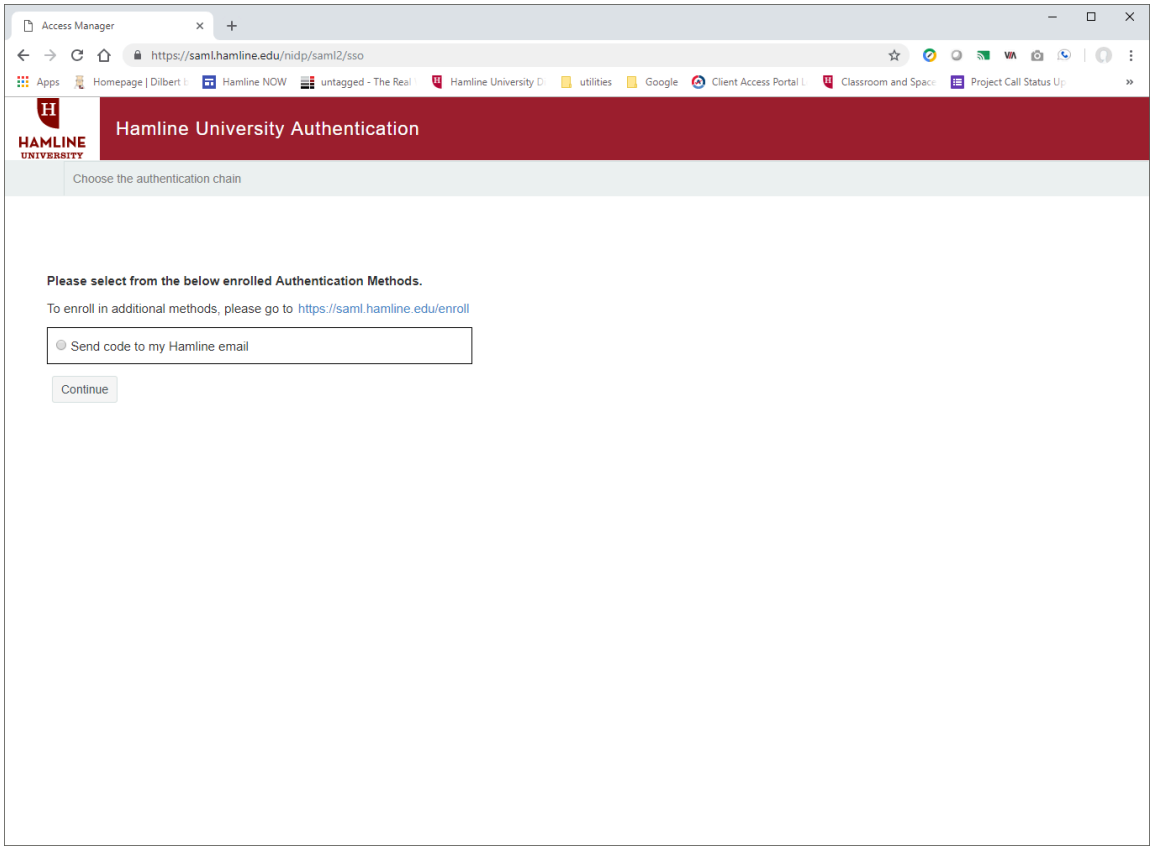
Workday Two-Factor Authentication

Sign In to Workday

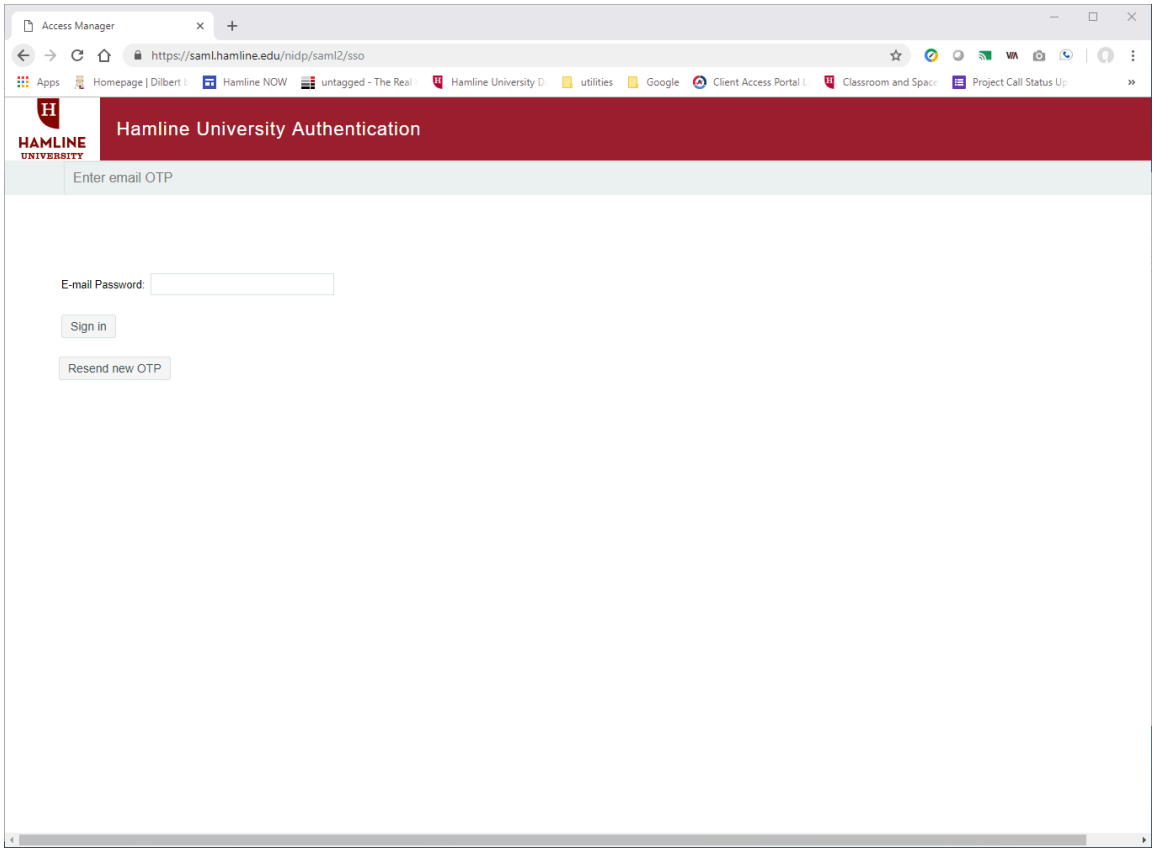
All employees and students will have Workday Two-Factor Authentication enabled, requiring a One-Time Password (OTP) in addition to their Hamline passphrase. This greatly enhances security by preventing unauthorized logins.

Please note that Workday Two-Factor Authentication is not connected to Google 2-step Verification and they are managed separately. Google 2-Step settings will not affect Workday Two-Factor settings and vice-versa.

Upon your first Workday login, you'll be prompted to set up a method for receiving the OTP. At the *Choose the authentication chain* screen, your Hamline email address is selected as the default method.



Select **Send code to my Hamline email** and click **Continue**. The *Enter email OTP* screen will appear with a prompt for "Email Password"

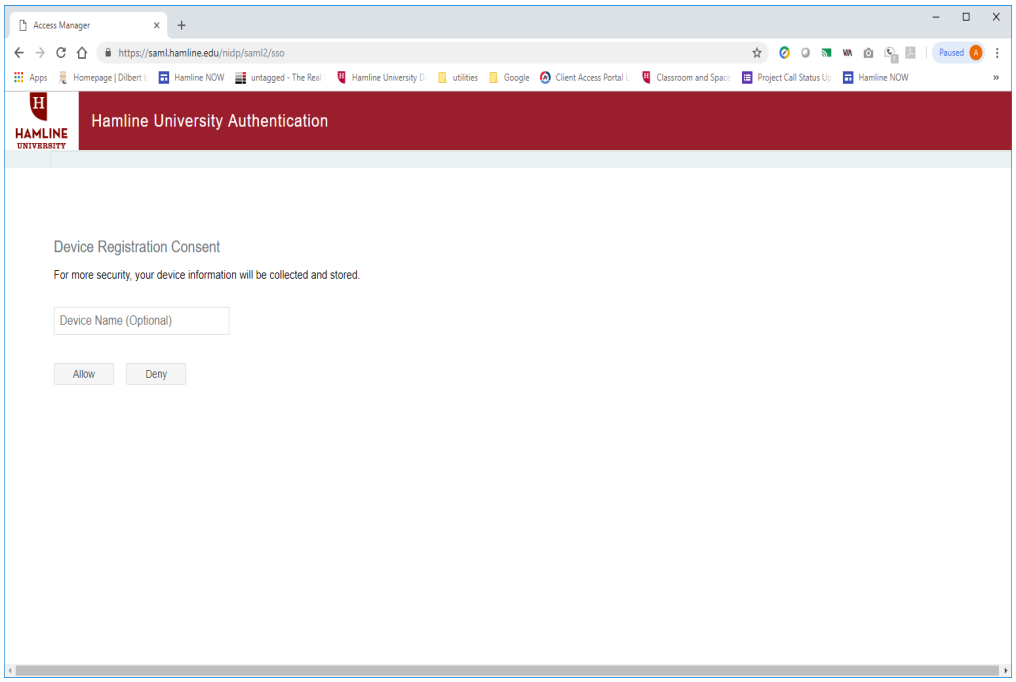


Check your Hamline Gmail for the email message containing the OTP, enter it in the Email Password field, then click **Sign in** to enter Workday. **Please note, even though it says "Email Password", you should put in the code that was sent to your email, not your Hamline password.**

Note: if the OTP is not entered within five minutes, the browser tab must be closed and the Workday login process restarted.

Additional Workday Two-Factor methods can be set up via https://saml.hamline.edu/account

Once your 2nd factor has been entered, it will prompt you whether you want to save the device:

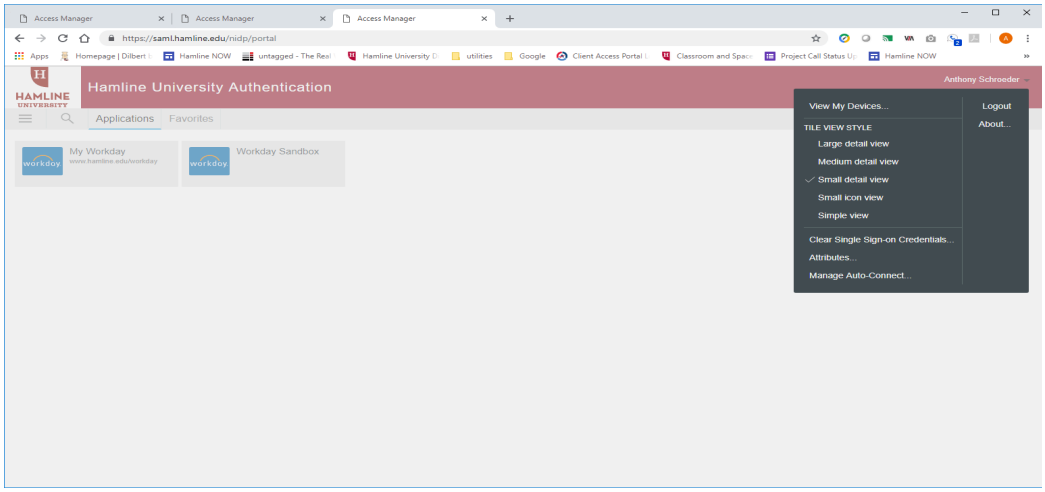


You can either

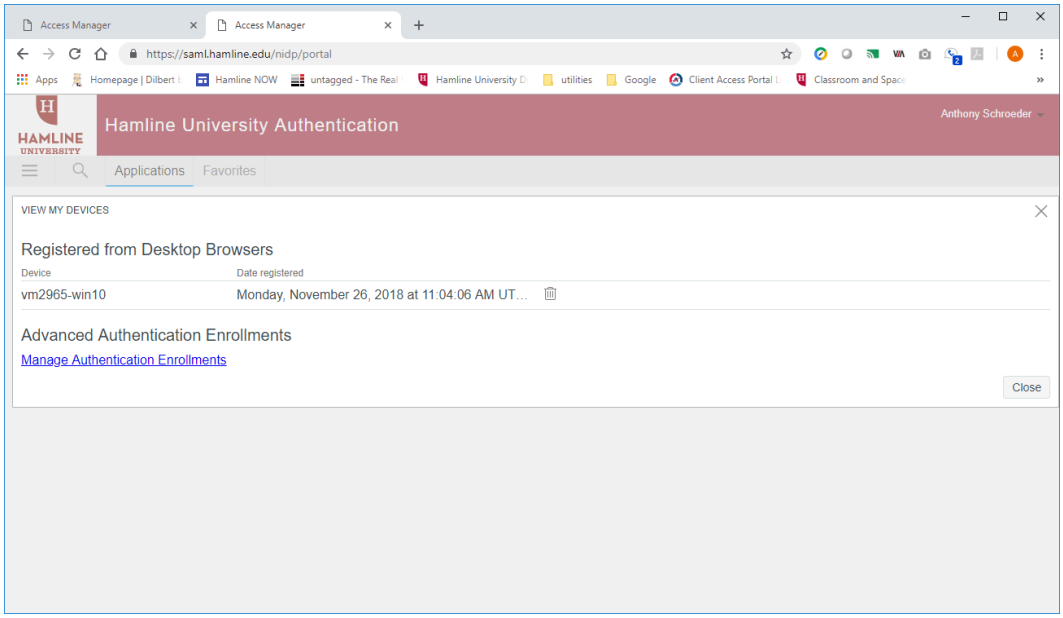
1. give the device a name and click “Allow”, which will save the device in your profile, and not prompt you on that device again for 30 days. This is only recommended for non-shared devices such as your chromebook, laptop, or desktop.
2. Click “Deny”, which will not save the device. This is recommended for “Public” devices, such as computer lab machines, kiosks, and public or untrusted terminals.

Please note - the system will remember up to 5 devices. Once you go over 5, the oldest device will be removed, and replaced with the newest registered device.

You can view your devices by going to https://saml.hamline.edu/nidp/portal and log in, if necessary. Once you have logged in, click on your name in the upper right, and there should be an option to “view my devices” on the menu that comes up:



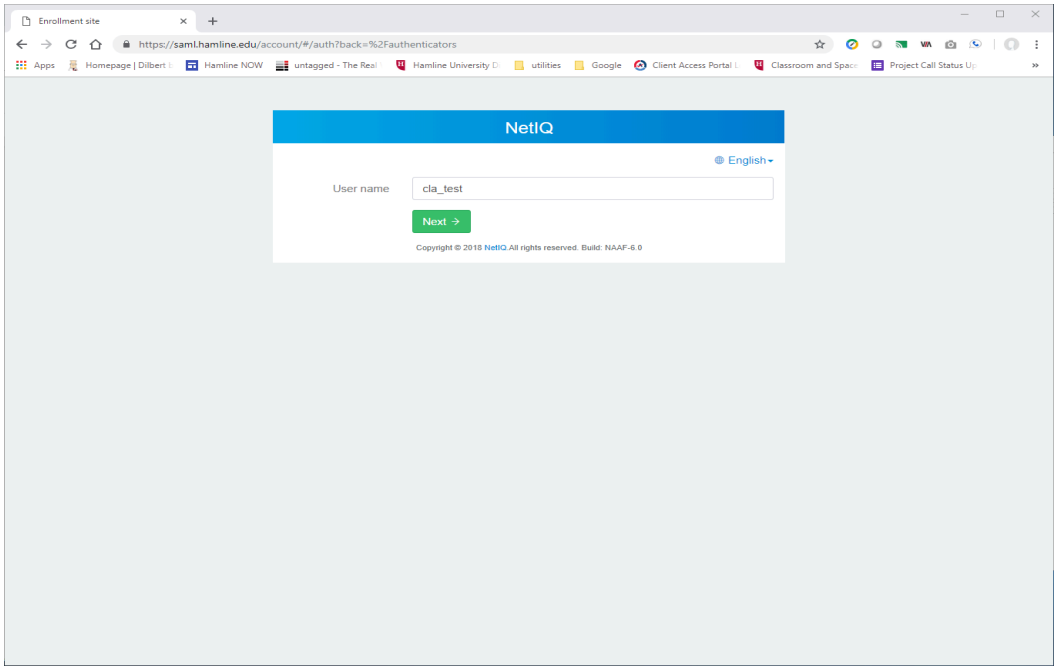
You can then view and delete any devices that you have saved:


Access Manager
Access Manager
https://saml.hamline.edu/nidp/portal
Apps
Homepage | Dilbert
Hamline NOW
untagged - The Real
Hamline University D
utilities
Google
Client Access Portal
Classroom and Space
HAMLINE
UNIVERSITY
Hamline University Authentication
Anthony Schroeder
Applications
Favorites
VIEW MY DEVICES
Registered from Desktop Browsers
Device
Date registered
vm2965-win10
Monday, November 26, 2018 at 11:04:06 AM UT...
Advanced Authentication Enrollments
Manage Authentication Enrollments
Close

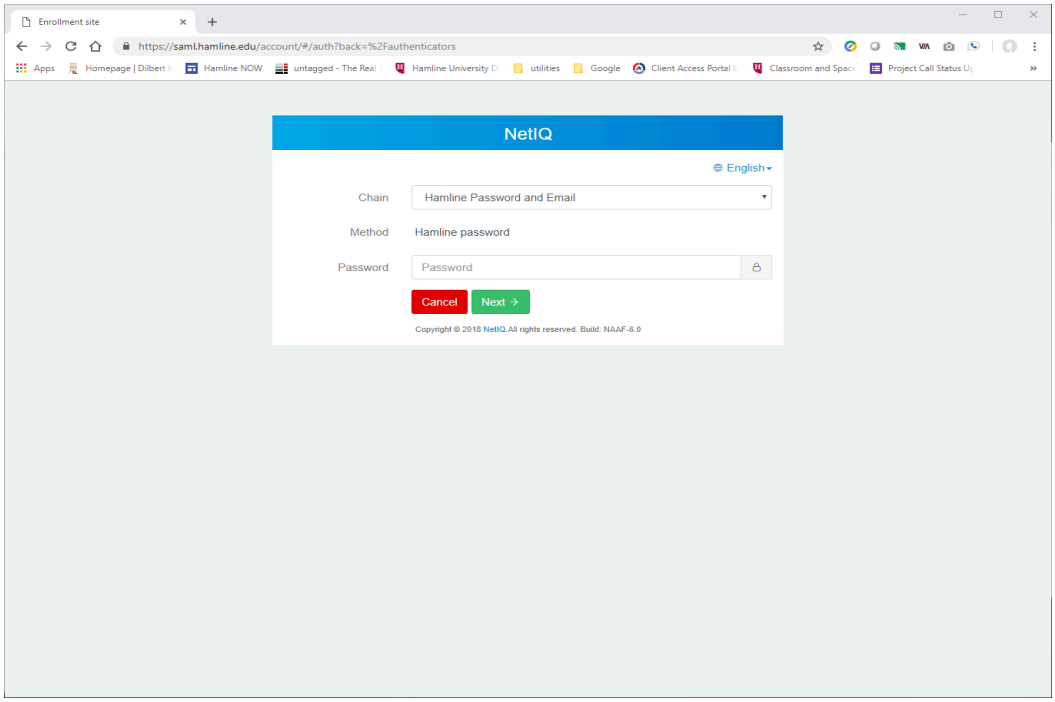
Setting up additional two-factor authentication methods

Additional Workday Two-Factor methods can be set up via https://saml.hamline.edu/account

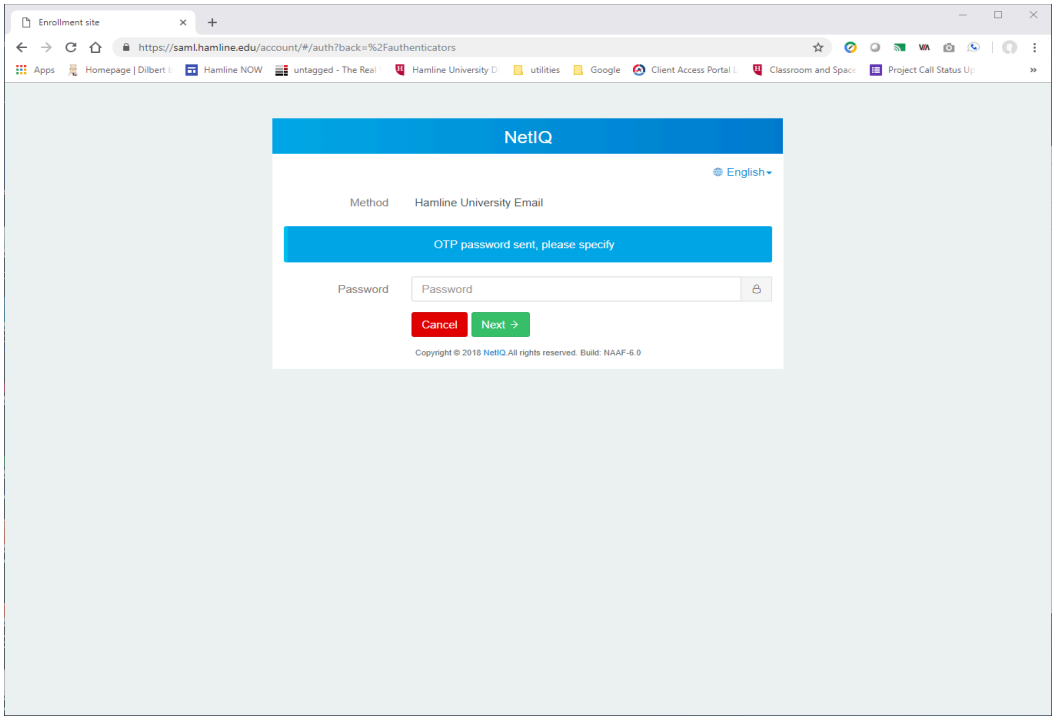
1. Log in with your Hamline username (without the @hamline.edu)



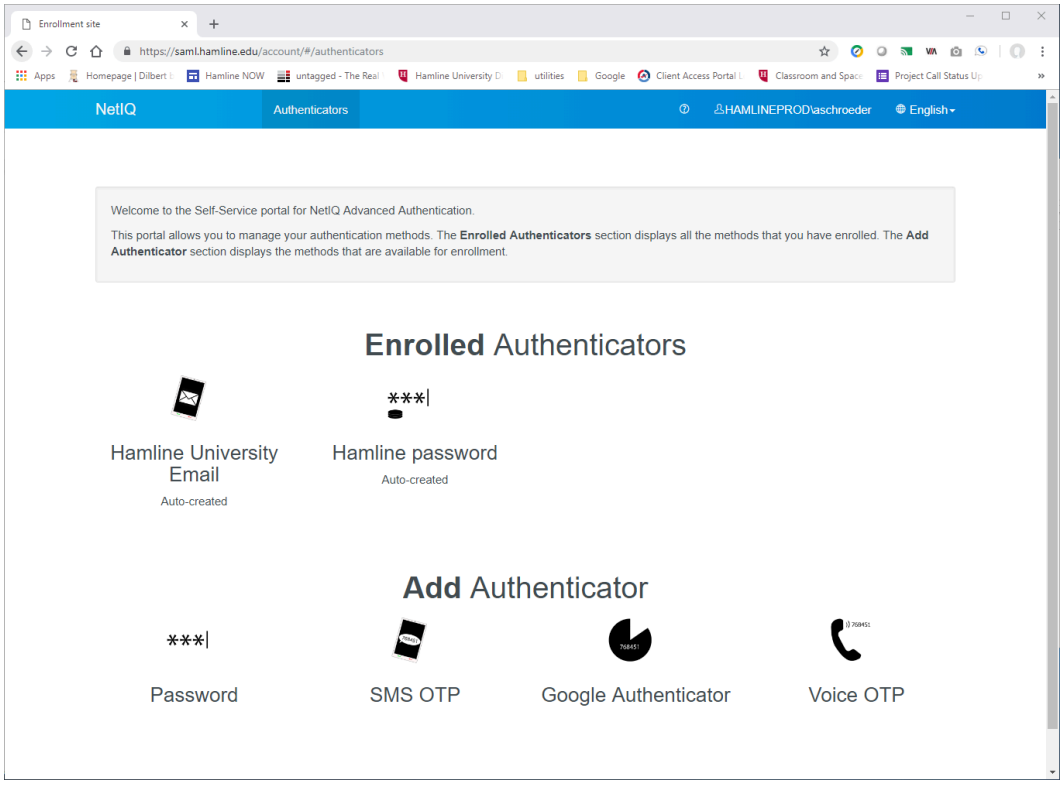
2. Type in your password



3. It will prompt you for a one time password (OTP) from your email - there should have been a code sent to your Hamline email address - type in that code



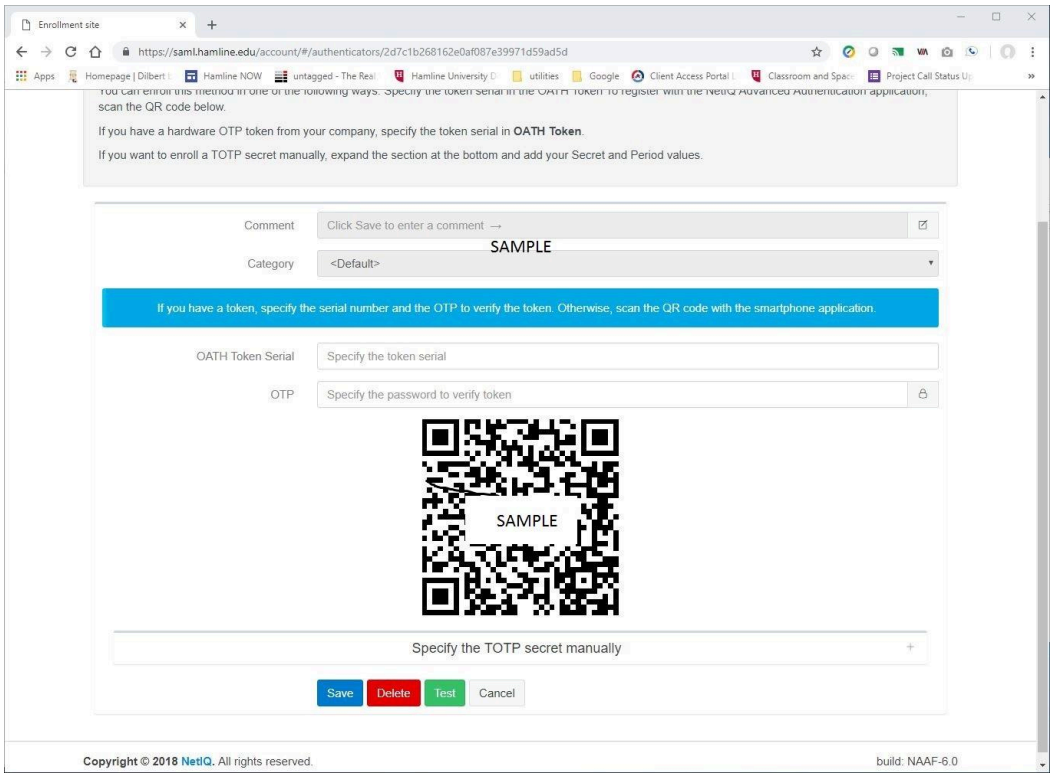
4. That should bring you to the self service portal. It will list your currently setup 2 factor methods under “Enrolled Authenticators”.



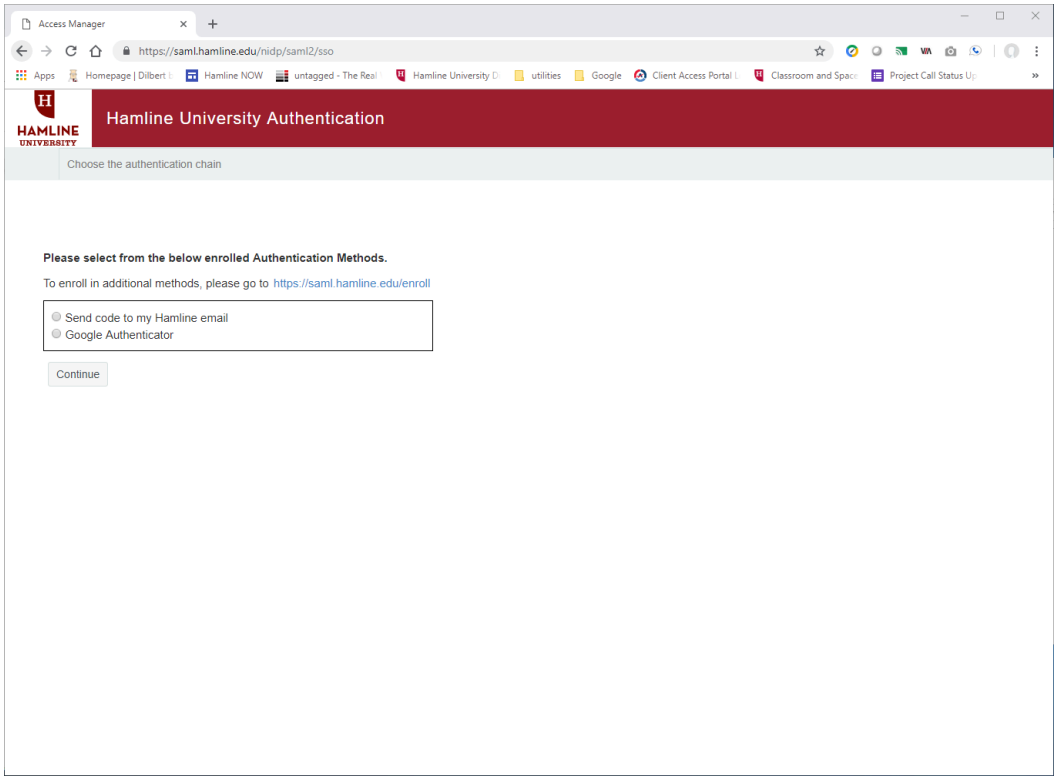
5. To set up additional authenticators, click on Add authenticator under “Add Authenticator”. You can have multiple authenticators tied to your account.

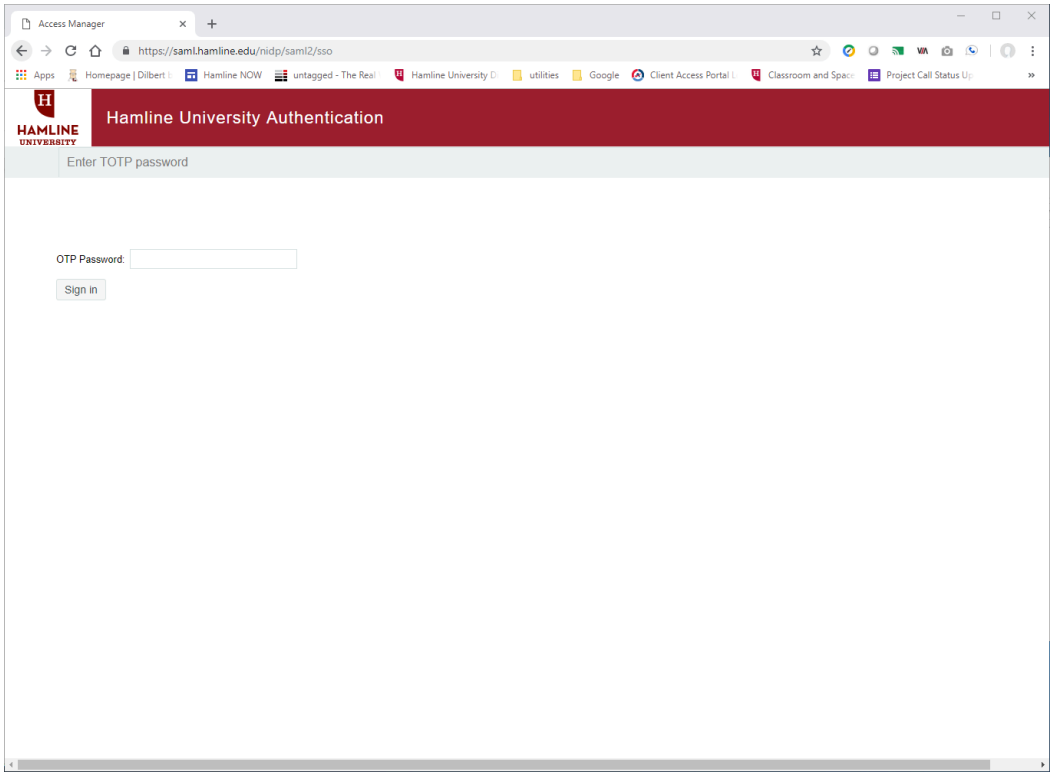
Add Google Authenticator

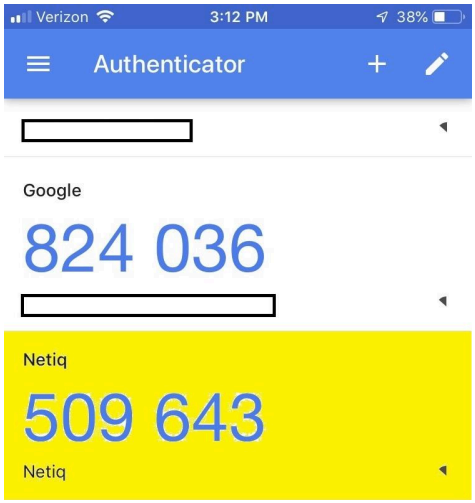
Please note, this uses the Google Authenticator application on your mobile device, but this 2 factor authentication is separate from your Google Apps 2 factor authentication. To add Google Authenticator as a 2nd factor, login to the portal as listed above, and click on “Google Authenticator” under “Add Authenticator”. This should bring you to a screen with a QR code. Take a picture of the QR code with your “Google Authenticator” application on your mobile device



This should add it to your Authenticator App with the application name of “Netiq”. You can then select “Google Authenticator” when logging in, and use the code from the app to login:

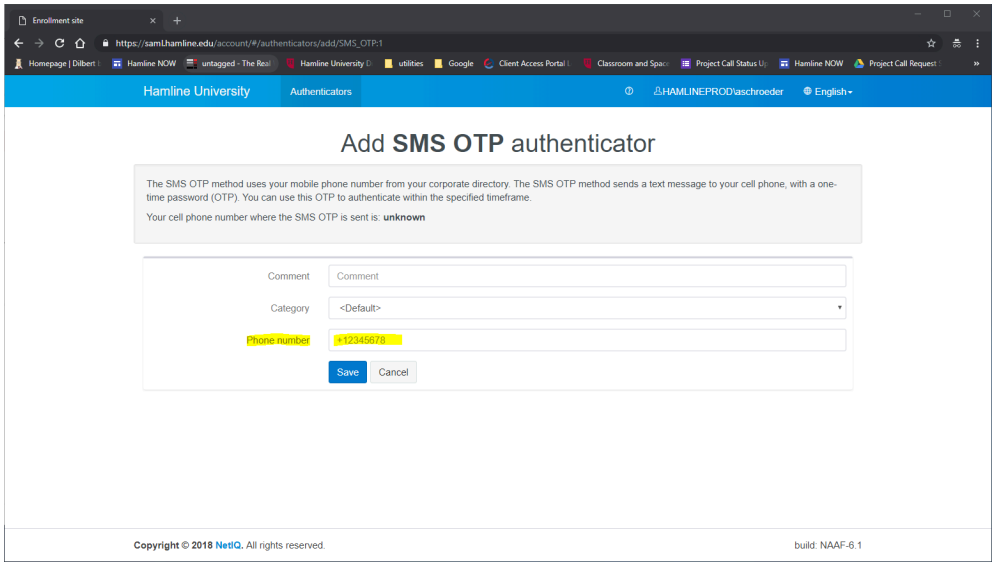






Add SMS

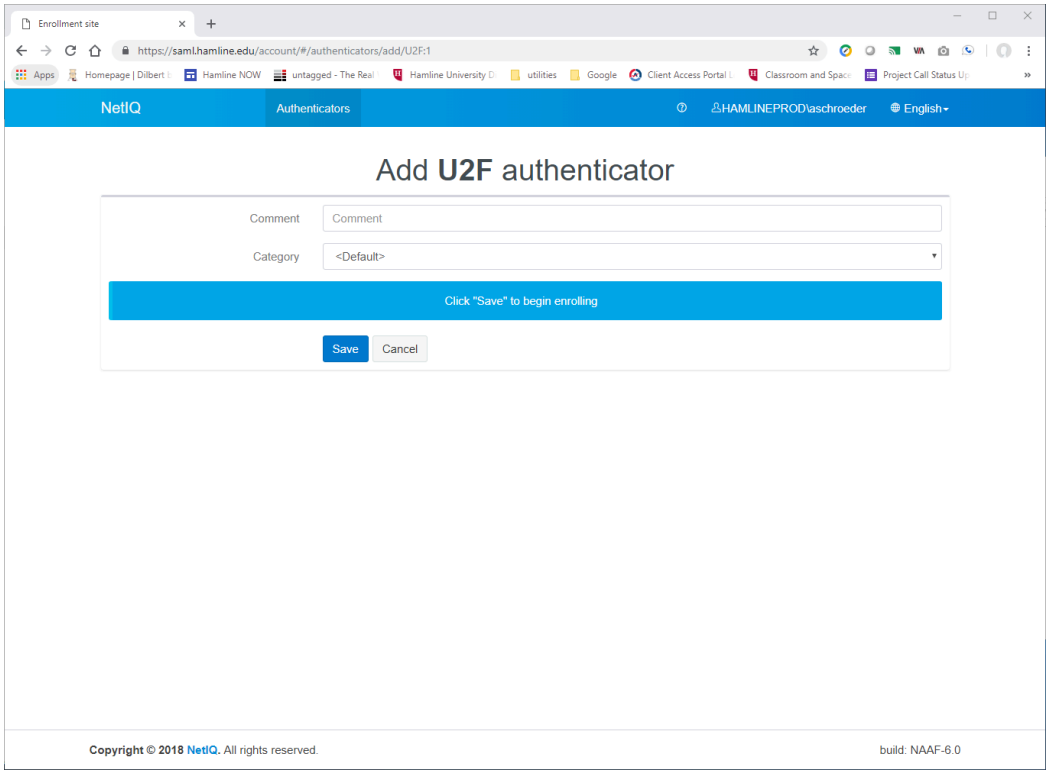
You can set up the service to send your one time passwords (OTP) to you via Text message (SMS) to your cell phone. Click on “SMS OTP” under “Add Authenticator” to bring you to the configuration screen to enter your mobile phone number:



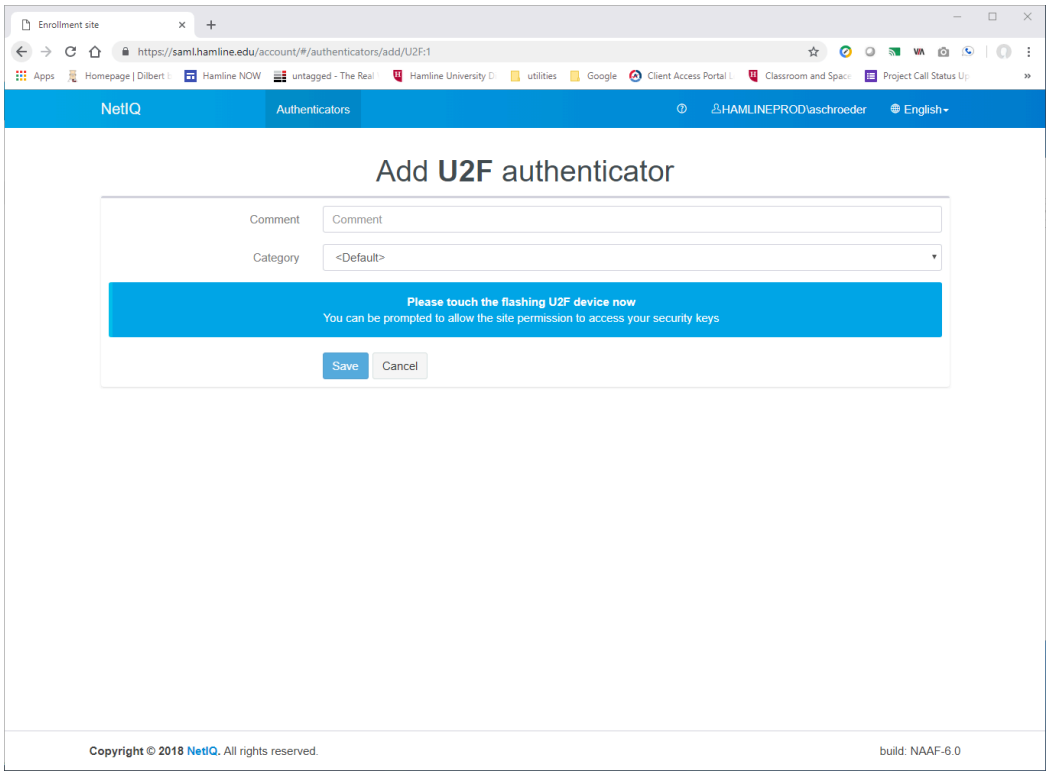
Type in your cell phone number in the box near “Phone Number”. You can also label this number with the “Comment” field, but you can have only one phone number registered for sending you SMS based 2-factor at any one time.

Add USB Key - not currently working

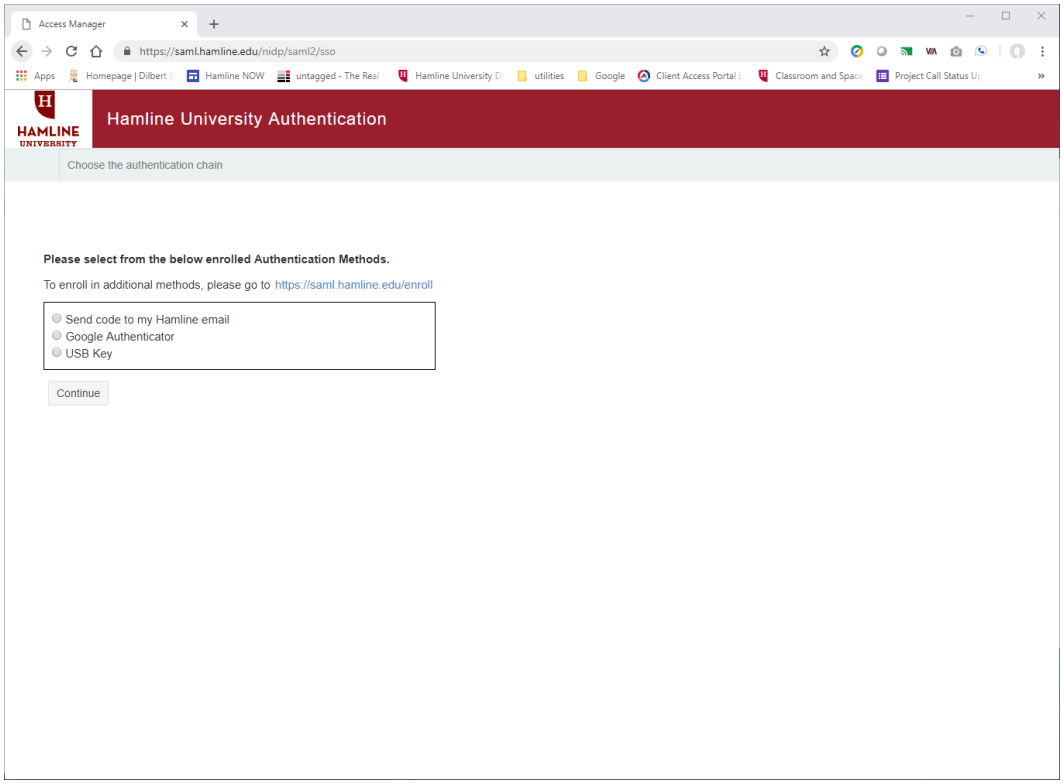
Please note, this uses the USB Key (U2F device), but this 2-factor authentication is separate from your Google Apps 2-factor authentication. To add your USB key as a 2nd factor, login to the portal as listed above, and click on “U2F” under “Add Authenticator”.



Insert your device before clicking on the “Save” button. It should prompt you to press the flashing logo on the device:



Which should add the USB key to your account. The next time you log into workday, it should allow you to select “USB key” as an option for your 2nd factor:


Access Manager
https://saml.hamline.edu/nidp/saml2/sso
Apps
Homepage | Dilbert
Hamline NOW
untagged - The Real
Hamline University D
utilities
Google
Client Access Portal
Classroom and Space
Project Call Status Up
HAMLINE UNIVERSITY
Hamline University Authentication
Choose the authentication chain
Please select from the below enrolled Authentication Methods.
To enroll in additional methods, please go to https://saml.hamline.edu/enroll
Send code to my Hamline email
Google Authenticator
USB Key
Continue