Information Technology Services

Multi-Factor Authentication (MFA)

Quick Start Guide

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) combines two or more independent credentials in order to gain access to a system.

MFA is a multi-step account login process that requires users to enter more information than just a password. Your password is one "factor" for authentication. Implementing MFA means you will need another "factor" to successfully authenticate and gain access to the system.

To gain access to the RF systems, **OneLogin Protect** will be used as a second "factor" to meet the MFA requirement. **OneLogin Protect** is a mobile-based app for both Apple and Android phones. It will provide you with a randomly generated 6-digit OTP (one-time password) to use as a second password. ***This Quick Start Guide will provide step by step instructions on how to set up OneLogin Protect and how to use it to gain access to RF systems***.

Why is MFA needed?

Applications are more secure with MFA as an additional security control. MFA creates a multilayered approach thereby making it difficult for any unauthorized person to gain access to a system, computing device, network or database. If one factor is compromised, such as a password, the unauthorized person will still need another factor such as a security token to gain access.

To set up MFA:

1. In the SUNYRF SSO login window enter your username. After entering your username credential click the **Continue** button to proceed.

Note: Checking the **remember my username** checkbox will enable the system to remember you for future logins.

2. The next window will prompt you to enter your current password. Enter your password then select **Continue**.

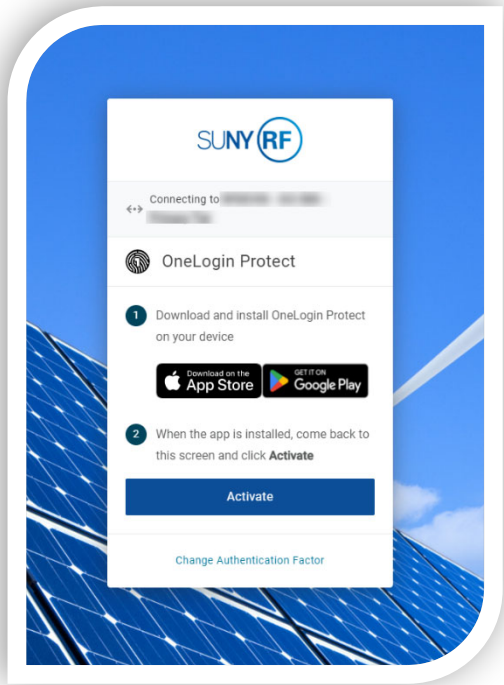
Note: If either the username or password supplied is incorrect, after selecting continue as noted above the system will display a red banner stating **Invalid username or password**. If needed, utilize the **forgot password** link to create a new password. If you need your username, please reach out to customerservices@rfsuny.org.

3 After suppling your credentials, you will then be prompted to begin the setup of Multi-Factor Authentication (MFA). Click on **Begin Setup** to proceed.

4 On the next screen you will be prompted to **Select Authentication Factor.** For this, select **OneLogin Protect**.

5 **OneLogin Protect** is a mobile based application used for MFA. From your smartphone device go to the App Store to download and install the OneLogin Protect application.

Note: When searching within the App Store enter **OneLogin Protect.** The application is free of charge to download onto your mobile device.



6 Once the **OneLogin Protect** App has completed installation on your mobile device, open it, return to your PC, and select the **Activate** button. On the page that follows a QR code will display.

7 At the same time, with the **OneLogin Protect** app open on your mobile device, select the **+** icon.

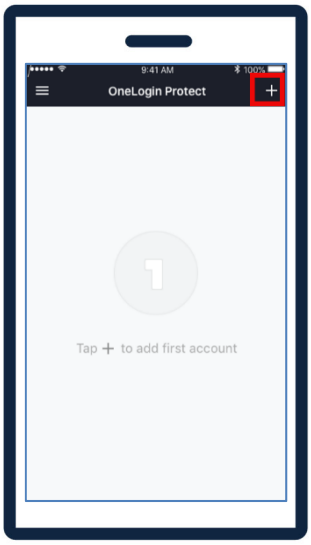
(A) For an Apple device locate the **+** in the upper right-hand side of the screen.

(B) For an Android device locate the **+** in the lower right-hand of the screen.

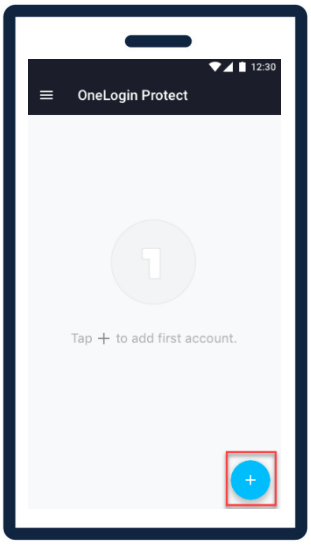
This will activate your mobile devices camera to scan the QR code on the PC screen. Align the blue box with the QR code, when successful scanned the box will turn green indicating a successful pairing.

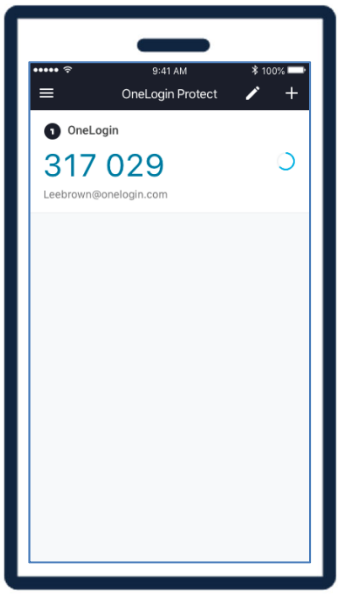
Note: You may be prompted to permit **OneLogin Protect** access to use your device's camera, click **OK**.

(A)



(B)





8

On your mobile device the **OneLogin Protect** home screen appears with the account you configured. You will now be prompted at your future logins to supply the one-time password (OTP) consisting of 6 random numerical digits. These numbers appear to have a space between them. The OTP you need to enter is only the 6 numbers (no spaces).

Note: Your OTP will frequently update to a new OTP for use during application authentication. As such, you will need to keep the **OneLogin Protect** application installed on your mobile device to reference for any future logins.