UPDATING USER CREDENTIALS/
MULTI FACTOR AUTHENTICATION
(MFA) GUIDE
## Contents

Updating User Credentials .................................................................................................................. 3

Multi Factor Authentication (MFA) Guide – app .................................................................................. 4

Multi Factor Authentication (MFA) Guide – phone ............................................................................. 11

Questions? ............................................................................................................................................. 19
Updating User Credentials

1. When logging into a GC computer, you will be prompted to change your current password to one that meets the updated credential criteria:

A passphrase is recommended versus a password as they are easier to remember and will allow you to easily fulfill the character length requirement. Updated credential criteria:

- Minimum password length: 15 characters
- No complexity rules
- Maximum password age: 365 days
Multi Factor Authentication (MFA) Guide – app

1. When attempting to access one of the applications that support MFA, you will be prompted to provide your credentials to begin the authentication process:
2. After providing the correct credentials, a screen will display informing you that additional information is needed:
3. After clicking on next in the previous step, you will be asked to install the Microsoft Authenticator app. The screenshot below has been provided for your convenience to access the application and begin your download:
4. You can also select “I want to use a different authenticator app” if you currently have another authentication application you would prefer to use for your work account. After an authenticator application has been installed on your device, click next on the window to continue with the set up:
5. If using Microsoft Authenticator, click on the add account button on the top right of the application indicated by a white plus sign to add your account.

6. Select “Work or school account” when prompted to specify what type of account you are adding to the authenticator. Input the credentials you use to log into your computer and click next to continue with the setup:
7. Using your phone or other device, scan the QR code that is provided to you to pair the device to your account. If you cannot see the QR code or are not able to scan it, click on the “Can’t scan image?” button located under the QR code. This will provide you with a URL and code combination needed to pair your mobile device to your account:
8. Next you will see a “Let’s try it out” window on your computer, click next. A notification will be sent to your mobile device via the Microsoft Authenticator app. Once you receive the notification in the app, press “Approve”. This action confirms that you are attempting to log in.

9. Once the connection is successful, the screen on your computer will show that your notification was approved by displaying a green check mark.
1. When attempting to access one of the applications that support MFA, you will be prompted to provide your credentials to begin the authentication process:
2. After providing the correct credentials, the next screen will indicate that additional information is needed. Click next.
3. You then will be prompted to install the authenticator app or you can select “I want to set up a different method” to skip the app installation process. You will be provided with a drop-down menu listing the phone option. Select phone and click next:
4. Input your phone number and select how you would like to be reached, via text or phone call:
5. If you opt for the text option, a message will be sent to your phone containing a 6-digit code. Input the code in the box and click next:
6. If you opt for the call option, a phone call will be made to your phone. Answer the call and follow the prompts to confirm you are attempting to authenticate:
7. After you verify your phone, a message will appear on your computer with a green check mark confirming that you are registered for MFA. Click next to continue with the set up:

![Keep your account secure](image)

- Phone
  - SMS verified. Your phone was registered successfully.

[Next button]
8. A final message will appear displaying the phone utilized to set up MFA. Click done to continue signing in:
Questions?

If you have any questions regarding the new password policies or the MFA process, please contact the IT Service Desk via the following methods:

- Phone: 409-944-4242
- Email: servicedesk@gc.edu