Multi-Factor Authentication Set-Up

These instructions will walk you through setting up Multi-Factor Authentication (MFA) on your Clark account.

Before You Get Started

Choose Your Factor

You’ll need to decide which factor you’d like to use as additional verification when accessing your account. If possible, we strongly recommend using the Authenticator App, as it provides a higher-level of security.

Authenticator App

If you use the Authenticator app as your factor, you will receive a notification on your phone when accessing your account.

To use the Authenticator App you’ll need continued access to an eligible Apple or Android smartphone with access to the app store and the ability to install an app.

- Apple Users: iOS 11 or more recent on an iPhone
- Android Users: Android 6.0 or greater smartphone

SMS Messaging

If you use SMS as your factor, you will receive a verification code via SMS and submit it in order to access your account. Your verification code will change every time. You should NEVER share your verification code with anyone.

To use SMS Messaging, you’ll need continued access to a cellphone with the ability to receive SMS text messages.

If you cannot use either of these options as a factor, please contact the Help Desk (508 793 7745 or helpdesk@clarku.edu).

Once you have a primary factor set up, you can add additional factors as a back-up. Visit our MFA webpage for more information on how to update your factors.

Location

If you are a staff or faculty member, you should be off-campus and logged out of the VPN.

Opt-In

If you’re an early-bird and opting into MFA before it is required – thank you!

Read the complete instructions to ensure that you’re ready to set-up MFA, and then click here to Opt-In. Once complete, wait about 20 minutes before continuing with the set-up.
These instructions will walk you through setting up MFA on your Clark account using the Microsoft Authenticator App. If using SMS Messaging, please proceed to the next section of the instructions.

**Step 1: Download the Authenticator (on your Smartphone)**

1. Download the Microsoft Authenticator to your smartphone.
   - iPhone: [https://apps.apple.com/us/app/microsoft-authenticator/id983156458](https://apps.apple.com/us/app/microsoft-authenticator/id983156458)
   - Be sure to look for this or a similar icon, and check that it’s published by Microsoft.

2. On your computer, navigate to [https://outlook.com/clarku.edu](https://outlook.com/clarku.edu) to start the enrollment process.
3. Log in with your Clark University username and password.
4. You will be presented with the following screen. Click **Next** to start the enrollment process.
5. Select **Mobile App (or Microsoft Authenticator)** from the drop-down menu as your authentication method.

![Additional security verification](image)

**Do not choose Authentication Phone if you want to use the Authenticator app.** Authentication Phone means you are choosing SMS Messaging as your factor.

6. Choose **Receive Notifications for Verification**.

![Additional security verification](image)

7. Click **Set up**

8. You will then be presented with a QR code, similar to the one below. Keep the QR code on your screen while you go to the next stop on your smartphone.

![Microsoft Authenticator](image)

If you don’t receive a QR Code, you may have chosen to be contacted by Authentication Phone. This will set you up with SMS Message authentication.

We recommend jumping to the SMS Message section of these instructions and completing the set-up. Once finished, you can add additional factors as a back-up. **Visit our MFA webpage** for more information on how to update your factors.
**Step 3: Complete the Process (on your Smartphone)**

9. Open the Microsoft Authenticator App on your smartphone
10. If prompted, select **Allow** when asked to allow notifications from the app
11. Select **Scan QR Code**
12. If prompted, select **Allow** when asked to grant permission to your device’s camera
13. Follow the directions by pointing your device towards the QR code on your computer screen. Your phone has now been added as a way to authenticate your account

   If you clicked on something in error, got lost, or your app is a little different, don’t worry, you can still enroll.

   Click on the “hamburger” button (three vertical lines or dots) or the “+” button at the top of the app. Choose **Add Account**. Choose **Work or School Account** if asked What kind of account are you adding? You will then be prompted to scan the QR code.

**Step 4: Test the Process (on your Computer & on your Smartphone)**

14. On your computer, click **Next** on the QR screen.
15. Click **Next** on the Additional Security Verification screen.
16. You will see the following screen on your Computer, and a prompt will be sent to your Smartphone.

   ![Microsoft Authenticator](image)

   17. Click **Approve** on your Smartphone
   18. You will see the following screen on your Computer. Click **Next**.

   ![Microsoft Authenticator](image)

   19. If you are using a computer that is not shared with other users, you can select **Yes** when prompted to **Stay Signed In**. This will ensure you will not have to perform multi-factor authentication the next time you need to access Office 365, unless you log out, or are logging in from a different computer.
SMS Message Instructions

These instructions will walk you through setting up MFA on your Clark account using SMS Messages as a second factor.

Step 1: Start the Process (on your Computer)

1. On your computer, navigate to https://outlook.com/clarku.edu to start the enrollment process.
2. Log in with your Clark University username and password.
3. You will be presented with the following screen. Click Next to start the enrollment process.

4. Select **Authentication Phone** from the drop-down menu as your authentication method.

5. Choose **United States (+1)** (or your correct country code) from the drop-down menu.
6. Enter your cellphone number
7. Choose **Send me a code by text message**
8. Click **Next**
9. You will then be presented with the following window. Keep this window on your screen while you go to the next stop on your cellphone.

![Additional security verification](image)

**Step 3: Complete the Process (on your Computer & Cellphone)**

10. You will receive an SMS message to your cellphone that will look similar to the image below. Remember to NEVER share your verification code with anyone.

    ![Use verification code](image)

11. Enter the verification code received in the SMS message to the Additional Security Verification window on your computer.
12. Click **Verify**
13. Once verified you may be prompted to also set up the Authenticator app. This is optional and you can choose to Cancel.
14. If you are a computer that is not shared with other users, you can select **Yes** when prompted to **Stay Signed In**. This will ensure you will not have to perform multi-factor authentication the next time you need to access Office 365, unless you log out, or are logging in from a different computer.