

Frequently Asked Questions (FAQs)

Multifactor Authentication for LiteBlue



“Unknown device or location” error message in LiteBlue

Question: Why am I getting an “Unknown device or location” error message when I attempt to log in to LiteBlue?

Answer: Due to recent security updates within LiteBlue, login attempts from unrecognized devices or locations are being blocked.

If you receive an “**Unknown device or location**” message and cannot advance past the initial LiteBlue login screen, please take the following steps:

- First, try logging in to LiteBlue from a device previously used to access the website since setting up your MFA preferences (on or after January 15, 2023).
- If you do not have access to that device, but have an ACE ID, try logging in to LiteBlue on the postal network.

When setting up MFA for LiteBlue, please use your preferred personal device. On your subsequent log in, please use a Postal Service device if you have access to one.

“Your account is locked” error message in LiteBlue

Question: Why am I getting a “Your account is locked” error message when I attempt to log in to LiteBlue?

Answer: Your account is locked because you have entered your password incorrectly more than six times or you have not set up your security question in LiteBlue. Please click on the Password Recovery / Password Reset link.

General Questions

Question: I am a contractor with the Postal Service, does MFA impact me?

Answer: No. Since your personal information is not housed on the LiteBlue postal network, you are not impacted by the SSP password reset or MFA requirements.

Question: Why is Multifactor Authentication (MFA) being required for LiteBlue?

Answer: MFA is a tool to assist the Postal Service in preventing cyberattacks and protecting you and your personal information. It provides an additional level of security to help protect your ID, passwords, and other personal data from unauthorized access and misuse.

Question: How do I set up my MFA preferences for LiteBlue?

Answer: Follow the step-by-step instructions in the User Guide and/or Videos posted on the MFA [Blue](#) and [LiteBlue](#) pages to establish your MFA preferences.

Question: Am I required to have a postal cell phone for MFA?

Answer: No, you can use any phone for MFA.

Establishing your MFA security methods

Question: Why can't I sign in to LiteBlue?

Answer: After January 15, you will be unable to access LiteBlue until you establish your MFA preferences. Please refer to the User Guide and/or Videos posted on the MFA [Blue](#) and [LiteBlue](#) pages for further instructions.

Question: I am trying to reset my SSP password but do not know the answers to my security question. What can I do?

Answer: Follow the step-by-step instructions in the User Guide posted on the MFA [Blue](#) and [LiteBlue](#) pages to establish your MFA preferences.

Question: What should I do if I do not have Google Authenticator or OKTA Verify on my smartphone?

Answer: To utilize these MFA preferences, you must download the application from your smartphone's App Store. Please refer to the User Guide and/or Videos posted on the MFA [Blue](#) and [LiteBlue](#) pages for instructions on how to download these options. Alternatively, you can select the "Phone" MFA option, which does not require a smartphone.

Question: What if I do not have a smartphone?

Answer: If you do not have a smartphone, you can select the "Phone (Voice)" MFA option and utilize any phone to include a landline. This MFA method allows you to proceed without the use of a smartphone by receiving your verification code via a voice message in the form of a phone call. Additionally, if your phone receives text messages, you may select the "Phone (SMS)" MFA option as well.

Question: If I am using a postal smartphone, where do I find the Google Authenticator or OKTA Verify applications?

Answer: If you are utilizing a postal smartphone, OKTA Verify and/or Google Authenticator can be found on the USPS AppStore on those devices. You may utilize the search feature to locate both applications.

Question: When setting up Google Authenticator or OKTA Verify on my smartphone, how do I scan the QR code?

Answer: When establishing OKTA Verify or Google Authenticator you must select "OK" when your phone notifies you that "OKTA Verify" or "Google Authenticator" would like to access the camera. Enabling this

feature within the application will automatically enable you to point the camera on your phone at the QR code and scan it.

Question: Does it matter what type of smartphone I have? (iOS, Android)

Answer: No, you can use either an iPhone (iOS) or Android model smartphone. Please note: The screenshots in the User Guide and Videos are from an iOS device. If you are utilizing an Android smartphone, your screen may appear slightly different. However, the steps for authentication remain the same.

Question: How can I change my MFA settings (to include my phone number on file)?

Answer: To change your previously established MFA settings, select the *“Self-Service Profile”* link on the LiteBlue sign in page or under HR Apps in LiteBlue. For detailed instructions please utilize the User Guide and refer to the *“How to access your Self-Service Profile”*.

Accessing your Self-Service Profile (SSP)

Question: How do I access my SSP?

Answer: After March 20, 2023, SSP is being relocated to LiteBlue to further protect your personal information. After March 21, 2023, you can access your Self-Service Profile via the following options:

- *“Self-Service Profile”* link on the LiteBlue sign in page.
- *“Self-Service Profile”* link under Employee Apps on the LiteBlue home page.
- *“Self-Service Profile”* link under Resource Index on the LiteBlue home page.
- *“Self-Service Profile”* tab on the apps page in LiteBlue.

For detailed instructions please utilize the User Guide and refer to the *“How to access your Self-Service Profile”*.

Question: Why does my SSP look different?

Answer: After March 21, 2023, SSP is being relocated to LiteBlue to further protect your personal information. The new SSP portal has been redesigned and simplified to include all your information in one place.

Question: Why do I have to set up MFA to access my SSP?

Answer: After March 21, 2023, MFA is required for access to SSP to further protect your personal information from unauthorized access and misuse.