Instructions to Enroll and Sign in to LiteBlue with Multifactor Authentication (MFA)

User Guide
January 15, 2023

CONTENTS

This user guide contains step-by-step instructions for end-users who are configuring a security method (or methods) to sign in to LiteBlue with multifactor authentication.

To navigate using the Table of Contents, click on the appropriate topic below.

OVERVIEW

Maintaining the privacy of your personal data is a shared priority for you and the Postal Service. Your private information stored online is a target for criminals who seek to compromise this data for their financial gain. As an additional safety measure, the Postal Service has deployed multifactor authentication (MFA) on LiteBlue.

This means that, in addition to providing your Employee Identification Number (EIN) and Password, you will be required to provide a second security factor (MFA), such as Push Notification approval from One-Time Passcode (OTP) SMS Text, One-Time Passcode (OTP) Phone call, Okta Verify, Google Authenticator or E-mail verification (default).

The objective of this document is to provide detailed instructions for users who are establishing a security method (or methods) to sign into LiteBlue with multifactor authentication.

There are steps that you will perform in a web browser from your computer, and steps that you will perform on your mobile phone.

The first step requires users to reset their password in the Self-Service Profile.

Users are then required to log in to LiteBlue and configure two or more MFA security methods. Instructions to configure all security methods are included in this document.

UNITED STATES
POSTAL SERVICE ®

How to reset your Self-Service Profile (SSP) password
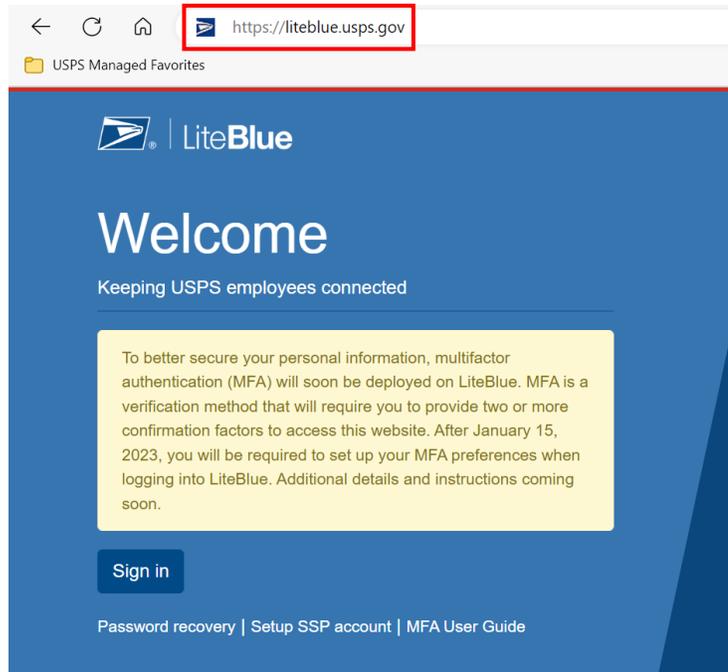
1. On your computer, open a web browser and navigate to LiteBlue: https://liteblue.usps.gov	
2. Select **Setup SSP Account.**	

3. Select **Enter SSP.**	**Welcome to Self-Service Profile (SSP)** The portal to the tools for the management of your Self-Service Profile. **Important Information** Self-Service Profile is available to all USPS Employees. Use your employee ID and password to access all self-service web applications. This is the place to manage your Self-Service Password, PIN, and more. Enter SSP
4. Enter **Employee ID and Password** and select **Sign In.**	**Sign In To SSP** Employee ID Enter Employee ID Password Enter Password Sign In Forgot / Change Password
5. Submit Answers to **Security Questions** and select **Submit Answers.** *If you do not know the answers to your security questions, please proceed to* [*How to reset your SSP password if you forget your security questions*](#)*.*	**USPS Self-Service Profile** **Password Reset - Security Questions** If you have forgotten your password, you can log on with your USPS Self-Service Profile (SSP) Credentials. * Please answer the two security questions from your SSP profile to get started. **EIN:**01548790 **Security Question 1:**In what city or town was your first job? **Answer 1:** **Security Question 2:**What street did you live on in third grade? **Answer 2:** Submit Answers Forgot Answers
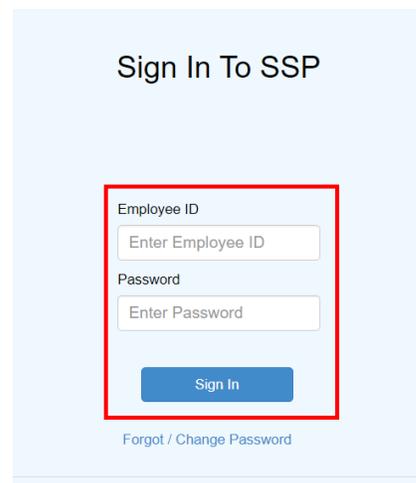
6. Enter **New Password**, **Confirm Password** and select **Update Password.**

Your password has expired. Please reset the password

Strong Password Requirements:

The password must be 15 to 64 characters in length, cannot contain your EIN, first name, or last name and cannot be the same as the 5 previously used passwords.

If you choose to use special characters in the password, only the following are allowed

! @ $ % ^ * _ + ~

New Password: [   ]
Confirm Password: [   ]

Update Password

7. **Logout** (top right) from Self-Service Profile**.**

If you would like to update your email, PIN or security questions, please do so before logging out of SSP.

SELF-SERVICE PROFILE
SSP

Help   Logout

vice's Self-Service applications.

, and when you set it up. Through the tabs it also allows you to create a new password and to add, update, ows you to update your security questions and answers. These are the questions you need to answer if you

	Last Updated Date (24 HR Format - Central Time Zone)
	09/08/2014 14:56:06
	09/08/2014 14:56:06
	03/24/2014 11:12:02
	07/30/2014 13:18:59
	07/30/2014 13:18:59

g back into SSP to see the Email component set to Yes in the Profile Summary.

8. Password reset is complete.

You may close out using the x on the upper right-hand corner of the page and continue on to configuring your MFA preferences below.

Self-Service Profile

Sign In To SSP

Employee ID
[Enter Employee ID]

Password
[Enter Password]

Sign In

Forgot / Change Password

New to SSP? This is the place to:

- Create your Self-Service Profile
- Update your Self-Service Password
- Update your PIN
- Add or change an Email address **
- Add or edit security questions

The Self-Service Password is different from your ACE password. This is for use with HR online applications.

Your PIN is now only used for IVR transactions.

**This helps changes to your profile to take effect much more quickly. You won't have to wait for the First-Class letter to arrive before confirming the change.

How to configure MFA for your LiteBlue user account (Employee ID)

1. On your computer, open a web browser and navigate to LiteBlue*:* https://liteblue.usps.gov	
2. Select **Sign In.**	
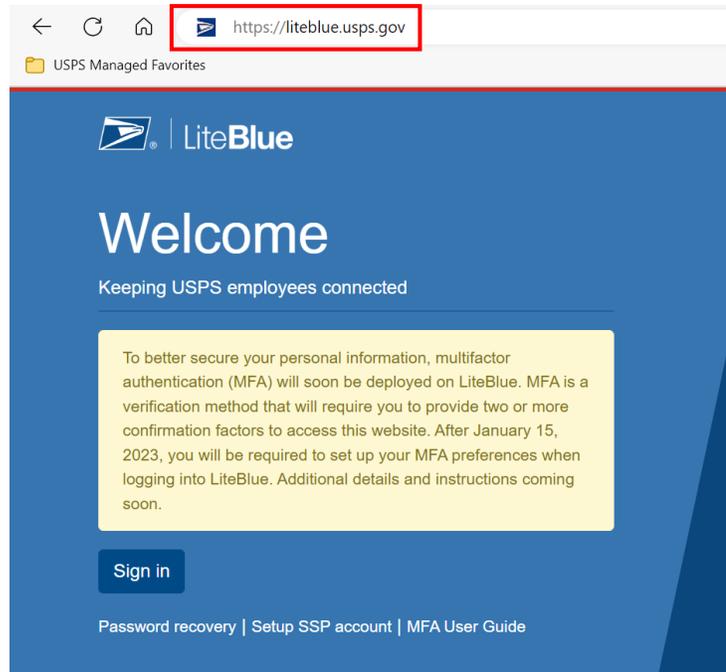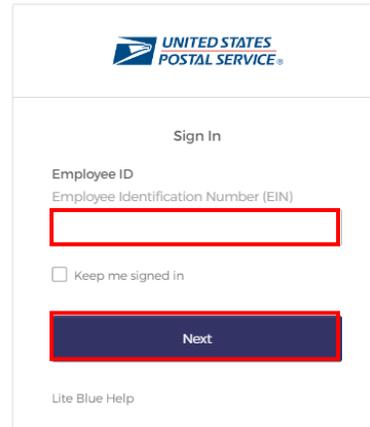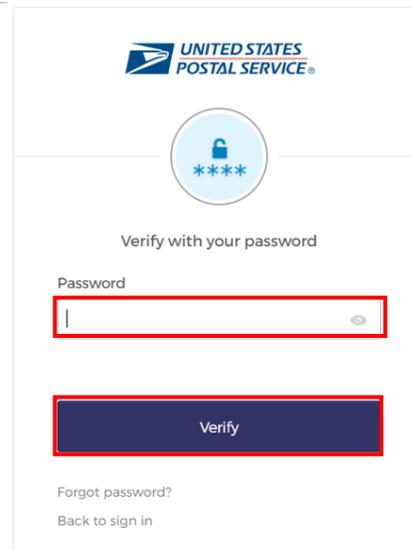
3. Enter **Employee Identification Number (EIN)** and select **Next.**		
4. Enter **Password** and select **Verify.**		
5. Enter the **last 4 digits of your Social Security Number** and select **Verify**. *This step will only occur during the initial security method enrollment login.*		
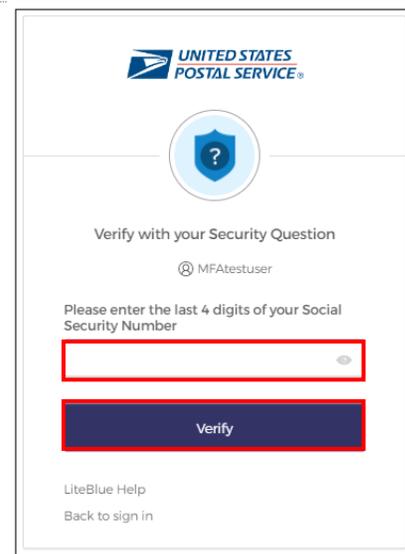
6. Select **Set up** under the first security method you would like to be your primary MFA security method.

   Users are required to select <u>two</u> (or more) security methods.

   You will be able to set up additional security method(s) after you set up your first security method.

   Detailed instructions for setting up each security method can be found in this document by using the following links:

   [How to set up Phone (SMS) MFA security method](#)

   [How to set up Phone (Voice) MFA security method](#)

   [How to set up Okta Verify MFA security method](#)

   [How to set up Google Authenticator MFA security method](#)

   Email is the default MFA security method but isn't an option until MFA security methods are set up.
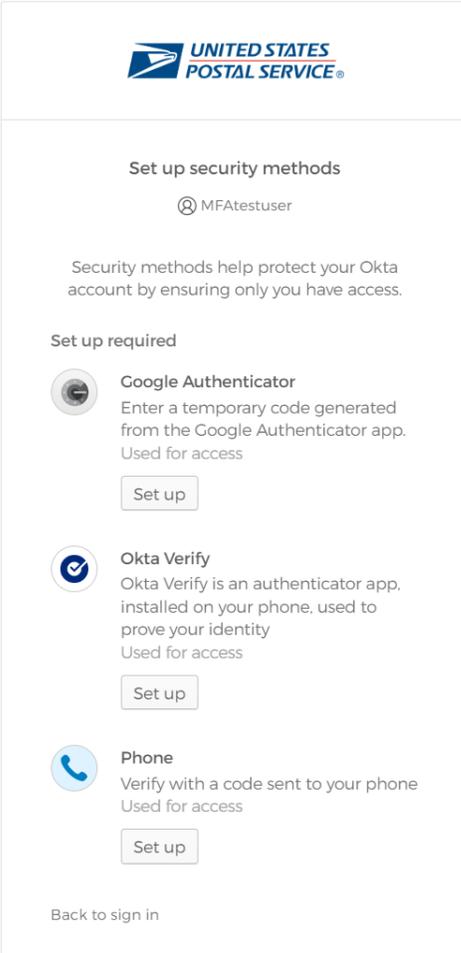
Set up security methods

MFAtestuser

Security methods help protect your Okta account by ensuring only you have access.

Set up required

Google Authenticator
Enter a temporary code generated from the Google Authenticator app.
Used for access

Set up

Okta Verify
Okta Verify is an authenticator app, installed on your phone, used to prove your identity
Used for access

Set up

Phone
Verify with a code sent to your phone
Used for access

Set up

Back to sign in

7. After your primary security method is set up, you will return to the set up security methods screen.

   Select **Set up** to configure an additional security method and follow the prompts (links to detailed instructions below).

   How to set up Phone (SMS) MFA security method

   How to set up Phone (Voice) MFA security method

   How to set up Okta Verify MFA security method

   How to set up Google Authenticator MFA security method

---
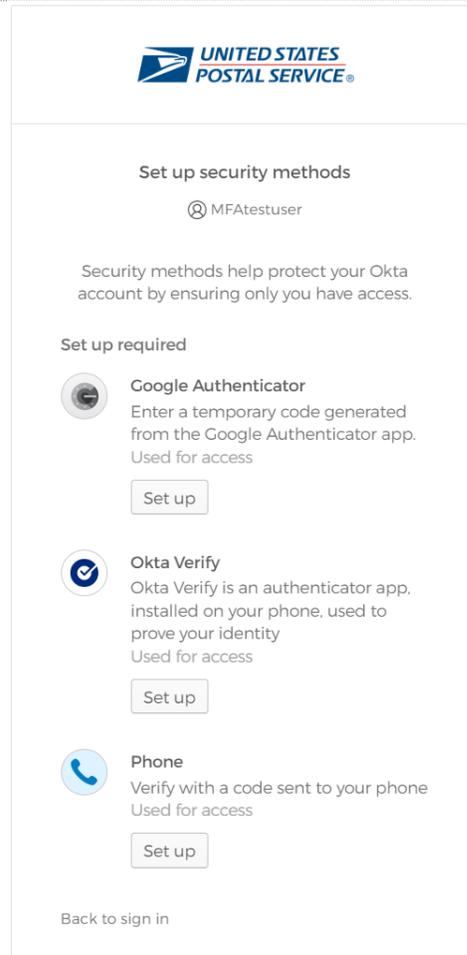
8. You have successfully configured your MFA security methods and signed in to LiteBlue!

   The next time you sign in to LiteBlue, you will be required to use the security method(s) that you configured.

   Click here for instructions to log in to LiteBlue after your MFA security methods are set up.

How to set up Phone (SMS) MFA security method

1. Select **Set up** under **Phone**.	
2. Select **SMS.** **Enter a phone number** where you can receive SMS text messages. Then select **Receive a code via SMS.**	

3. **Enter** the **Code** that you received on your phone via SMS message and select **Verify.** You have successfully configured your Phone SMS security method. Click here to return to security method configuration set up options.	**UNITED STATES POSTAL SERVICE ®** Set up phone authentication Ⓐ MFAtestuser Calling your phone. Enter the code below to verify. Carrier messaging charges may apply Enter Code Verify Return to authenticator list Back to sign in

How to set up Phone (Voice) MFA security method

1. Select **Set up** under Phone to configure **Voice call**.

2. Select **Voice call**. **Enter a phone number** where you can receive a verification code via voice call. Then select **Receive a code via voice call**.	
3. Receive a phone call and **enter the code** (six-digit numeric code) provided via the phone call. Select **Verify.** You have successfully configured your Voice Call security method. Click here to return to security method configuration set up options.	

How to set up Okta Verify MFA security method

1. Select **Set up** under **Okta Verify** to configure an additional security method.

   This option requires the Okta Verify application to be downloaded to your smart phone.

2.	The Set up Okta Verify screen with a QR code will then appear. Proceed to the next step to continue Okta Verify set up.	
3.	On your **smart phone**: Select the appropriate **app store** based on the type of mobile phone you have.	

User Guide

4. Search for Okta Verify in your phone's App store.		
5. On your phone, **Select** and **Install** the Okta Verify application.		

15

6. Verification of installation. Select **OK.**	
7. The Okta Verify app is now available on your home screen. **Select** the app to continue the set up.	
8. Select **Get Started.**	
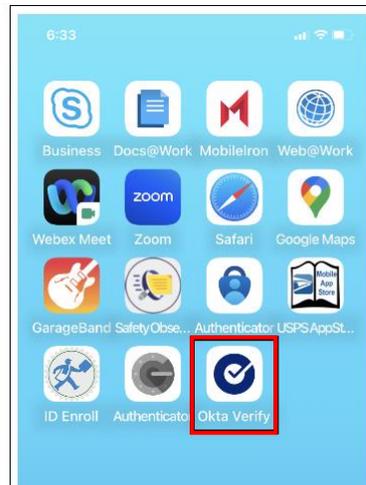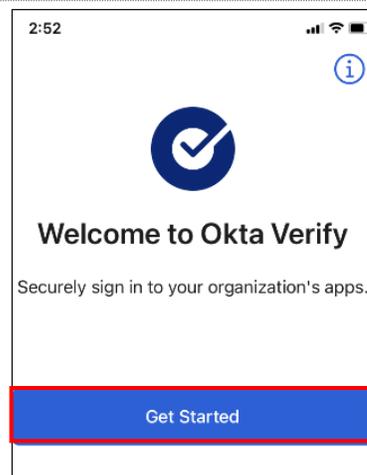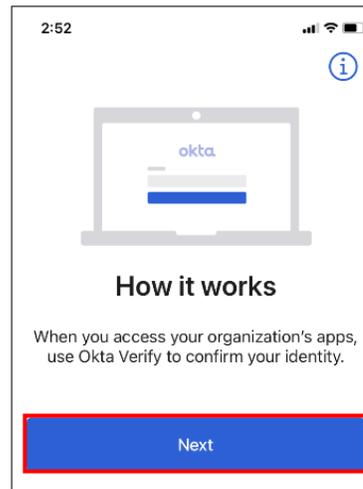
9. Select **Next.**	How it works When you access your organization's apps, use Okta Verify to confirm your identity. Next	
10. Select **Add Account.**	Ways to verify When signing in, enter a code from this app, tap Yes on a push notification, or tap the "Sign in using Okta Verify on this device" button. Add Account	
11. Select **Organization.**	Close Add Account **Choose Account Type** Choose the type of account you would like to add Organization Work, school, company > Other Facebook, Google, etc >	
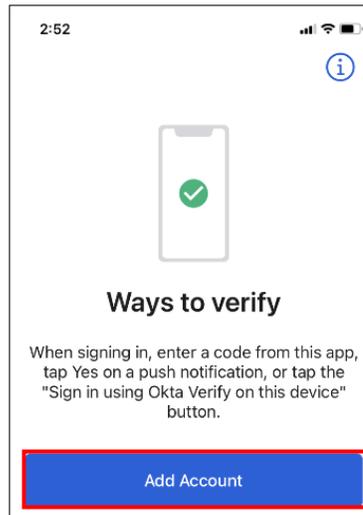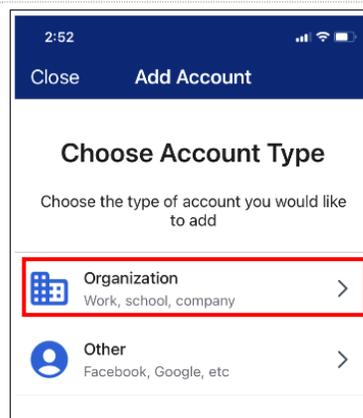
12. Select **Yes, Ready to Scan.**		
13. **Allow** Okta Verify to access your camera by selecting **OK.**		
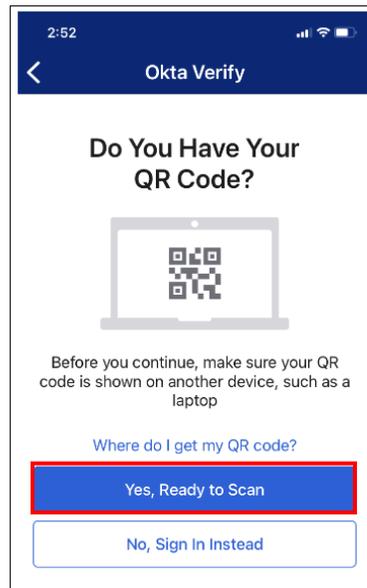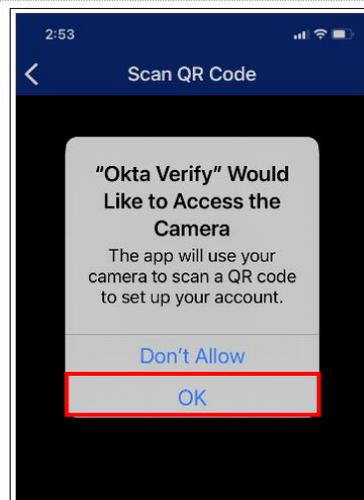
14. Using your phone's camera, **scan** the QR code on the computer. *Installation and setup of Okta Verify on an Android may look different than the screen shots in this user guide (which are from an iPhone). The process will be the same.*	
15. Select **Allow** the Push Notifications option and select **Allow** to confirm. *Push Notifications is the preferred Security Option.*	
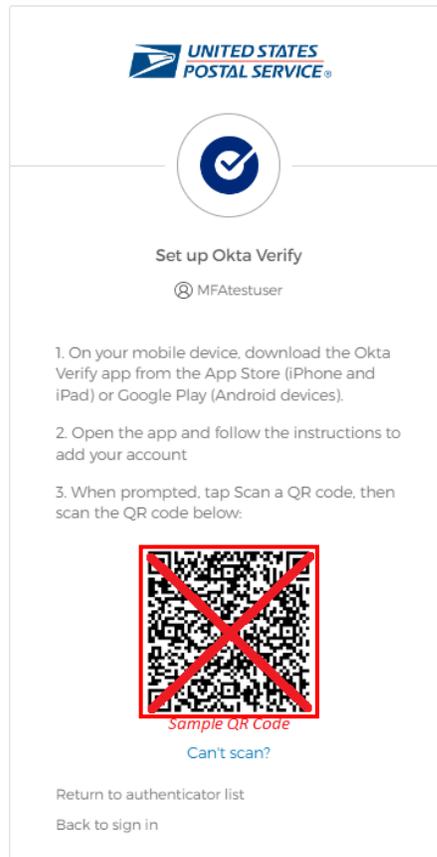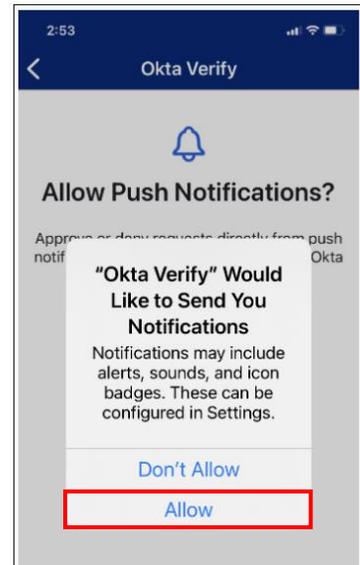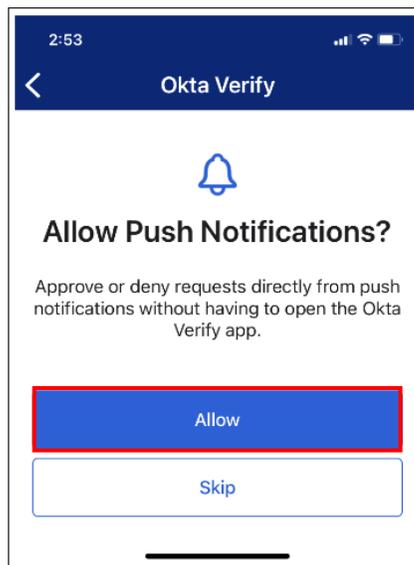
16. **Enable** Face ID, select **OK** to enable face ID. *Face ID is an additional security feature in Okta Verify. If you are not comfortable using Face ID, you can select Don't Allow. You will still be able to use Okta Verify as an MFA security method.*	
17. **Select Done** on Account Added screen.	
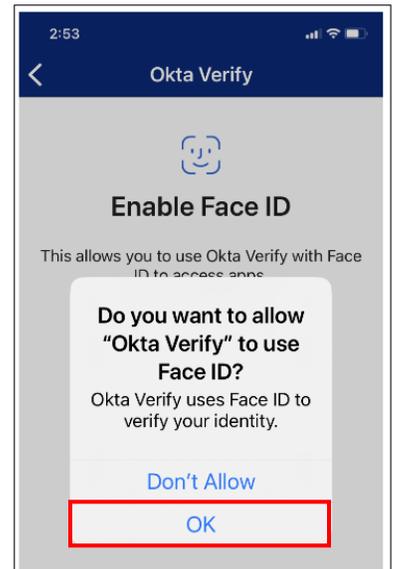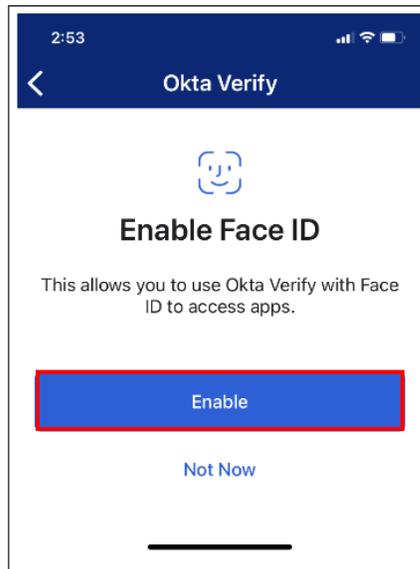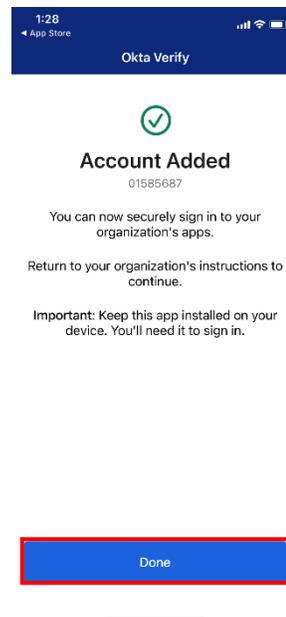
18. On your phone, you will receive the Push Notification.

    Select **Yes, It's Me.**
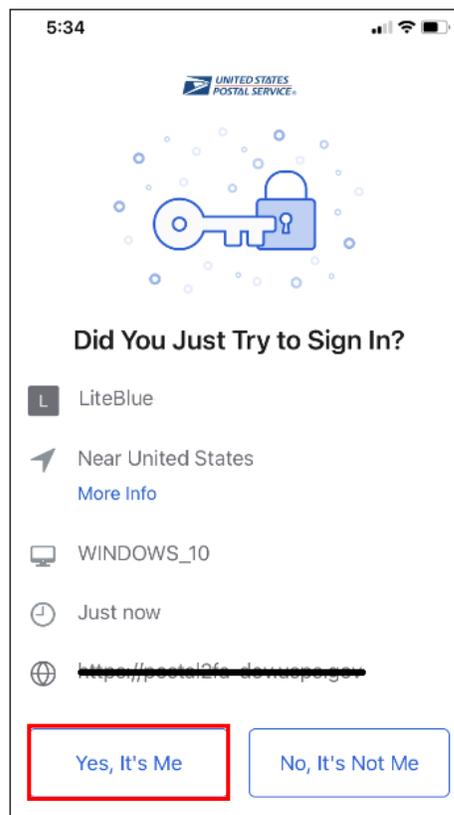
19. On your phone, you will receive confirmation of the Push Notification.

    You have successfully configured your Okta Verify security method.

    Click here to return to security method configuration set up options.
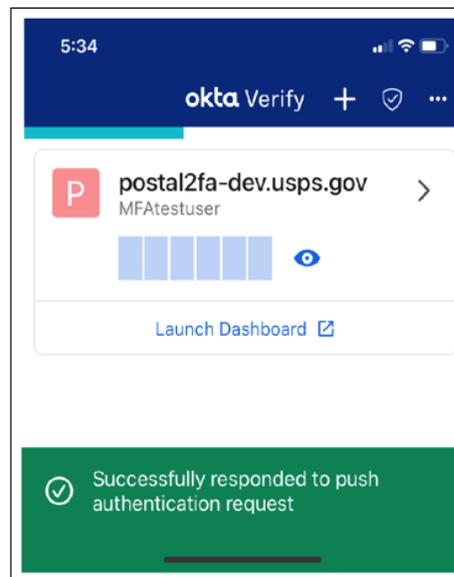
How to set up Google Authenticator MFA security method

1. Select **Set up** under **Google Authenticator** to configure this security method. *This option requires the Google Authenticator application to be downloaded to your smart phone.*	
2. Screenshot indicates the next steps to set up Google Authenticator. You will now need to download the Google Authenticator app to your smart phone. Please proceed to the next step. *Installation and setup of Google Authenticator on an Android may look different than the screen shots in this user guide (which are from an iPhone). The process will be the same.*	
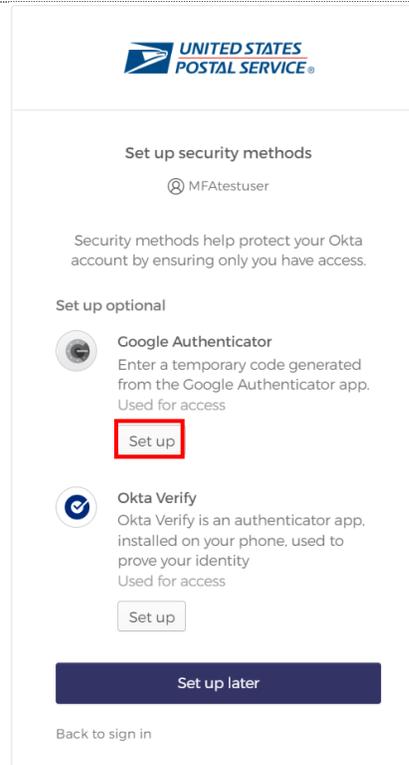
3.	On your **smart phone**: Select the appropriate **app store** based on the type of mobile phone you have.	
4.	In the appropriate app store, **search for Google Authenticator.**	
5.	On your phone, **Select** and **Install** the Google Authenticator app.	
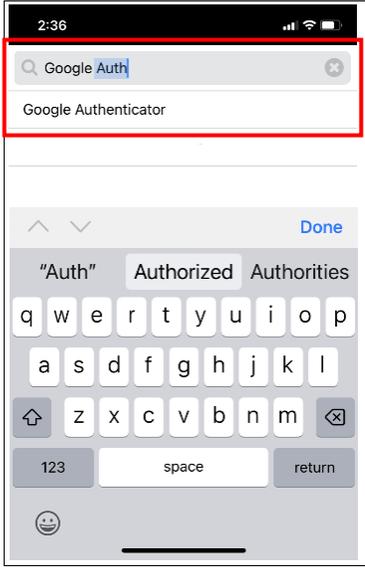
23
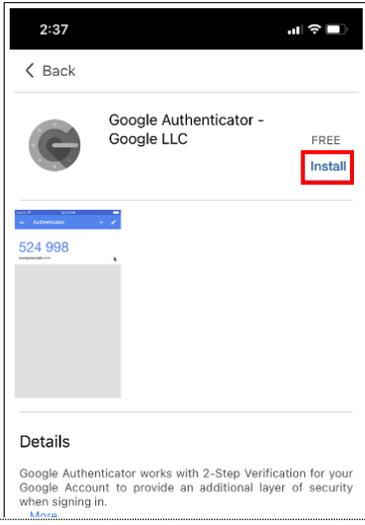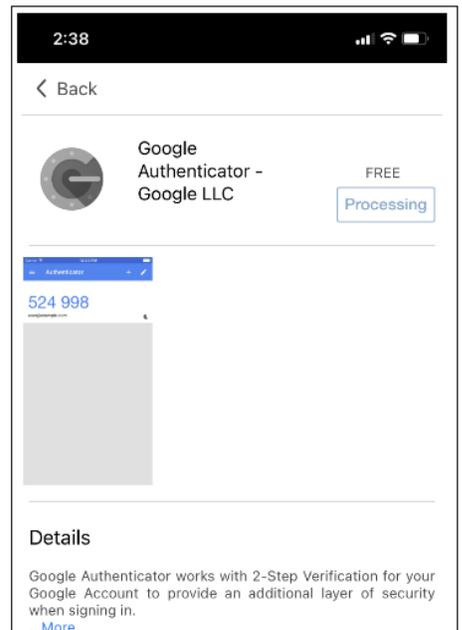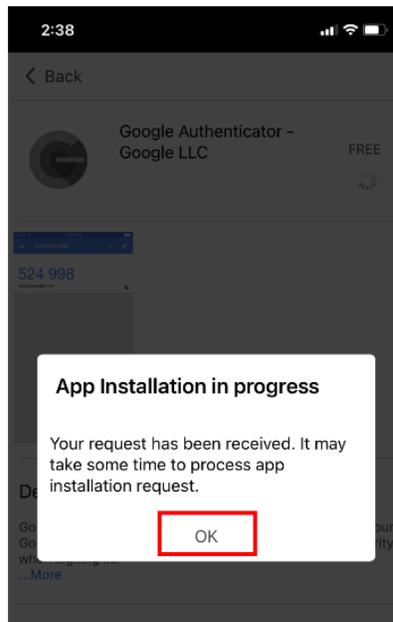
6.	Verification of installation. Select **OK.**	
7.	The Google Authenticator app is now available on your home screen. **Select** the app to continue the setup.	

8. Select **Get Started.**		
9. Select **Scan a QR Code.**		
10. **Allow** the Authenticator to access your camera by selecting **OK.**		
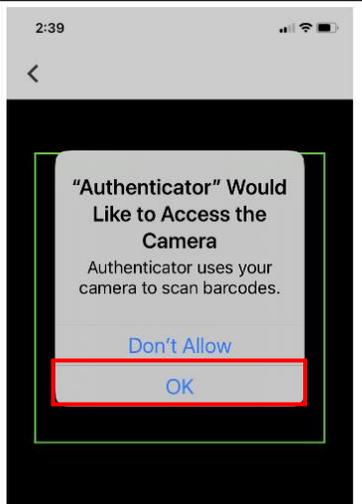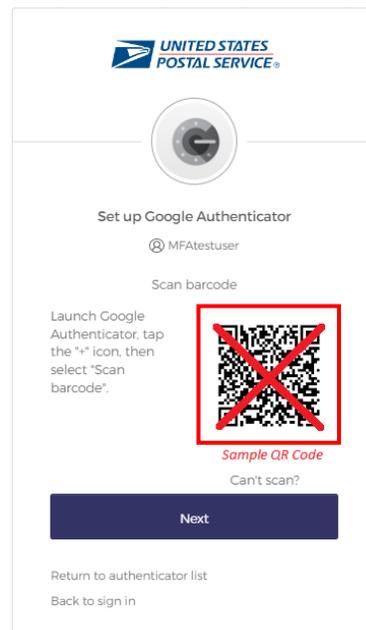
11. Using your phone's camera, **scan** the QR code on the computer.	
12. On your phone, the Google Authenticator app will begin generating a six-digit verification code.	
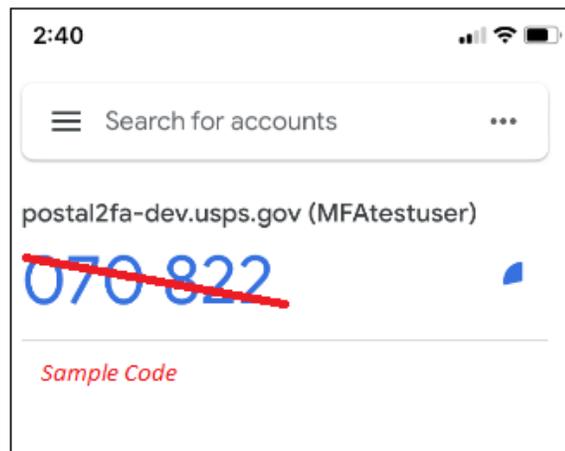
13. On your computer, enter the **code** generated on your phone and select **Verify**.

    You have successfully completed the setup of the Google Authenticator app.

    Click here to return to security method configuration set up options.
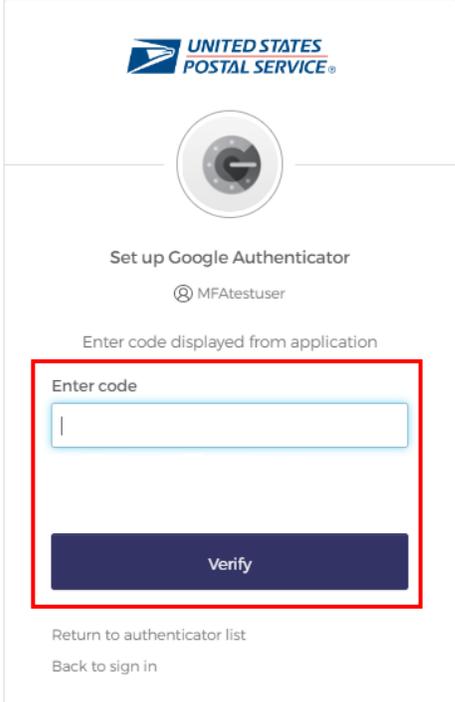
    Set up Google Authenticator

    (Ⓡ) MFAtestuser

    Enter code displayed from application

    Enter code

    Verify

    Return to authenticator list

    Back to sign in

How to log in to LiteBlue after MFA is set up

1. On your computer, open a web browser and navigate to LiteBlue: https://liteblue.usps.gov	
2. Select **Sign In.**	
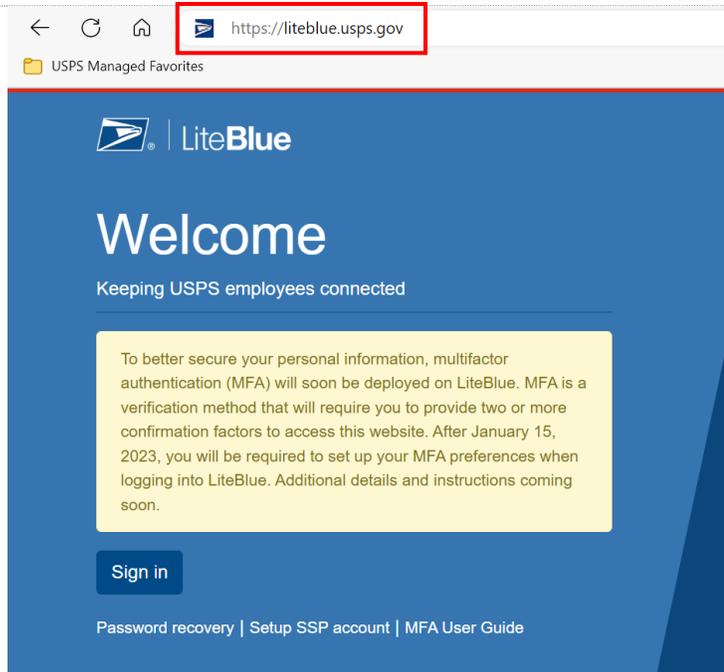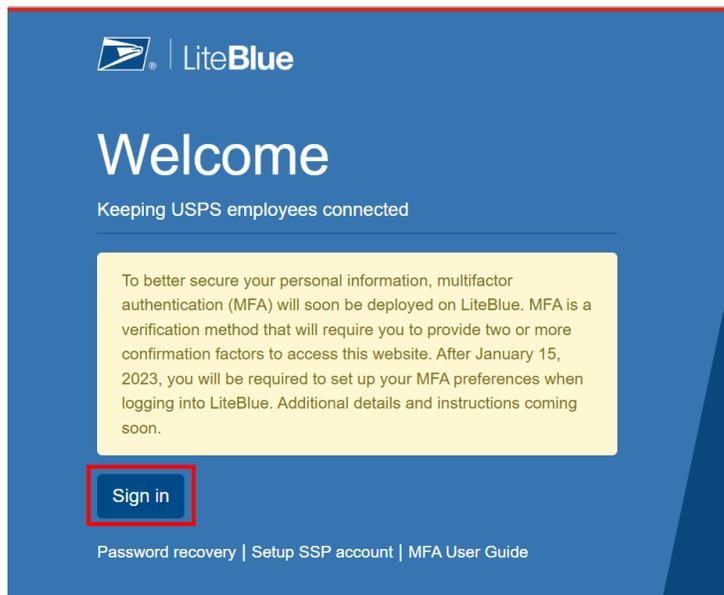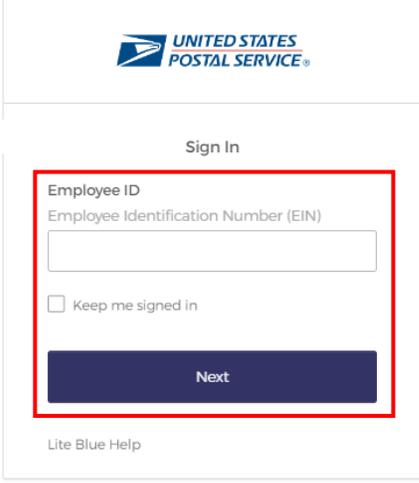
3. Enter **Employee Identification Number (EIN)** and select **Next.**

4. Enter **Password** and select **Verify.**
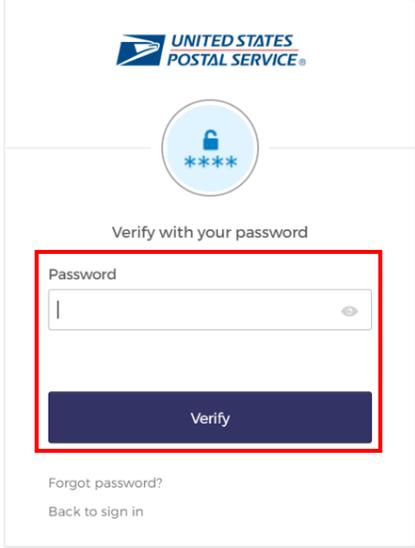
5. For demonstration purposes, the Phone SMS security method is illustrated in the following steps.

   Click on **Receive a code via SMS.**

   You will then receive a code to your mobile phone.

   Or

   *Click on **Verify with something else** and follow the prompts.*

   If you verify with another security method, follow the prompts on your phone and on the screen to log into LiteBlue.
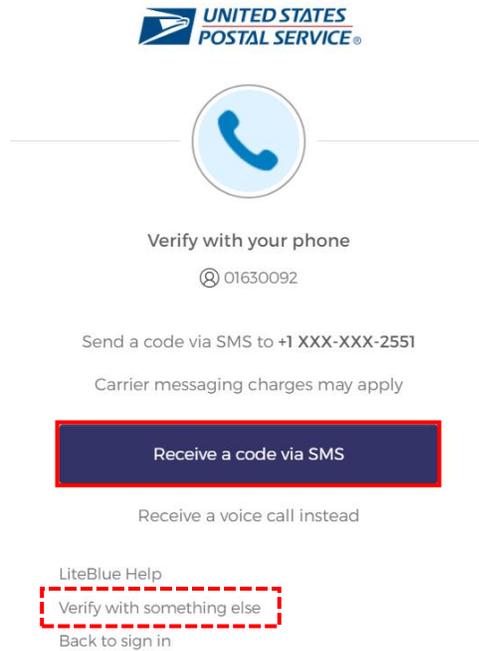
6. **Enter code** received via SMS.
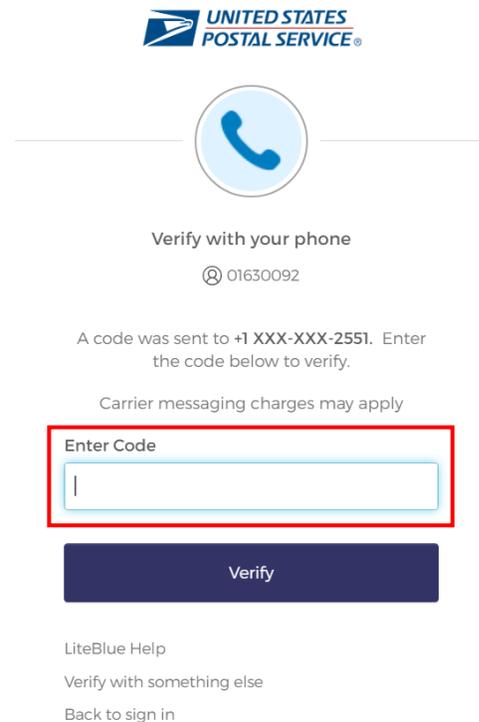
7. You have successfully logged into LiteBlue.

How to reset your SSP Password if you forget your Security Question Answers

1. Select **Forgot Answers.**	**USPS Self-Service Profile** **Password Reset - Security Questions** If you have forgotten your password, you can log on with your USPS Self-Service Profile (SSP) Credentials. * Please answer the two security questions from your SSP profile to get started. **EIN:**01548790 **Security Question 1:**In what city or town was your first job? **Answer 1:** **Security Question 2:**What street did you live on in third grade? **Answer 2:** Submit Answers Forgot Answers
2. Enter your **Employee ID**, **Birth Date, Last 4 digits of SSN,** and **PIN.**	**USPS Self-Service Profile** **Password Reset** To reset your password provide the information below and then select "Request Reset". * All fields are required. Employee ID: Enter Employee ID Birth Date: mm/dd/yyyy Last 4 digits of SSN: Personal Identification Number(PIN): Delivery Method Options: * ●Email (Registered in Profile) ○First-Class Mail Enter the code from the image below: * Image Code: 782b3 Request Reset Please Click Here to go to SSP Login Page

3. **Select delivery method** (Email or First-Class Mail)

   This is how you will receive your password reset link.

4. **Enter the code** from the image below.

5. Select **Request Reset.**	**USPS Self-Service Profile** **Password Reset** To reset your password provide the information below and then select "Request Reset". * All fields are required. Employee ID: * [Enter Employee ID] Birth Date: * [mm/dd/yyyy] Last 4 digits of SSN: * [ ] Personal Identification Number(PIN): * [ ] Delivery Method Options: * ◉Email (Registered in Profile) ○First-Class Mail Enter the code from the image below: * [ ] Image Code: 782b3 [Request Reset] Please Click Here to go to SSP Login Page
6. You will then receive an email or first-class mail with a password reset link. **Click on the link** in the email or **enter the web address** from the first-class mail into your browser.	**From:** SSP_DO_NOT_REPLY@USPS.GOV <SSP_DO_NOT_REPLY@USPS.GOV> **Sent:** Wednesday, January 11, 2023 11:52 AM **To:** Iverson, John A - Eagan, MN - Contractor <John.A.Iverson@usps.gov> **Subject:** Password Reset Verification - ACTION REQUIRED Dear MANUEL ORTIZ, On January 11, 2023 at 11:52, our records indicate that you have successfully regained access to change your password through the employee Self-Service Profile (SSP) application. Click ONCE on the link below (or) Copy and Paste it in the Web Browser's address bar,within 72 hours to verify that you initiated this change. ************************************** https://ssp-cat.usps.gov/ssp-web/forgotpasswordchange.xhtml?verificationkey=a7932ca4-d7d8-49e6-ba7e-22ca0921a5a5 ************************************** If you have questions, or need assistance, contact the HR Shared Service Center at 1-877-477-3273, option 5. HR Shared Services Please do not reply to this Email as it is an unmonitored account and will likely not be read. If you need assistance please contact Shared Services at the number listed above. NOTE: All times listed are in Central Time Zone.
7. Enter **New Password**, **Confirm Password** and select **Update Password.**	**Your password has expired. Please reset the password** **Strong Password Requirements:** The password must be 15 to 64 characters in length, cannot contain your EIN, first name, or last name and cannot be the same as the 5 previously used passwords. If you choose to use special characters in the password, only the following are allowed ! @ $ % ^ * _ + ~ New Password: [ ] Confirm Password: [ ] [Update Password]

UNITED STATES
POSTAL SERVICE ®

9.	**Logout** (top right) from Self-Service Profile**.** *If you would like to update your email, PIN or security questions, please do so before logging out of SSP.*	SELF-SERVICE PROFILE SSP Help Logout vice's Self-Service applications. , and when you set it up. Through the tabs it also allows you to create a new password and to add, update, ows you to update your security questions and answers. These are the questions you need to answer if you |	Last Updated Date (24 HR Format - Central Time Zone)
	09/08/2014 14:56:06
	09/08/2014 14:56:06
	03/24/2014 11:12:02
	07/30/2014 13:18:59
	07/30/2014 13:18:59 | g back into SSP to see the Email component set to Yes in the Profile Summary.
10.	Password reset is complete.	Self-Service Profile Sign In To SSP **New to SSP?** This is the place to: • Create your Self-Service Profile • Update your Self-Service Password • Update your PIN • Add or change an Email address ** • Add or edit security questions The Self-Service Password is different from your ACE password. This is for use with HR online applications. Your PIN is now only used for IVR transactions. **This helps changes to your profile to take effect much more quickly. You won't have to wait for the First-Class letter to arrive before confirming the change. Employee ID Enter Employee ID Password Enter Password Sign In Forgot / Change Password