NAVAL NUCLEAR LABORATORY

Fluor Marine Propulsion, LLC

Oracle Fusion Cloud Multi-Factor Authentication Instructions for Suppliers

Table of Contents

Introduction

The purpose of these instructions is to describe how to establish Multi-Factor Authentication (MFA) for Oracle Cloud Infrastructure (OCI) IAM Domain. These instructions apply to non-organizational users accessing NNL Oracle Fusion Cloud (OFC) applications. Specifically, for users accessing OFC via the Supplier Portal.

Please note the screenshots in the following slides may change. This guidance will be updated as appropriate.

Technology Overview

Users requiring access to OFC are required to establish Multi-Factor Authentication (MFA) for their identities. Non-organizational users (i.e., Suppliers) establish MFA in the OCI IAM Domain.

Option 1: Authenticator App

Users will have an account in the OCI IAM Domain for which they may establish MFA using an authenticator app such as Microsoft Authenticator or Google Authenticator.

Microsoft Authenticator App

Google Authenticator App

Option 2: Fast Identity Online (FIDO) 2 Security Key

FIDO2 security keys are based on an open standard that provides added security and simplifies MFA. The one that is approved for use must be FIPS 140-2 certified and is available for purchase from Yubico at this site. It is a USB-based device that supports FIDO standard and is compliant with OFC.

Password Requirements

Prior to activating your account, you will need to think of a password that meets the following:

1. No less than 15 characters
2. No more than 40 characters
3. Must contain at least 1 upper case character
4. Must contain at least 1 lower case character
5. Must contain at least 1 numeric character
6. Must contain at least 1 special character
7. Cannot contain more than 2 repeat character (e.g.,111)
   - In other words, cannot repeat the same character more than 2 times (e.g., Me**ll**0wYe**ll**0w1**2**1**22**4)
8. Cannot contain username
9. Cannot contain first name
10. Cannot contain last name
11. Cannot repeat any of the last 24 passwords
12. Cannot contain whitespaces

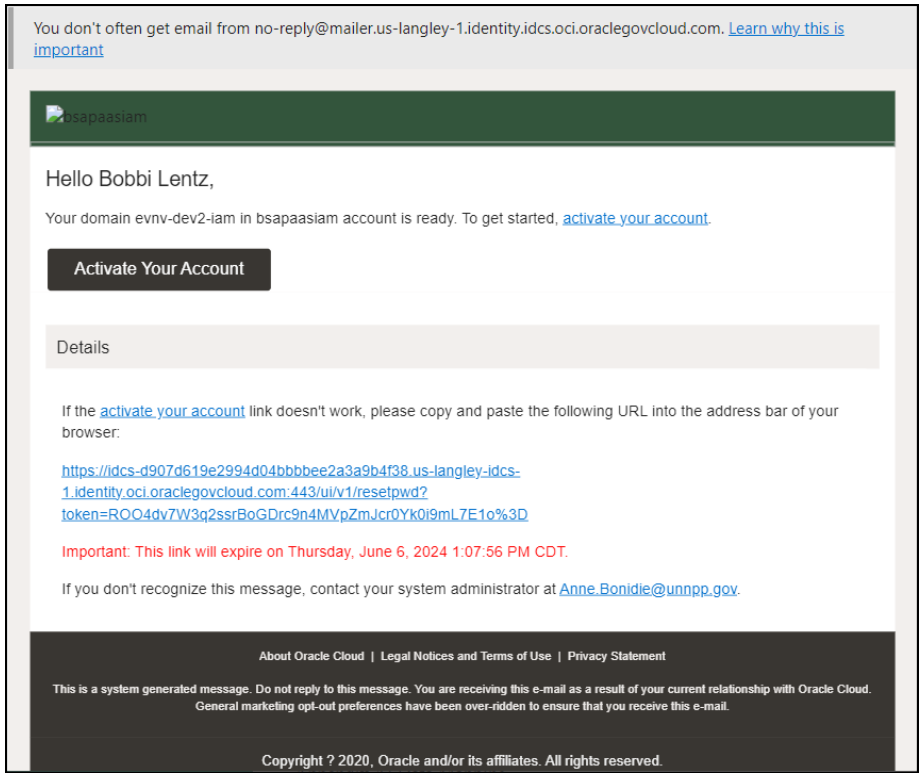
Once you think of a password to use, go ahead and follow the instructions to activate your account.

Activate Account

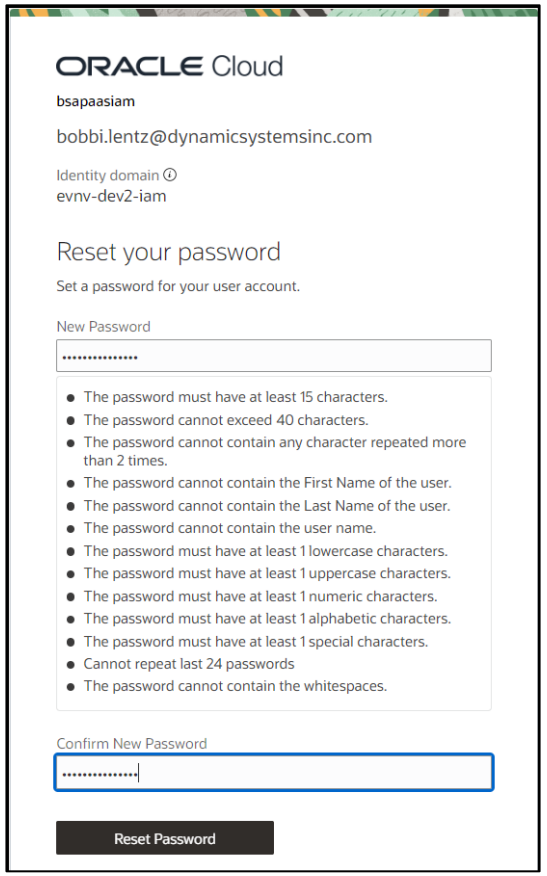
Activate Account

1. When the IAM Domain Administrator creates the user account in OCI IAM Domain, the user receives an automated email from the domain. The sender is no-reply@mailer.us-langley-1.identity.idcs.oci.oraclegovcloud.com.

2. Click on **Activate Your Account**.

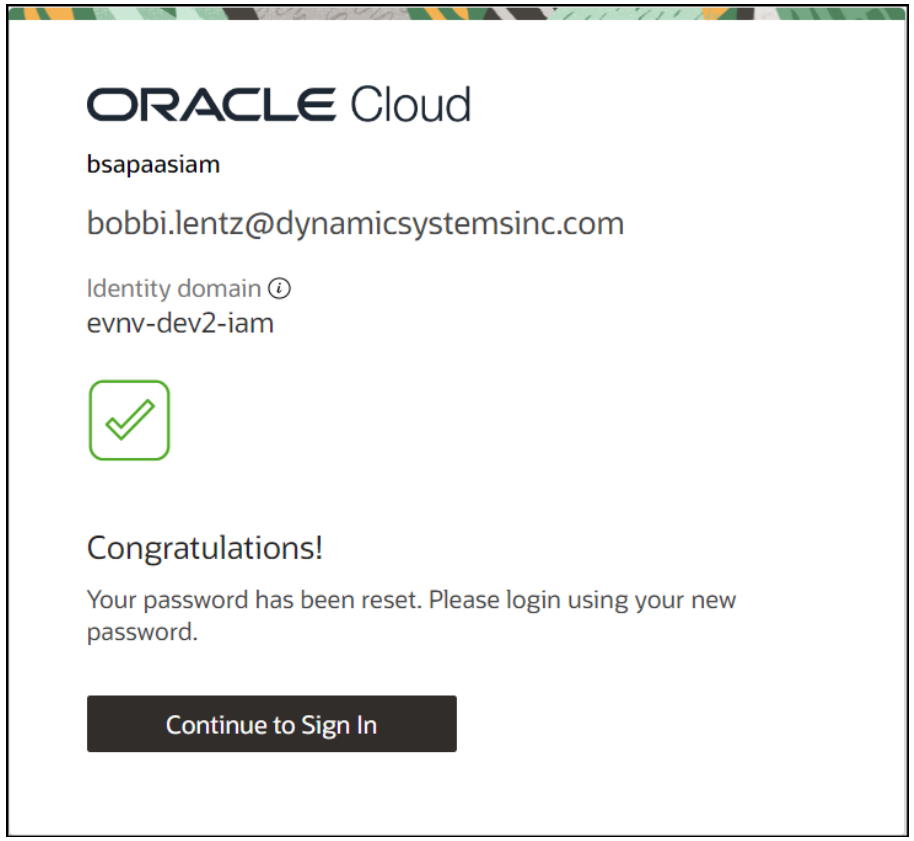


3. The user is redirected to *Reset your password* site. Enter a **password** and **confirm password**. As the user enters a password, the password requirements will display. Click **Reset Password.**

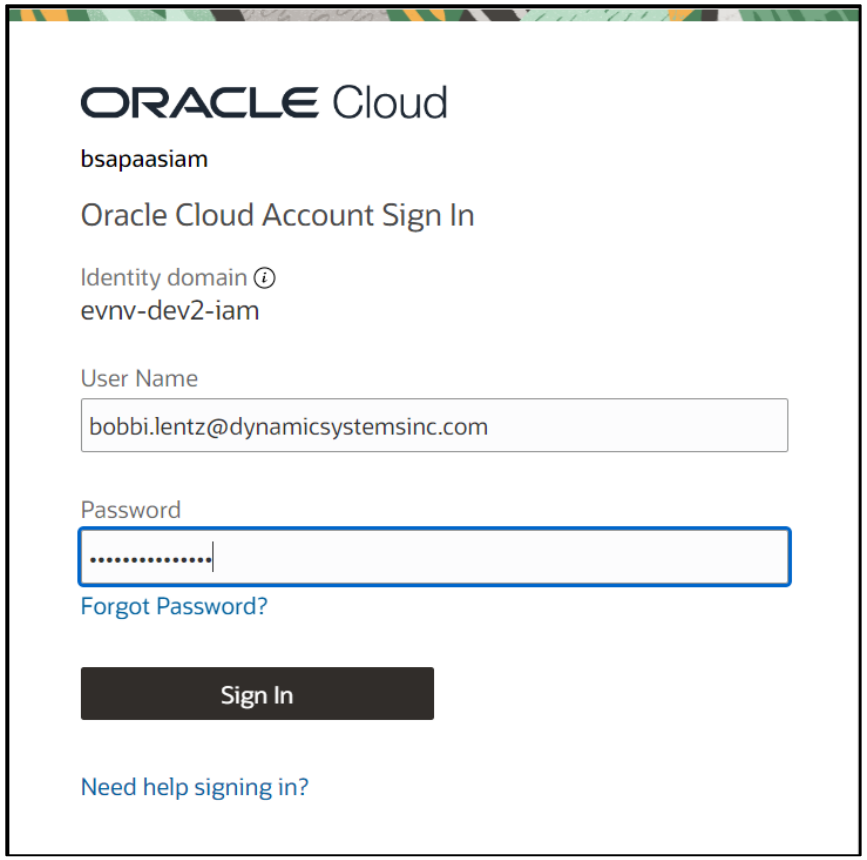


Activate Account (cont.)

4. When a **New Password** and **Confirm New Password** are entered that meet requirements, the success window is displayed.
5. Click **Continue to Sign In**.

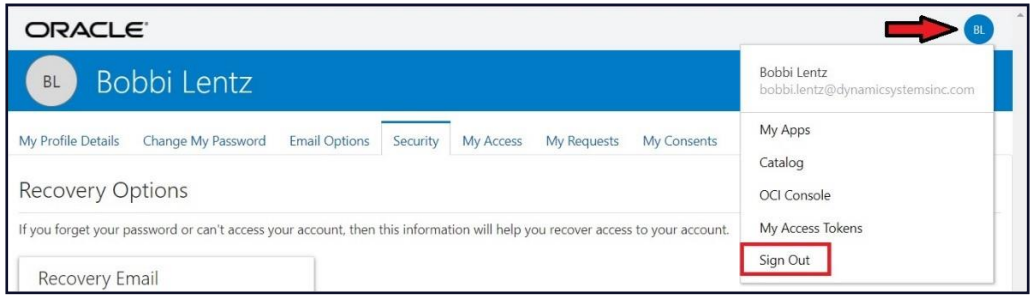


6. The login window is displayed. The user enters their **User Name** and **Password**.
7. Click **Sign In**.

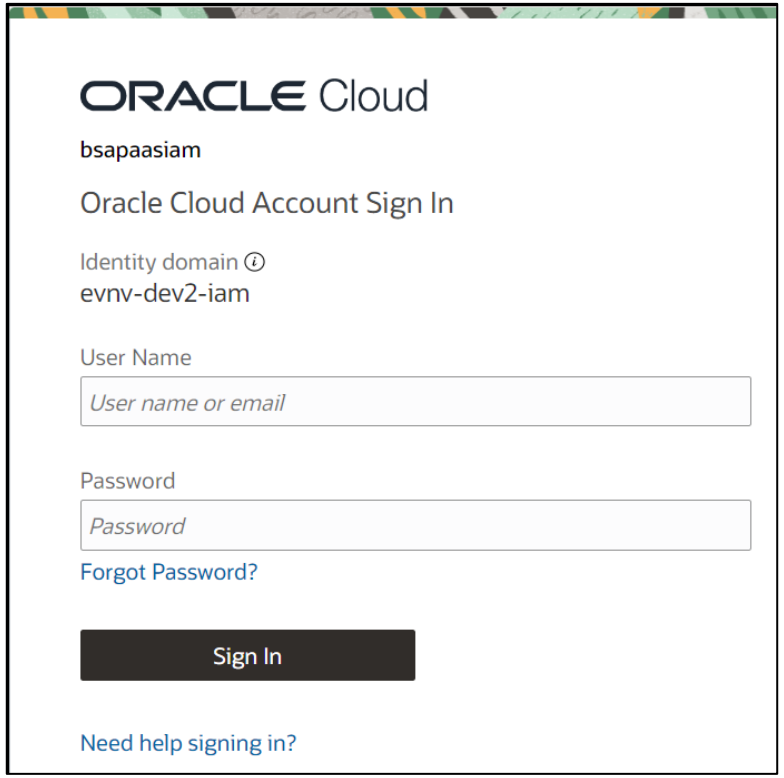


Activate Account (cont.)

8. The user's profile page is displayed. At top right, click the circle containing your initials, select **Sign Out** from the dropdown.



9. You are returned to the login page for the identity domain.



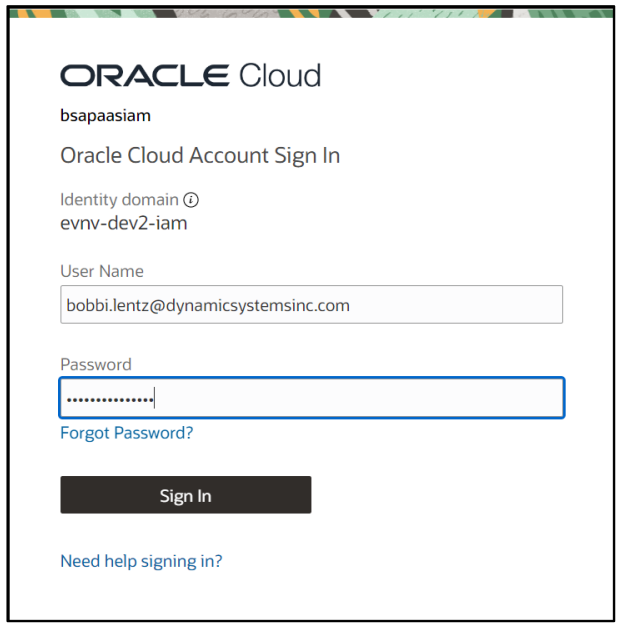
Activate Account (cont.)

- You have activated your account. Go back to your browser and make sure any tabs that are opened with the OCI sign-in screen have been closed.
- Continue to next step.
  - Users opting to establish MFA using an authenticator app, proceed to **OCI IAM Domain – Authenticator App** instructions.
  - Users who are required to or opting to establish MFA using a FIDO security key, proceed to **OCI IAM Domain – FIDO2 Security Key** instructions.

OCI IAM Domain – Authenticator App

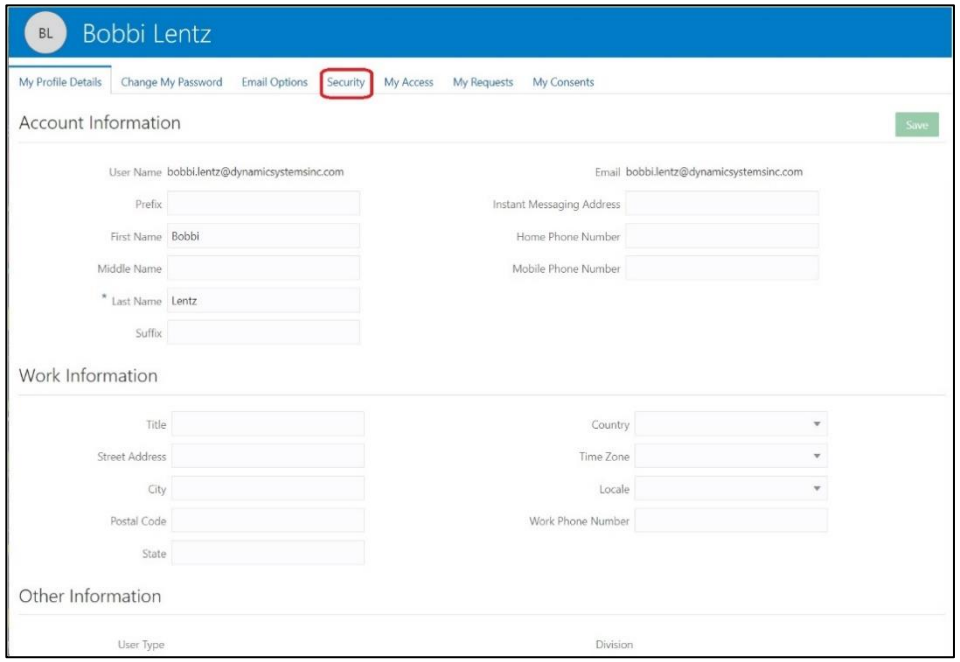
OCI IAM Domain – Authenticator App

1. At the login window, enter your **User Name** and **Password**. Click **Sign In**.



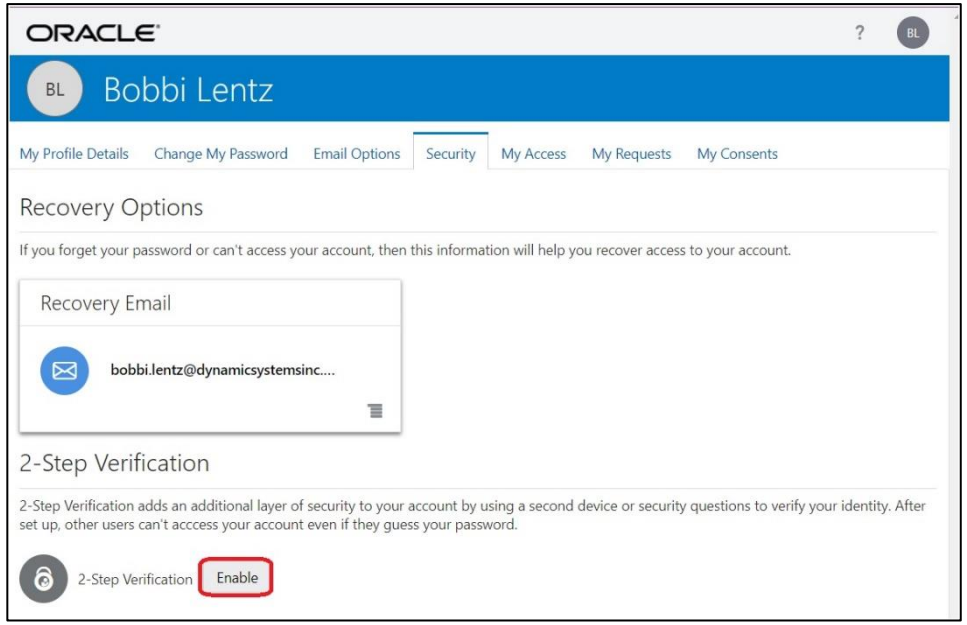
2. The user should be prompted to enable 2-Step Verification.

3. The user's profile page is displayed. Click **Security** on the top menu.



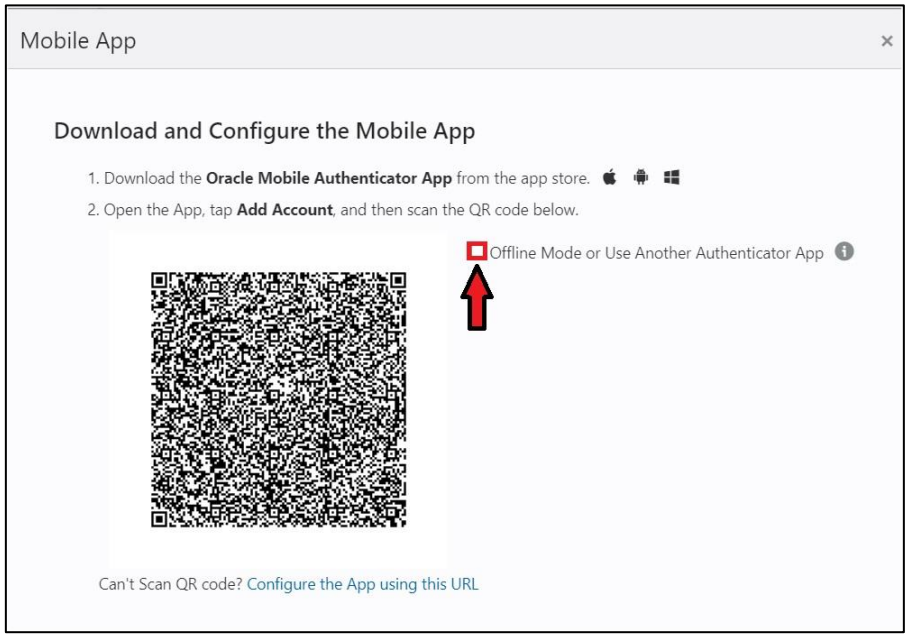
OCI IAM Domain – Authenticator App (cont.)

4. On the *Security* page, under *2-Step Verification*, click **Enable**.



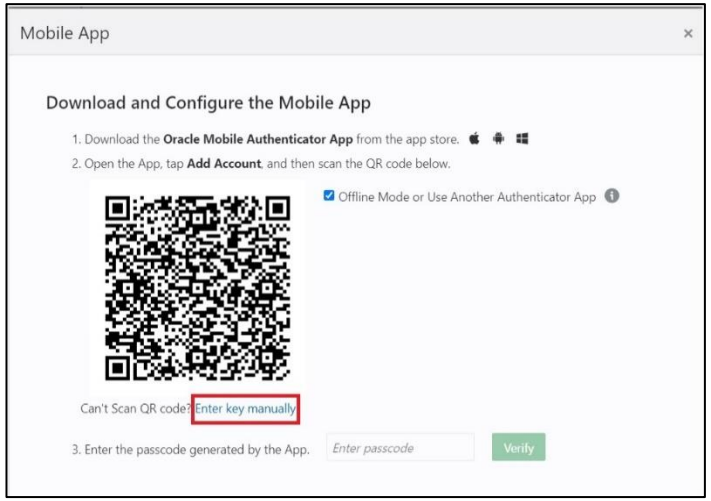
5. On the *2-Step Verification* pop-up, click **Mobile App**.

6. On the *Mobile App* pop-up, click the checkbox next to **Offline Mode or Use Another Authenticator App**.

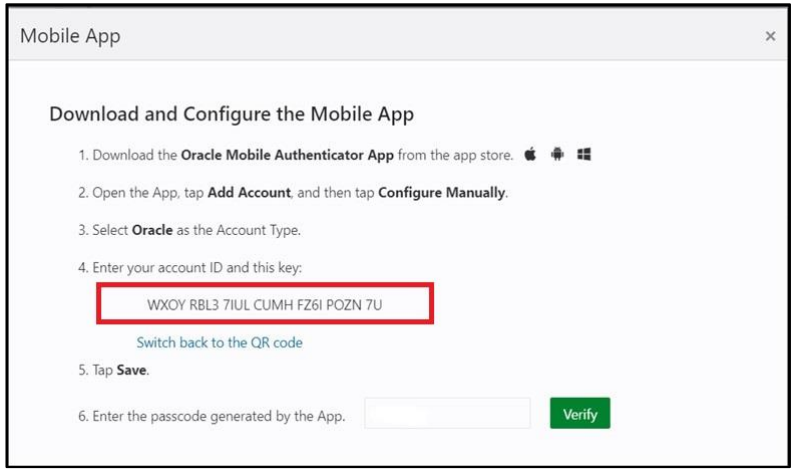


OCI IAM Domain – Authenticator App (cont.)

7. Click **Enter key manually**.



8. On the *Mobile App* page, find the key located in Step 4.

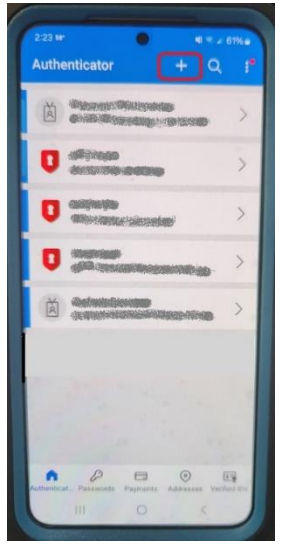


9. On your phone, open one of the authenticator apps.

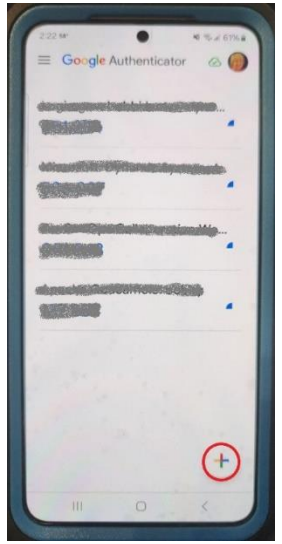
Microsoft Authenticator App

Google Authenticator App

10. Click the plus sign to **Add Account**.



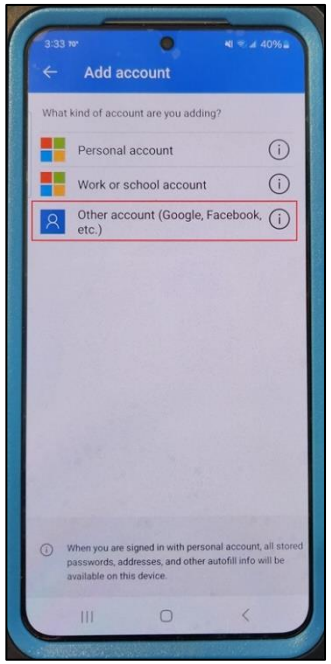
Microsoft Authenticator App



Google Authenticator App

OCI IAM Domain – Authenticator App (cont.)

11. Microsoft Authenticator App only - select **Other account (Google, Facebook, etc.)**



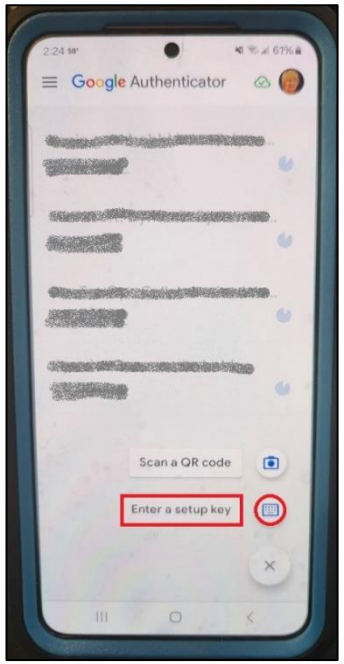
Microsoft Authenticator App

12. On next screen, at bottom of screen, touch the following depending on the app you're using:

ENTER CODE MANUALLY

Microsoft Authenticator App

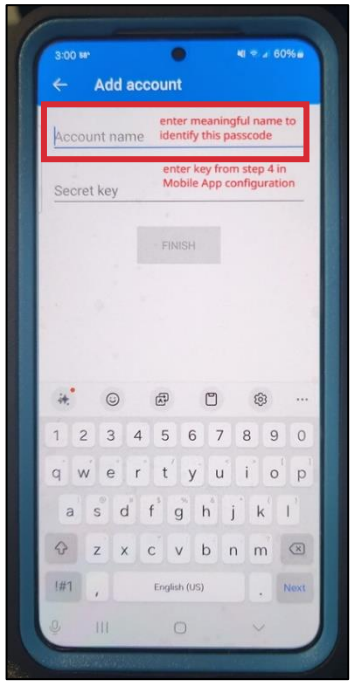
Enter a setup key



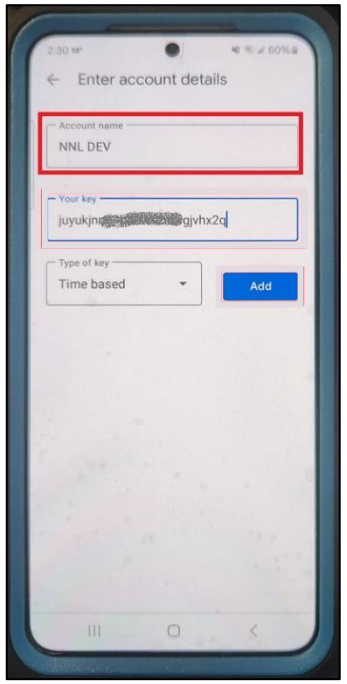
Google Authenticator App

OCI IAM Domain – Authenticator App (cont.)

13. On the next screen, in **Account name**, enter a meaningful name to identify the account (i.e., NNL OFC).



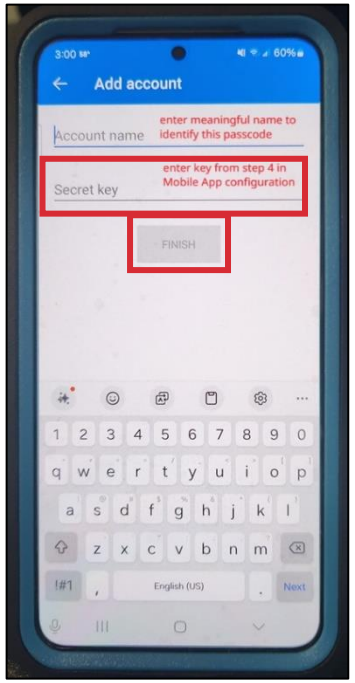
Microsoft Authenticator App



Google Authenticator App

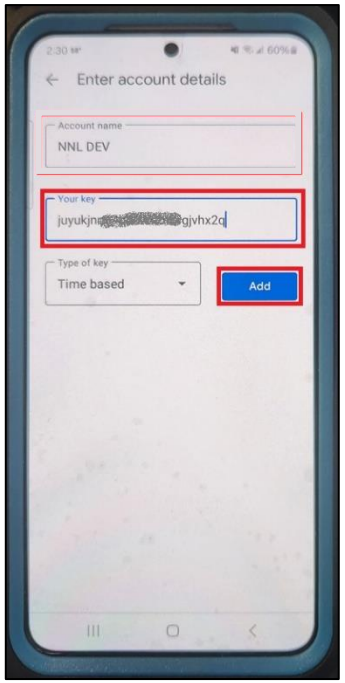
14. Enter the key displayed in the OCI Identity Domain Mobile App.
    - NOTE: The key is not case-sensitive. The spaces are for readability but not required when entering in authenticator app.
    - Google Authenticator App only - leave *Type of key* as the default, "Time based".

Click **Finish**.



Microsoft Authenticator App

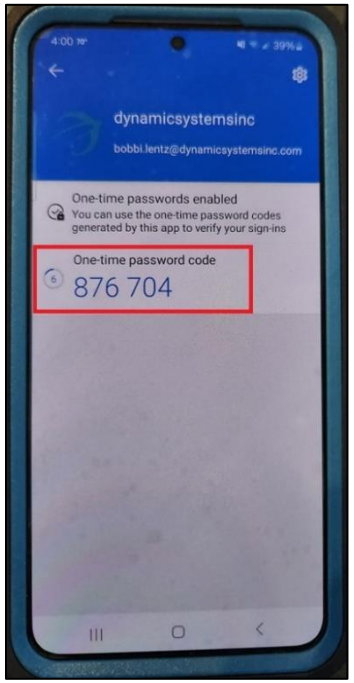
Click **Add**.



Google Authenticator App

OCI IAM Domain – Authenticator App (cont.)

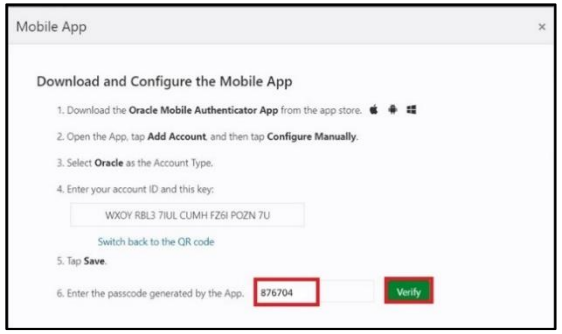
14. A *One-time password code* is generated in the authenticator app.



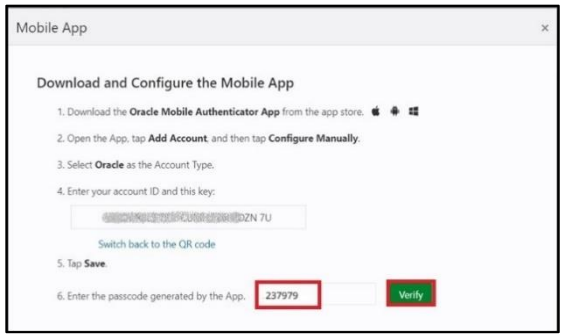
Microsoft Authenticator App

Google Authenticator App

15. Enter the *One-time password code* displayed in the authenticator app in the OCI Identity Domain *Mobile App*. Click **Verify.**



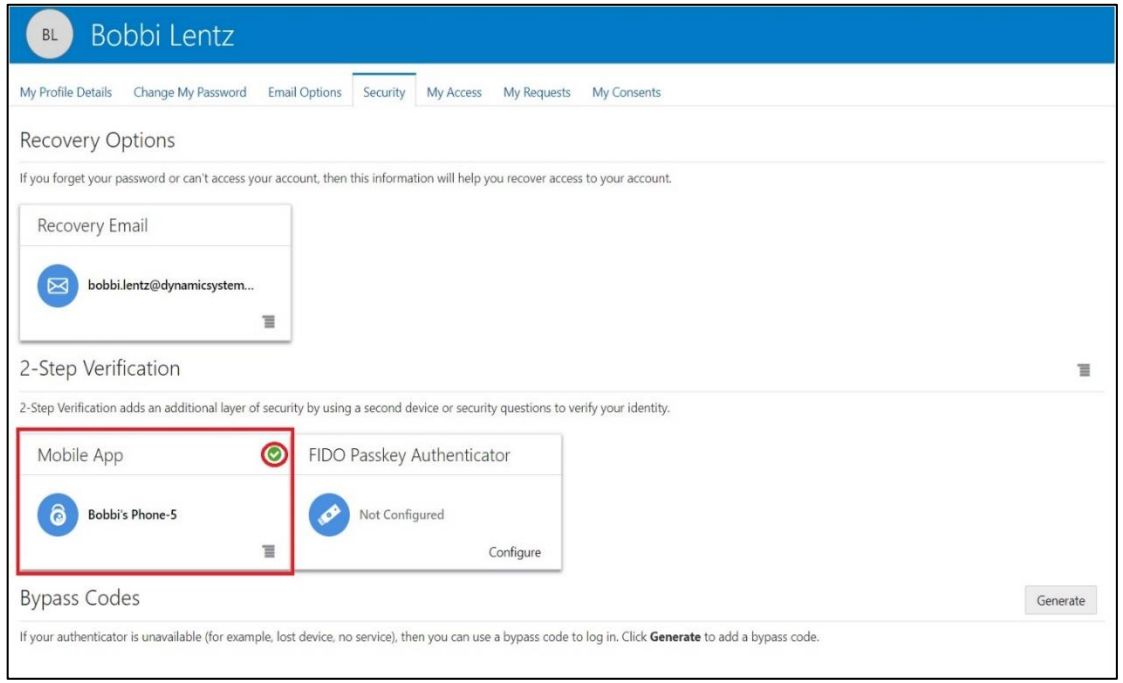
Microsoft Authenticator App Code



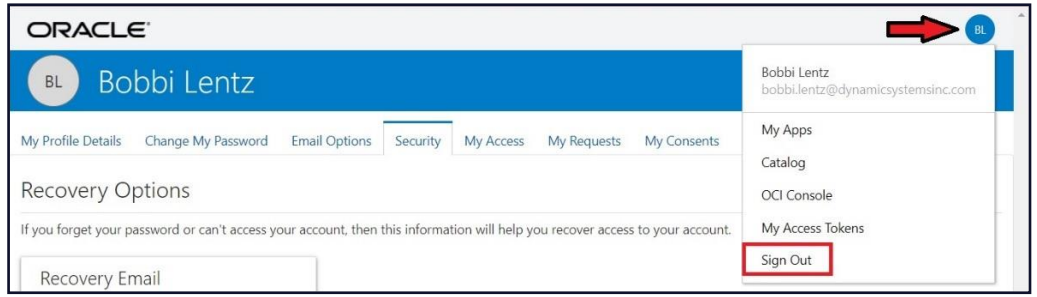
Google Authenticator App Code

OCI IAM Domain – Authenticator App (cont.)

16. You are now returned to your profile page. Mobile App box shows green checkmark and identifies the mobile device used.

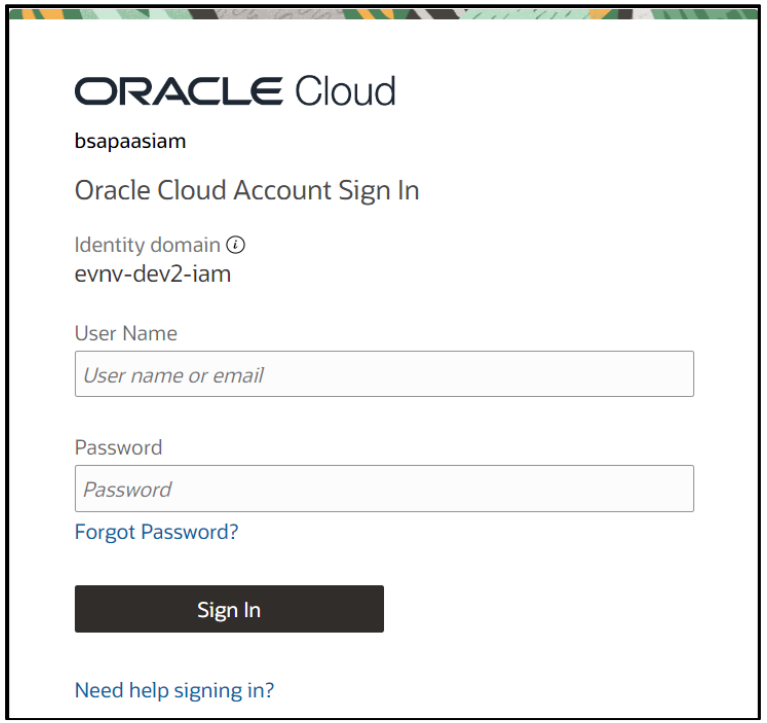


17. At top right, click the circle containing your initials, select **Sign Out** from the dropdown.



OCI IAM Domain – Authenticator App (cont.)

18. You are returned to the login page for the identity domain.



STOP.

End of Process

OCI IAM Domain – Authenticator App (cont.)

Authenticator App Configuration

It is helpful to assign a meaningful name to the account in authenticator apps. If you did not do it during setup or want to change it, follow the appropriate instructions below.

Microsoft Authenticator App

- Select the account you added in the Microsoft Authenticator App
- Select the gear icon at top right
- Click the name next to Account name
- Rename account box will appear
- Enter a meaningful name to identify the account (i.e., NNL OFC)
- Select **Done**

Google Authenticator App

- Press and hold the account you added in the Google Authenticator App
- Select the pencil icon at top
- Enter a meaningful name to identify the account (i.e., NNL OFC)
- Select **Save**

OCI IAM Domain – FIDO2 Security Key

OCI IAM Domain – FIDO2 Security Key

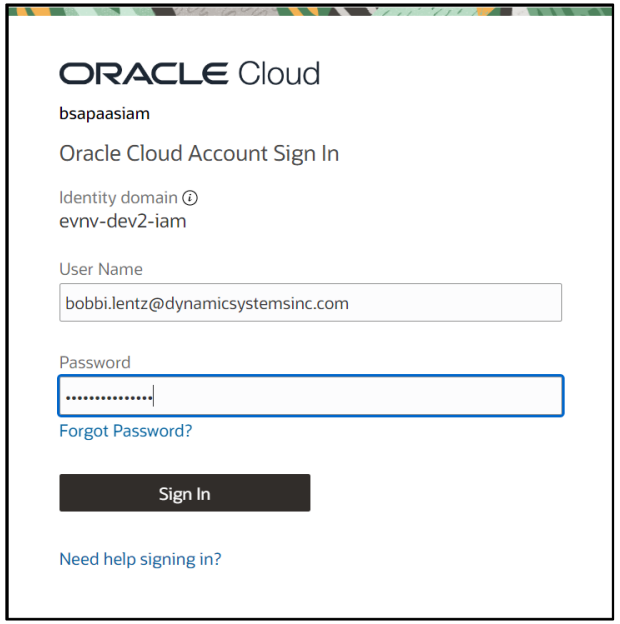
A user who is required to or chooses to use a FIDO2 security key must select one that is FIPS 140-2 certified. The one that is approved for use with NNL's OFC environment is available for purchase from Yubico at this site:

https://www.yubico.com/product/yubikey-5-fips-series/yubikey-5-nfc-fips/

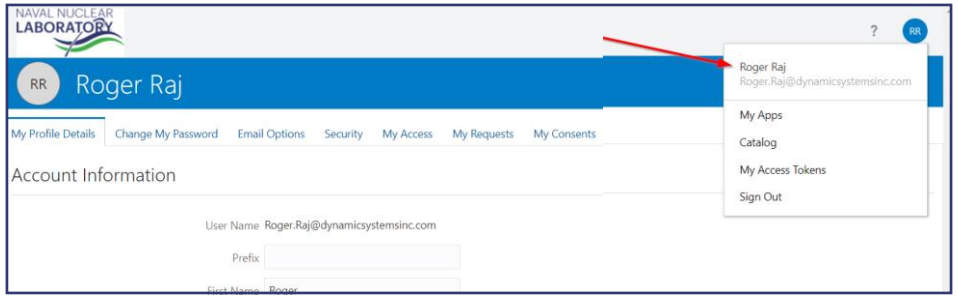
With an approved FIDO2 security key in possession, use the following instructions.

OCI IAM Domain – FIDO2 Security Key (cont.)

1. At the login window, enter your **User Name** and **Password**. Click **Sign In**.

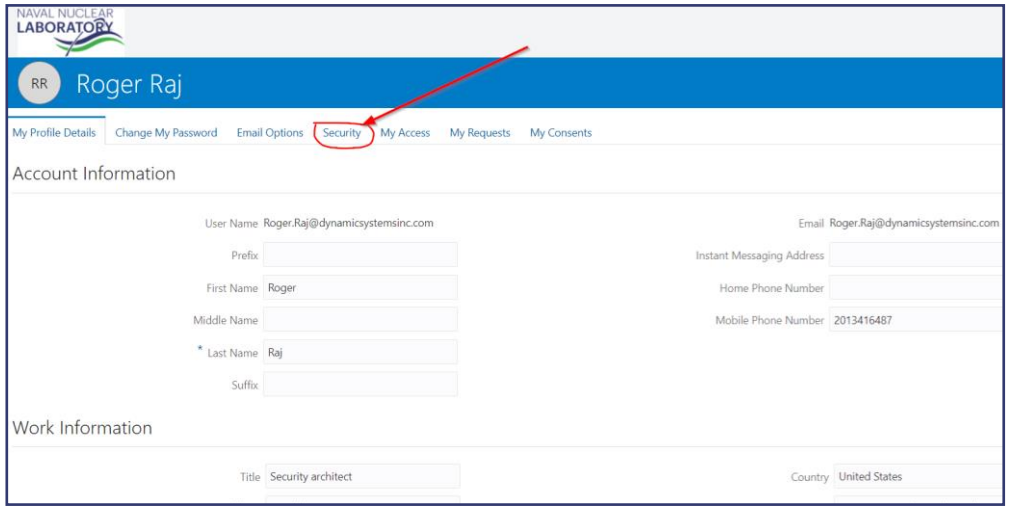


2. Upon login, choose the **Profile** option to modify the user's profile.

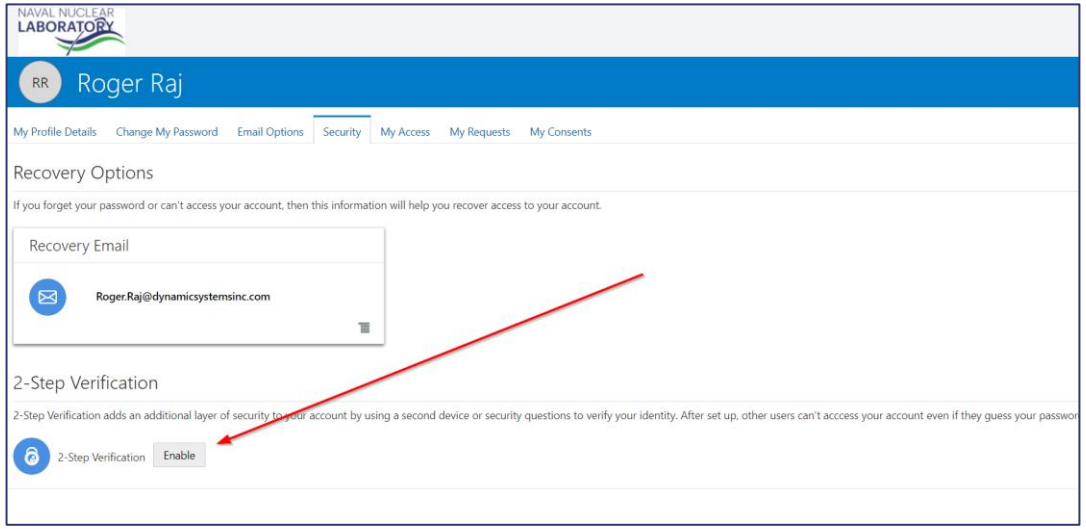


OCI IAM Domain – FIDO2 Security Key (cont.)

3. Click on the **Security** tab.

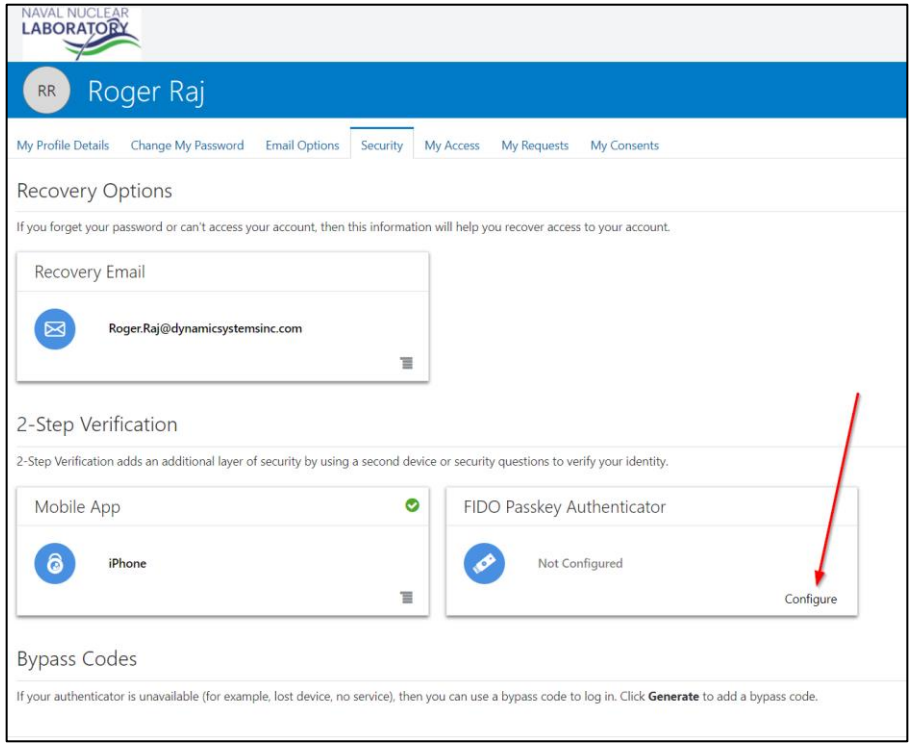


4. Below *2-Step Verification*, click **Enable**.



OCI IAM Domain – FIDO2 Security Key (cont.)

5. On *FIDO Passkey Authenticator,* click **Configure**.



6. You will be prompted to choose a passcode. Choose a **minimum of a 6-digit passcode** and verify it.
7. The system will prompt you to ‘touch’ the blinking green LED on the Yubikey twice. After doing this, it will register the key with OCI and with your system and will be used for future 2-factor Authentication.

Configuration of the FIDO2 security key is complete.

OCI IAM Domain – FIDO2 Security Key (cont.)

To login to the OFC environment in the future:

1. Insert the Yubikey in the USB slot
2. Navigate to the OFC login page (*to be established*)
3. Enter your username and password at the login screen
4. Select Verify
5. Select security key from the Windows Security pop-up and touch the Yubikey.
6. You will then be presented with the login warning banner (Terms of Use). Click to agree and then click **Continue**.
7. You will be presented with the OFC applications home page.

Support

If you are experiencing issues with your account, please reach out to NNL ERP Security at:

nnl-erpsecurity@unnpp.gov