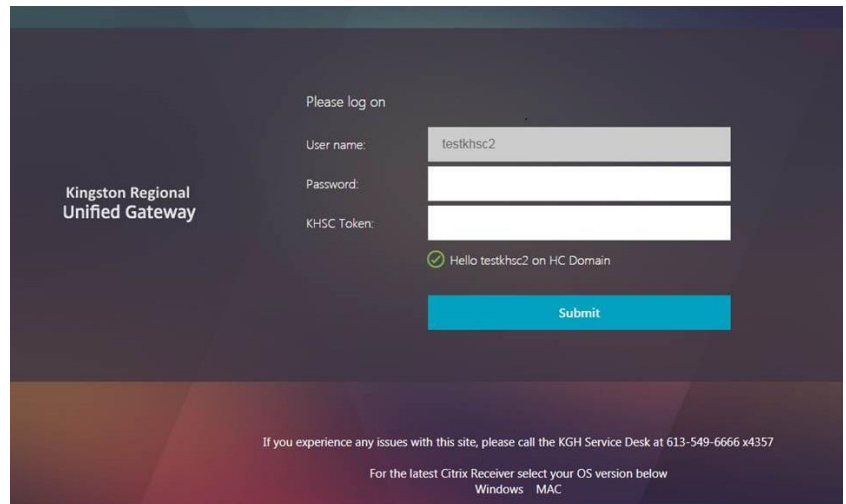


Moving to Multi Factor Authentication (MFA)

Starting on June 29, 2018 MFA will be enforced on all of our public facing services, including: Webmail, KGH Today and Kronos (Self-Serve).

If you are not enrolled by June 29 you will lose remote access to these services on any non-KHSC secured network (see diagram below for breakdown of networks).

The MFA service will be provided in the form of an app on your smartphone (with other options available if required) that gives you a passcode (aka 'a token') to enter. The existing process of logging into Citrix, Webmail, Kronos, etc. will remain the same, the only addition is that the user will open their MFA application and enter the six-digit passcode provided within it into the field labeled 'KHSC Token,' along with their username and password (see example above).



How to Enroll in Multi Factor Authentication

Before MFA is fully implemented across the organization, KHSC is encouraging staff who would like continued access to remote services on non-KHSC secured networks (such as your home, Queen's campus, the KGH-Guest Network, etc.), to enroll in MFA before the scheduled go-live on June 29, 2018.

Enrollment Instructions

Setting up your account to use the MFA tool is quick and simple. The entire process involves downloading an app on your mobile device (e.g. a smartphone or tablet), and proceeding to the MFA enrollment page.

Step 1: On your smartphone or mobile device, search for and open one of the following Apps:

- a. Android users look for the Google Play Store in your list of applications and open it.



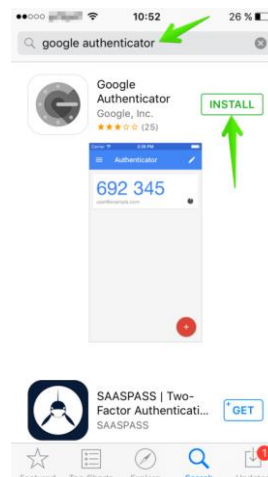
- b. Apple users look for the App Store in your list of applications and open it.



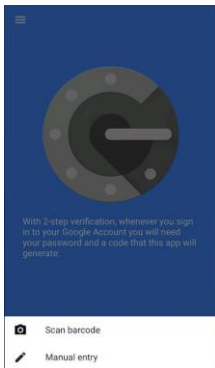
If you do not have a phone with internet access, the ability to download apps or use a BlackBerry and do not have access to the Google Play Store app, please email KHSC.IMIntegration@kingstonhsc.ca or call:

**John Saunders (Manager of IT Services – 613 546 6666 ext. 3721) or
Percy Barr (IT Coordinator – 613 546 6666 ext. 3410) for support.**

Step 2: Once you have opened your respective App, search for Google Authenticator and click install.

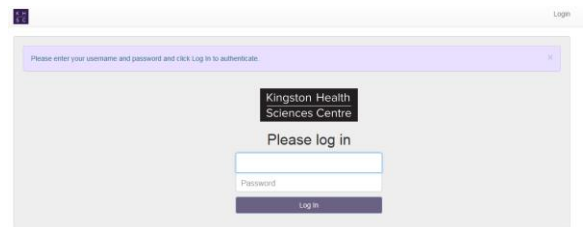


Step 3: Once the download/ installation has completed, you will now have Google Authenticator installed on your device. Look for the following app on your phone to use it:

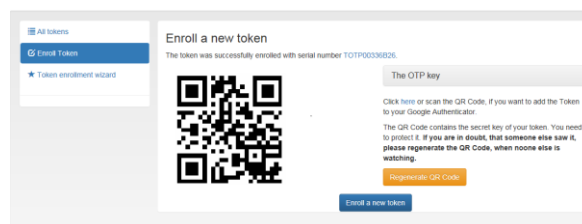


Step 4: Open Google Authenticator and click 'Begin Setup'. Follow the instructions on your device until you are prompted to add an account and select 'Scan a Barcode'.

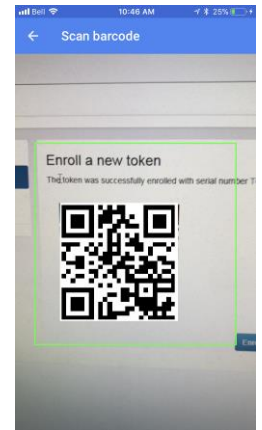
Step 5: On your computer or laptop, log into Citrix and open Internet Explorer or Chrome. Go to <https://otp.kingstonhsc.ca/> (on a KHSC secured network) or <https://enroll.kingstonhsc.ca/logon/LogonPoint/tmindex.html> (on a non-KHSC secured network) and enter your username and password to login (the same credentials you would normally enter to login to your laptop).



Step 6: You will be brought to the 'Enroll a New Token' screen. Click the 'Enroll Token' icon and a Barcode will appear.

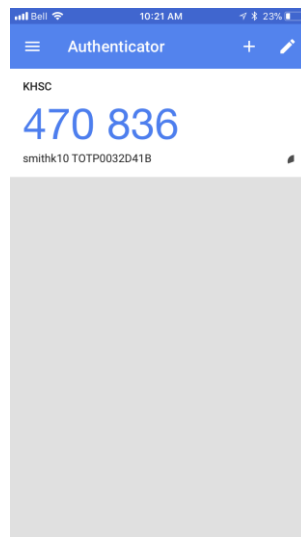


Step 7: Ensure that Google Authenticator is open on your mobile device and select 'Scan a Barcode' if you haven't already. Following the instructions on your device, point your device's camera to scan the barcode on your laptop/ PC. Your device will then add KHSC to the Google Authenticator app.



Congratulations! You are now enrolled in Multi-Factor Authentication (MFA). Starting on June 29, you will be required to use the passcode generated in Google Authenticator to login to Citrix, Webmail, Kronos and KGH Today when on non-KHSC secured networks. Continue onto page four for more details on what the login process will look like.

If you have any questions, please feel free to contact Help Desk at ext. 4357



**Example of a KHSC
Token (Passcode)**

Logging into Citrix with Multi-Factor Authentication (MFA)

Now that you are enrolled in MFA, below is a quick overview of the differences you'll see when logging into KHSC services once MFA has gone live on June 29, 2018.

Old Login Process

Before MFA was implemented, users logged in through the Citrix Receiver (See Figure 1) or directly through the application (e.g. Webmail log-in Screen (See Figure 2) and were granted access to remote services.

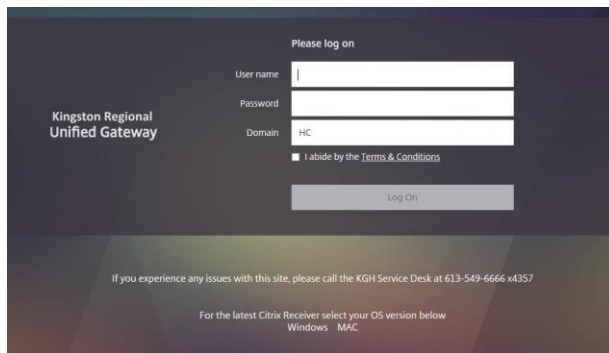


Figure 1. Old User Login Screen

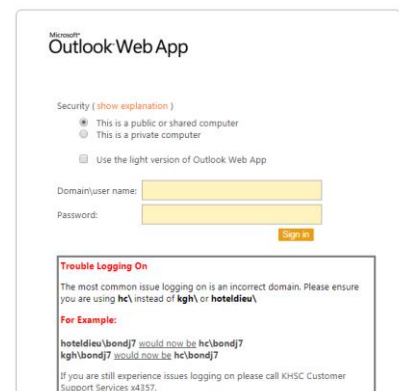


Figure 2. Old Webmail Login Screen

New “Multi-Factor Authentication” Login Process

Now that MFA has been implemented you will see the following screen at login on ALL KHSC services (See Figure 3).

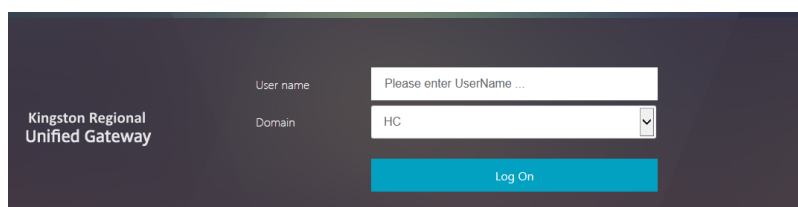


Figure 3. New User Login Screen

Once you have entered your username, you will be sent to the following page if you've enrolled in MFA (See Figure 4). Note: you must be enrolled in MFA to remotely access KHSC services on non-KHSC secured networks. If you have not yet enrolled in MFA, return to page two for instructions on how to do so.

Figure 4. User Credentials Screen when enrolled in MFA.

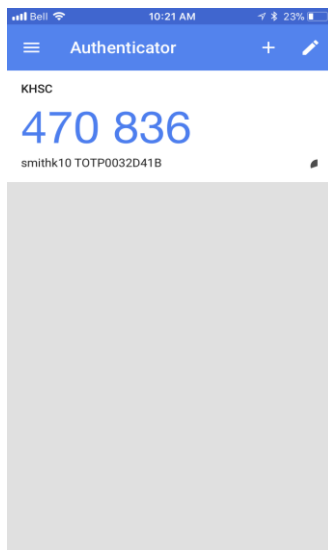


Figure 5. Sample Token (6 Digit Passcode).

In addition to your Password, you'll also need to enter your KHSC Token to log-in. Open your Google Authenticator App or use the hard token you purchased (either a fob or a key card) and enter the 6 digit number that is displayed on your device.

Remember, in order to enhance security, this KHSC Token will change every 30 seconds. If you've entered the token number and are told your credentials are not valid, please try a second time using the most recent KHSC Token number you see on your App (See Figure 5). Hit the submit button and you will have access to the service you are attempting to utilize.