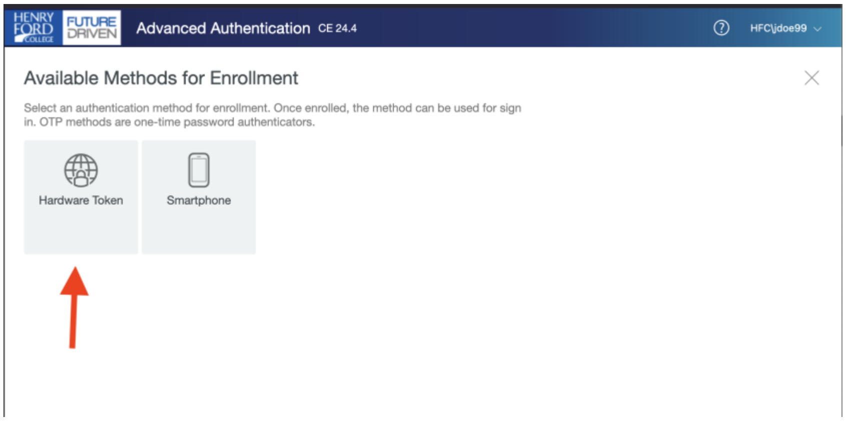
Advanced Authentication

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

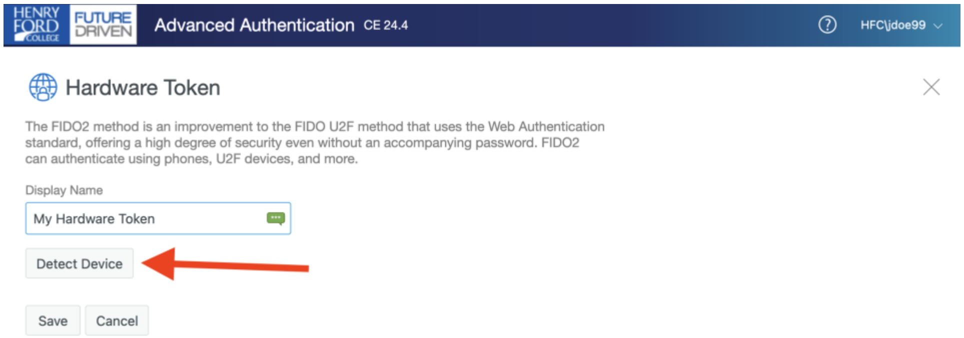
On the next screen, select Hardware Token:



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.

On the next screen, give the token a name and then click "Detect Device."

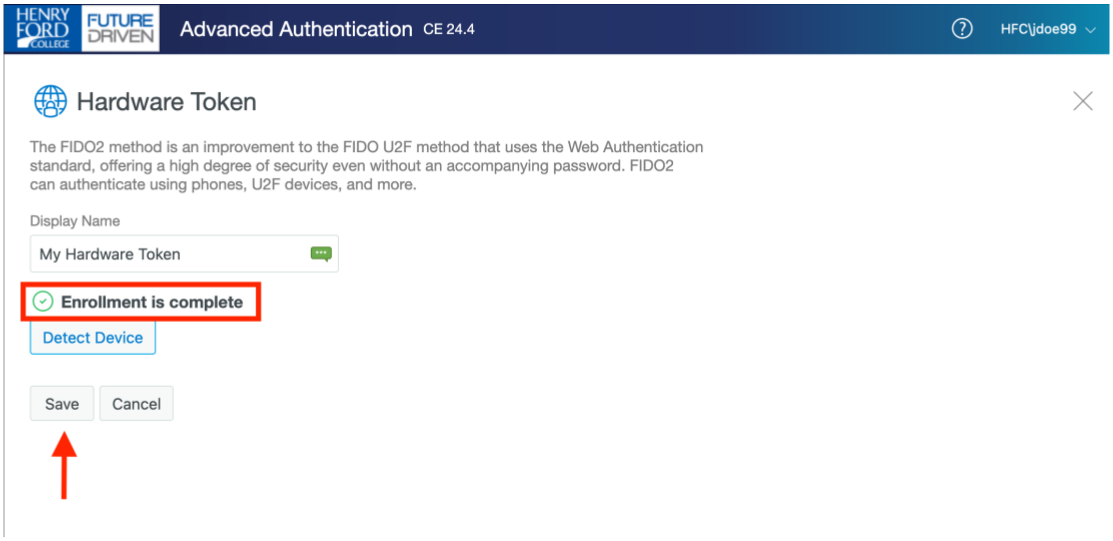


Hardware Token

The FIDO2 method is an improvement to the FIDO U2F method that uses the Web Authentication standard, offering a high degree of security even without an accompanying password. FIDO2 can authenticate using phones, U2F devices, and more.

Display Name: My Hardware Token

Once you click "Detect Device", you will be prompted to either insert your token into a USB port on your computer or, if your computer and token both support NFC, bring the token near your computer, and touch the device. If your token requires that you enter a Personal Identification Number (PIN) code, you will be prompted to enter the code and touch the token a second time. If you are using a MacBook with the Touch ID feature, you can use it as a FIDO token if you desire. If you are using a MacBook and do not want to use the MacBook's built in Touch ID as a FIDO token, you may need to indicate that you would like to use a different security key after clicking the "Detect Device" button. Once enrolled, you will see a screen as follows:



Advanced Authentication CE 24.4

HFC\jdoe99

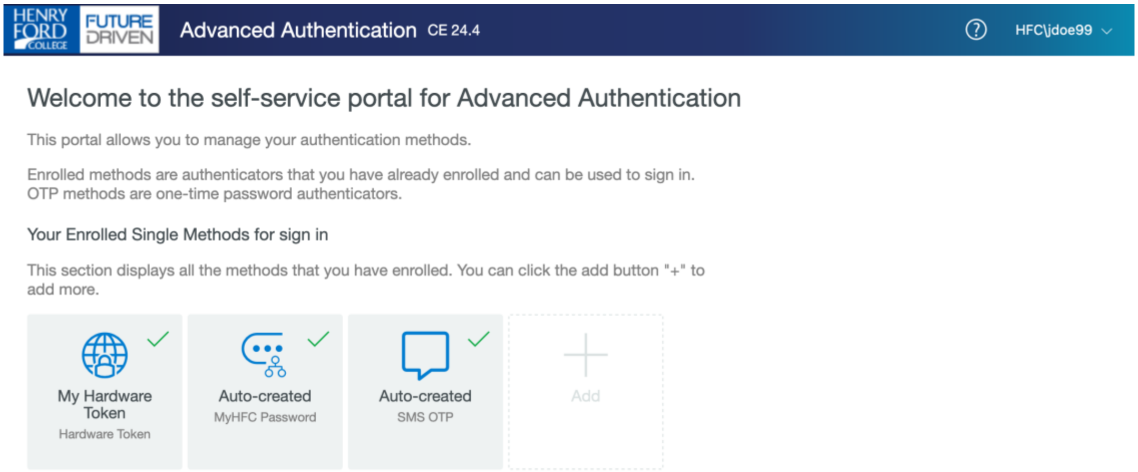
Hardware Token

The FIDO2 method is an improvement to the FIDO U2F method that uses the Web Authentication standard, offering a high degree of security even without an accompanying password. FIDO2 can authenticate using phones, U2F devices, and more.

Display Name: My Hardware Token

✓ Enrollment is complete

Click save to save the enrollment and you should now see the following screen:



Advanced Authentication CE 24.4

HFC\jdoe99

Welcome to the self-service portal for Advanced Authentication

This portal allows you to manage your 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.

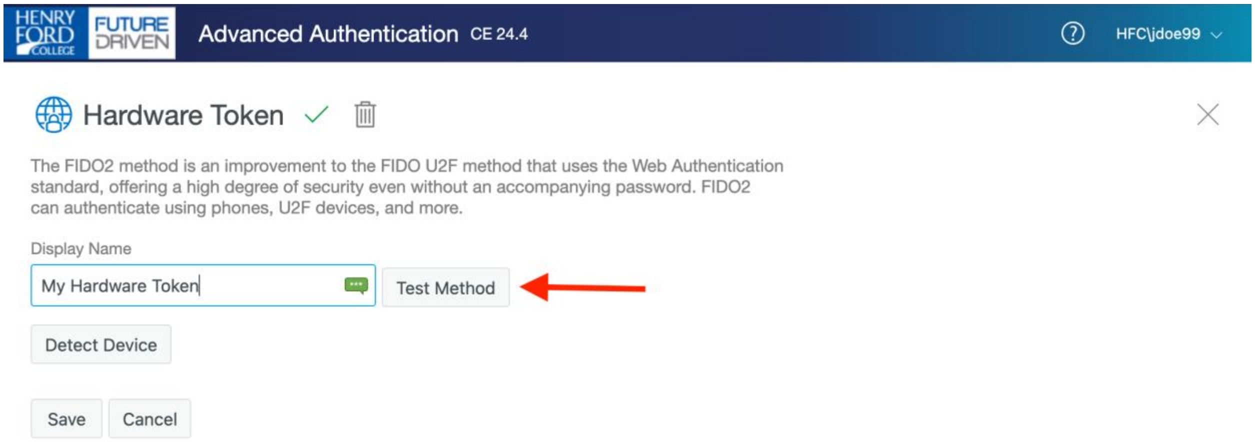
Your Enrolled Single Methods for sign in

This section displays all the methods that you have enrolled. You can click the add button "+" to add more.

This completes enrollment of a hardware token.

Testing Your Enrolled Hardware Token

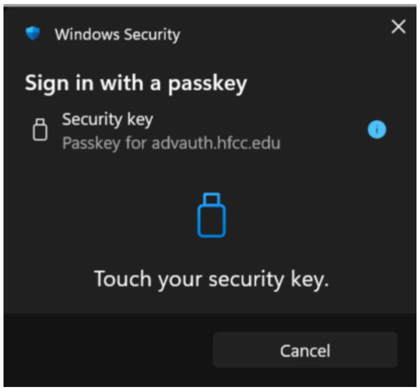
Once your token is enrolled, you can verify that the token works properly with the authentication system. Login back into the Enrollment Portal and select the “My Hardare Token” (or whatever name you choose for the token). On the next screen, select the “Test Method” button.



The FIDO2 method is an improvement to the FIDO U2F method that uses the Web Authentication standard, offering a high degree of security even without an accompanying password. FIDO2 can authenticate using phones, U2F devices, and more.

Display Name: My Hardware Token

The browser will prompt you to insert your token (or bring it near) and touch the token to satisfy the request (Microsoft Windows 11 example shown below).

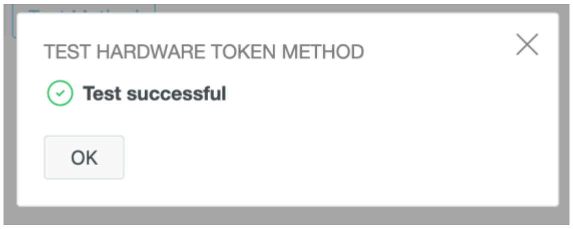


Sign in with a passkey

Security key
Passkey for advauth.hfcc.edu

Touch your security key.

If it is successful, the following will be seen:



TEST HARDWARE TOKEN METHOD

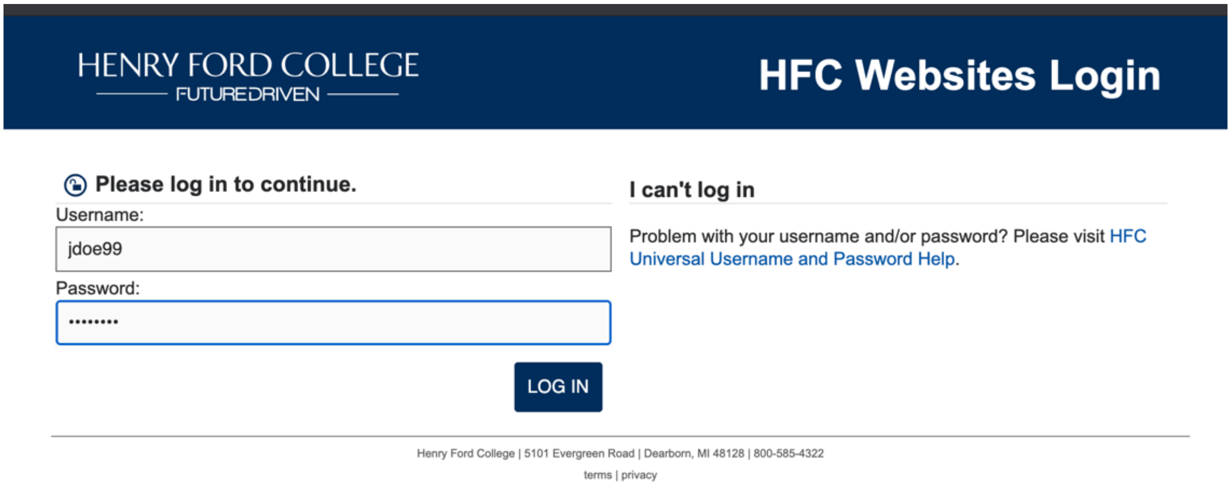
Test successful

This indicates a successful test of the FIDO token.

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:



Username: jdoe99

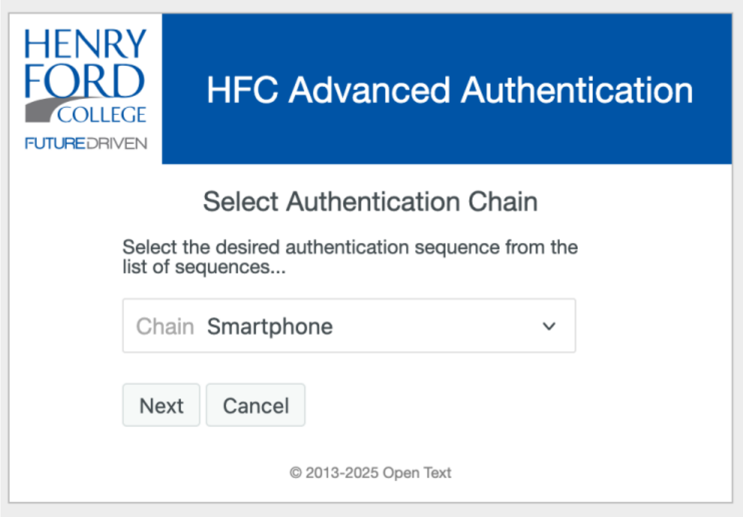
Password: ••••••••

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

If you have multiple 2FA methods enrolled you will be prompted to select the method you would like to use (current options are Smartphone, SMS, or Hardware Token):

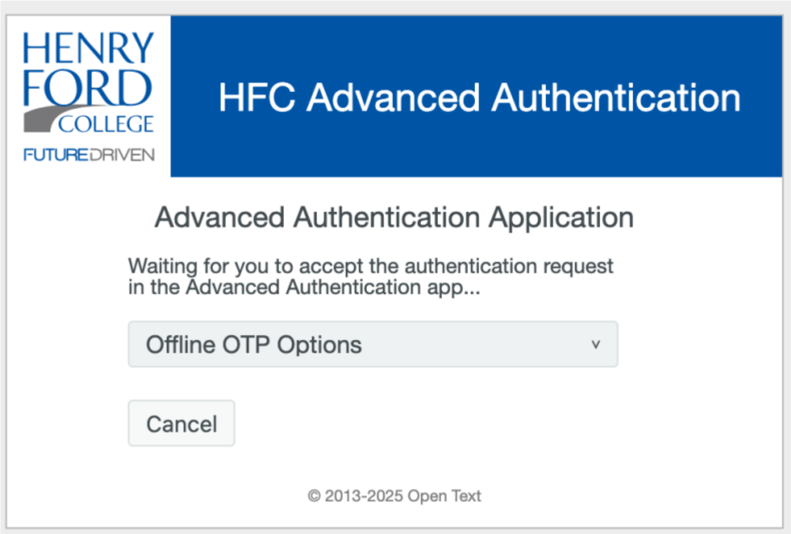


Select the desired authentication sequence from the list of sequences...

Chain Smartphone

© 2013-2025 Open Text

In this example, we take the default of “Smartphone” and hit “Next”. On the following screen, you will see:



HENRY FORD COLLEGE FUTUREDRIVEN

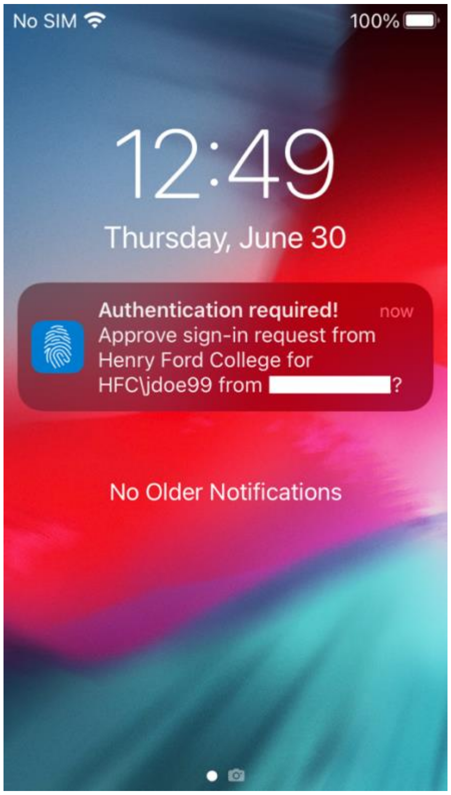
HFC Advanced Authentication

Advanced Authentication Application

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

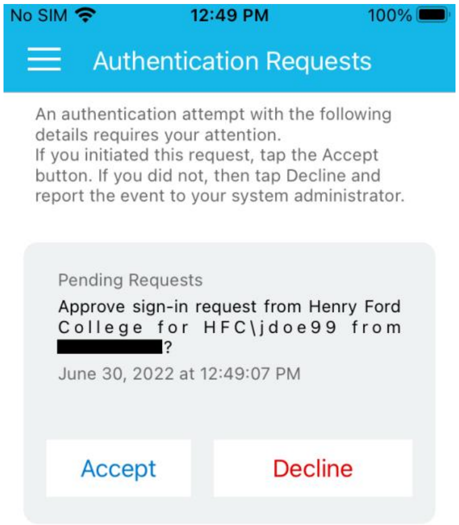
© 2013-2025 Open Text

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 (iOS device shown):



Authentication required! now
Approve sign-in request from Henry Ford College for HFC\jdoe99 from [redacted]?

On devices running the Android operating system, you have the option to Accept or Decline from this message without going into the NetIQ Authentication application. On iOS, Click the notification and unlock your device. NetIQ Authentication will prompt you to Accept or Decline the request:



An authentication attempt with the following details requires your attention.
If you initiated this request, tap the Accept button. If you did not, then tap Decline and report the event to your system administrator.

Pending Requests

Approve sign-in request from Henry Ford College for HFC\jdoe99 from [redacted]?

June 30, 2022 at 12:49:07 PM

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

Frequently Asked Questions

Q. Can I enroll multiple smartphones?

A. You can only enroll one smartphone at this time.

Q. Can I enroll multiple hardware tokens?

A. You can only enroll one token at this time.

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 lost my phone and cannot get SMS text messages, what can I do?

A. The HFC Help Desk can provide you with a one-time use emergency password to get you into the enrollment portal so that you can enroll a new device. If you have an alternate phone number that can receive text messages, your mobile number can also be updated in HANK. If you do update your phone number, please allow time for the authentication system to receive the updated information.

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

A. Follow 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, SMS OTP, or a hardware token (if enrolled) as your second factor. Receiving push notifications requires that your smartphone has unrestricted Internet access and that notifications for the NetIQ App are allowed on your phone.

Q. I don’t want to use my phone as a second factor, what are my options?

A. Hardware (FIDO) Token.