Information Technology Services

MFA Rollout: Monday April 24, 2023

Implementation by Business Application and FAQs

Implementation by Business Application

The following instructions are designed to assist you with implementing Multi-Factor Authentication (MFA) for each of the business applications listed below.

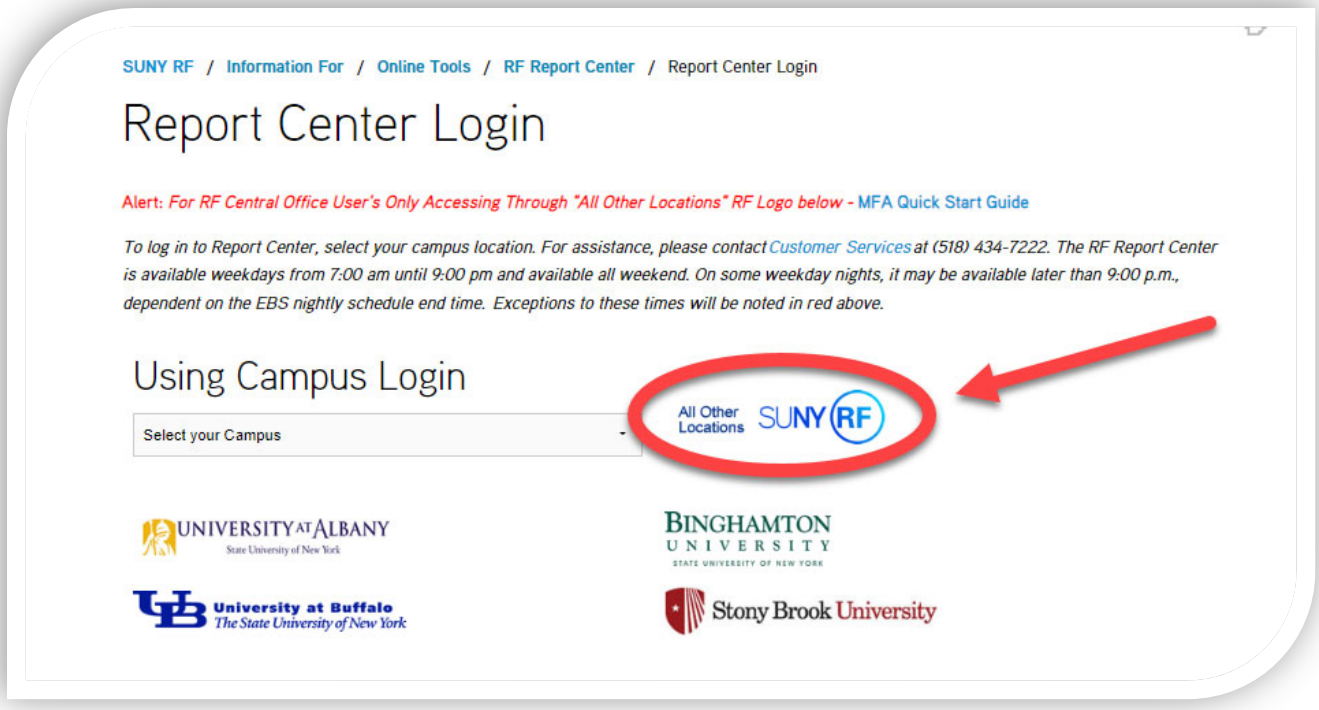
Oracle Business Applications and Self Service

******* ALL ACCESS WILL NOW REQUIRE MFA VIA ONELOGIN PROTECT *******

Please Note: this does **NOT** apply to SUNY Poly/NYCREATES who already use MFA

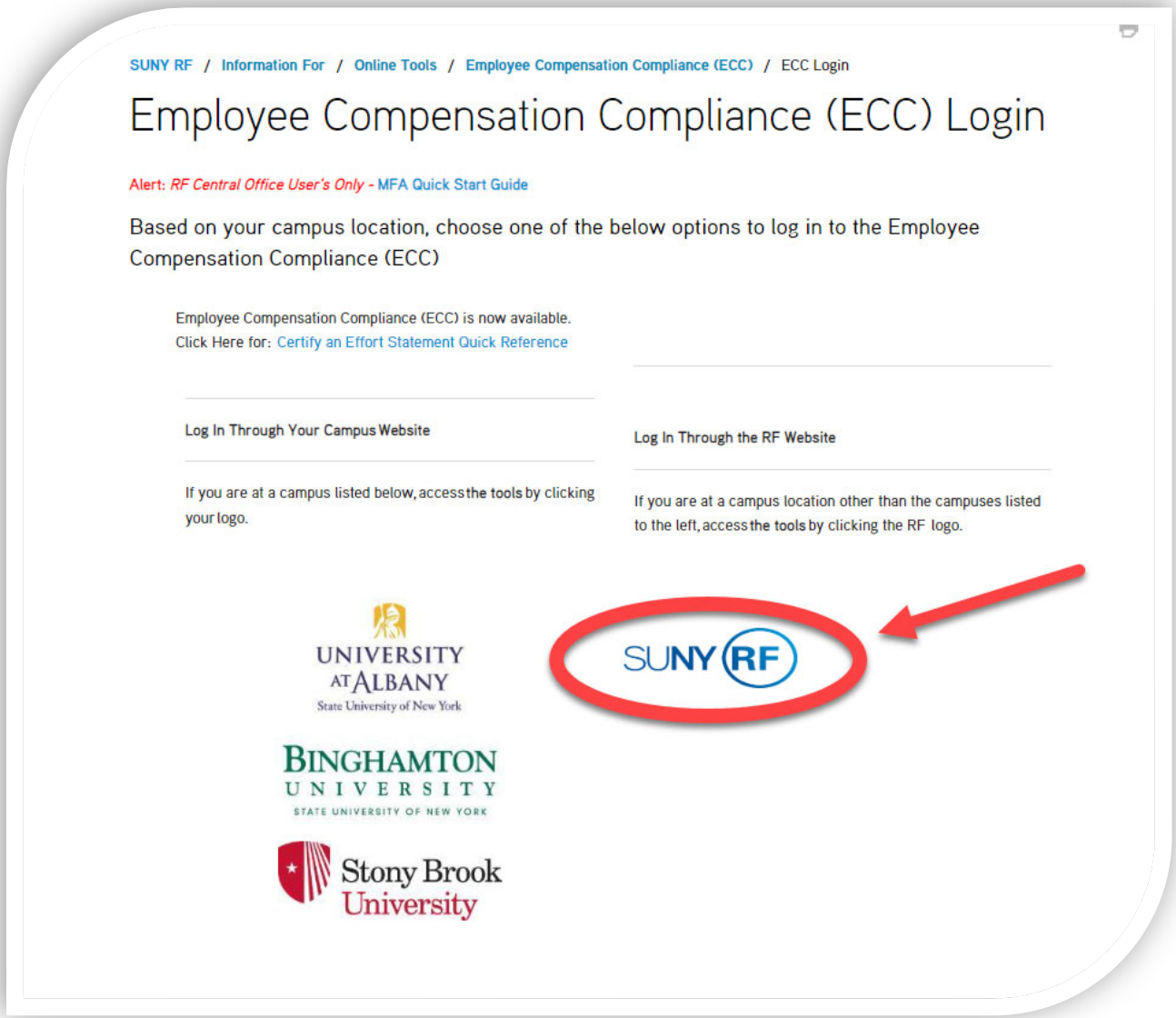
RF Report Center

ONLY affecting users who use the "All Other Locations SUNYRF" link on the Report Center login page:



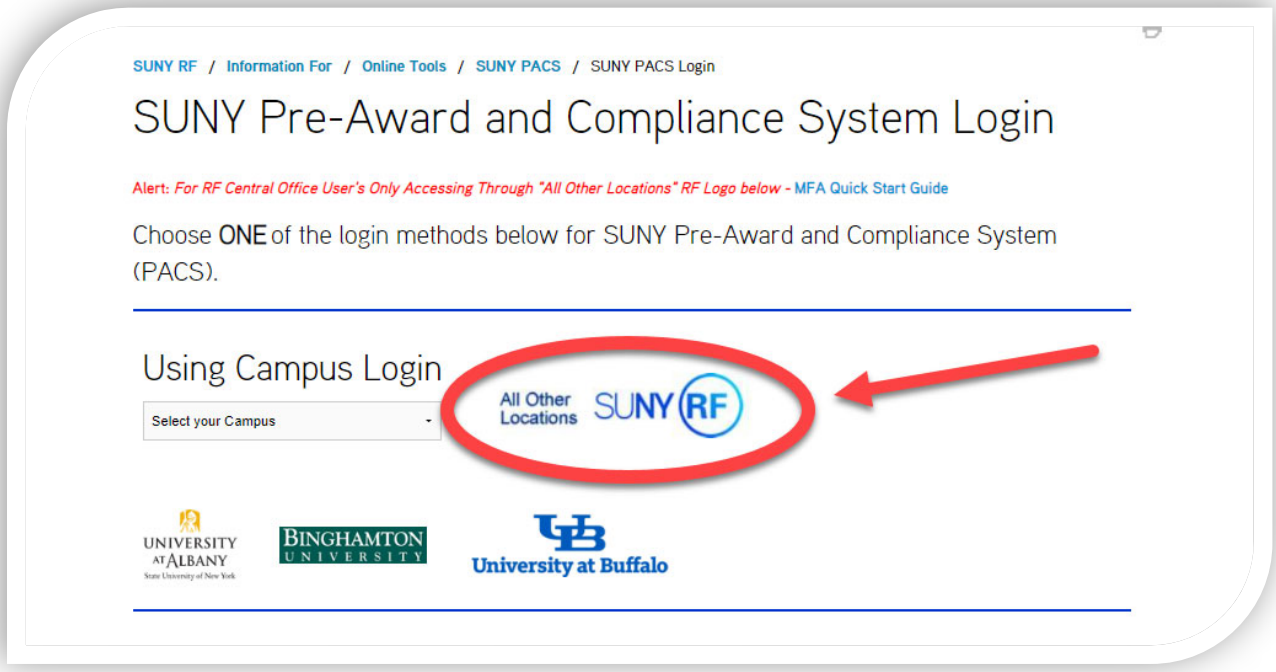
Employee Compensation Compliance (ECC)

ONLY affecting users who use the "SUNYRF" link on the ECC login page:



SUNY Pre-Award and Compliance System (PACS)

ONLY affecting users who use the “All Other Locations SUNYRF” link on the PACS login page:



Frequently Asked Questions (FAQs)

What is Multi-Factor Authentication (MFA)?

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

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.

Who is impacted by MFA?

MFA will be required for all faculty, staff, and students who access the applications below using the links described in this document. Please share this information with your campus users as deemed necessary.

- EBS
- Self Service
- Report Center (RC)
- Employee Compensation Compliance (ECC)
- Pre-Award and Compliance System (PACS)

What applications/systems are currently protected with MFA?

- EBS
- Self Service
- Report Center (RC)
- Employee Compensation Compliance (ECC)
- Pre-Award and Compliance System (PACS)

When does the MFA requirement take effect?

Monday, April 24th at 6am.

How can I prepare for this change?

The only step that can be performed before this requirement takes effect at 6am on Monday, April 24, 2023, is to install the OneLogin Protect application on your mobile device. Please see the ***MFA Quick Start Guide*** posted on your application's login page for details.

How do I set up MFA on my phone?

Follow the steps highlighted in the ***MFA Quick Start Guide*** posted on your application's login page.

What if I don't want to use my personal device or do not own a smart phone?

Users who are unable to install the MFA App on their personal mobile device must contact Customer Services at customerservices@rfsuny.org or (518) 434-7222 for assistance.

What if I forget my mobile device at home?

Please contact RF Customer Services at customerservices@rfsuny.org or 518.434.7222 for assistance.

How often do I have to re-authenticate?

RF systems have varying amounts of timeout periods. Please be prepared to re-authenticate if your MFA access is inactivated after a period of time. You will need to re-authenticate on each device and each browser you use.

What if I experience issues with MFA?

You can contact Customer Services at customerservices@rfsuny.org or (518) 434-7222, or review the ***MFA Quick Start Guide*** posted on your application's login page.

Moreover, RF ITS will have a zoom meeting open for MFA assistance on April 24, 2023, from 7am to 10am and 1pm to 3pm at the following location: MFA Assistance.

Does screen lock need to be enabled on my device prior to installing the application?

Yes, similar to why it is a requirement to have passwords and timed lockouts on desktops/laptops, screen lock is required for security measures.

This is addressed in the NIST Cybersecurity Framework (CSF) generally in PR.AC-7 which refers more specifically to NIST 800-53 AC-11 (Device Lock):

> *Control:*
> *a. Prevent further access to a system by:*
> - *initiating a device lock after a defined time period of inactivity;*
> - *requiring the user to initiate a device lock before leaving the system unattended; and*
>
> *b. Retain the device lock until the user re-establishes access using established identification and authentication procedures.*