

# MFA (Multi-Factor Authentication) Requirement

## Reference Guide



### Table of Contents

**MFA Requirement** ..... 1

**Different Authentication Methods** ..... 1

**Authenticator Application** ..... 1

    How to – Set-up an Authenticator Application ..... 1

**Email** ..... 5

    How to update Email Address: ..... 5

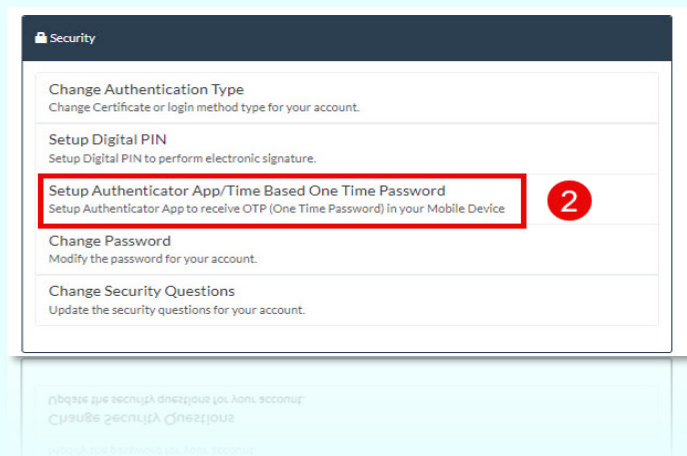
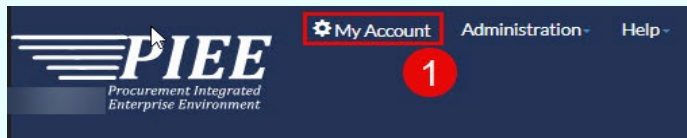
**MFA Login Process** ..... 7

<b>MFA Requirement</b>	<p>In addition to traditional login credentials, PIEE mandates the setup of at least one authentication method to enhance account security. This requirement for Multi-Factor Authentication (MFA) is necessary when logging in with a user ID and password. However, MFA is not required for users logging in with Common Access Card (CAC) or software certificates. This critical layer of protection significantly safeguards sensitive information, ensuring that only authorized users can access accounts and reducing the risk of unauthorized access.</p>
<b>Different Authentication Methods</b>	<p>It is encouraged that users add two authentication methods to their account: an authenticator application and email. This approach ensures that if access to the primary method, such as a phone, is lost, recovery can still occur through a secondary option. This dual strategy provides greater flexibility and peace of mind, catering to diverse individual and organizational needs. Implementing these methods not only strengthens account security but also facilitates easier recovery in case of issues. Each method has its own advantages depending on specific preferences. Below are descriptions of two common MFA methods, along with their pros and cons, to assist in making an informed decision.</p> <ul style="list-style-type: none"> <li>• <a href="#">Authenticator Application</a></li> <li>• <a href="#">Email</a></li> </ul>
<b>Authenticator Application</b>	<p>Authentication applications are tools that users install on their devices to generate secure, time-sensitive one-time passcodes (OTP) for account sign-ins. When a user attempts to access their PIEE account, they first enter their login credentials. Then, the system prompts for a unique six-digit OTP code from the authentication app. This code, which refreshes every 30 seconds, is essential to complete the login process. By requiring both the password and the constantly changing OTP, this method adds an additional layer of security, effectively preventing unauthorized access to the account. The combination of these two factors greatly enhances overall account protection.</p> <p><b>Pros:</b> Stronger Security, Offline Accessibility, convenience, easy access, App is free to use, Phishing resistance.</p> <p><b>Cons:</b> Smartphone required, Device loss, Phone malfunction, App deletion, App availability.</p> <p><b><u><a href="#">How to – Set-up an Authenticator Application</a></u></b></p> <p><b>Set-up:</b> This is a onetime set-up process. Please follow these recommended steps to download and install one of the supported applications and configure it to work with user's PIEE account.</p> <p><b>Step 1:</b> Choose a device, such as a computer or mobile device (phone or tablet), on which user can install apps.</p>

**Step 2:** Download and install any one authentication app which supports Time-Based One-Time Password (TOTP) from either the Apple App Store or the Android Google Play store to the chosen device. Please use the appropriate application that is compliant within your organization and preferably one that is recommended by the DoD. Some popular options include:

- **MS Authenticator with Passkey**
- **Okta Verify with Fastpass**
- **Army Mobile-Connect (MC) MFA**

**Step 3:** Log in to **PIEE**. Navigate to **My Account > Setup Authenticator App/Time-Based One-Time Password**.



**Step 4:** Enter the current **PIEE password**, click the **Submit** button to generate **Secret key** and **QR code** scan for TOTP. Sample screenshots are provided below.

### Setup Authenticator App

#### Prerequisite -

- Download An Authenticator App which supports Time-based One Time Password from either the Apple App Store or the Android Google Play store. These applications are typically free of cost. When selecting an authenticator app, please use one that is compliant within your organization and preferably one that is recommended by the DoD. Examples of mobile applications which support TOTP.
  - MS Authenticator with Passkey
  - Okta Verify with Fastpass
  - Army Mobile-Connect (MC) MFA

#### Setup -

- Step 1. Enter your current password
- Step 2. Click on the 'Submit' button to generate secret key for TOTP

Current Password \*

•

✓ Submit

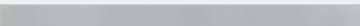

🏠 Home

#### Buttons:

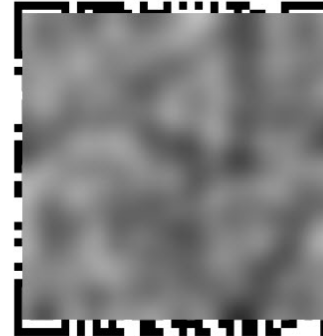
- Submit
- Home


Time-based One Time Password (TOTP) generated successfully

## Setup

- Your Secret Key is  
- Mobile Device Step 1: Download An Authenticator App which supports Time-based One the Android Google Play store. These applications are typically free of cost. When selecting an authenyour organization and preferably one that is recommended by the DoD.  
Examples of mobile applications which support TOTP:
  - MS Authenticator with Passkey
  - Okta Verify with Fastpass
  - Army Mobile-Connect (MC) MFA
- Mobile Device Step 2: Open the App from your mobile device
- Mobile Device Step 3: Follow the app guideline to add account. For the most apps, you jusce.
  - You can either manually type in the **Secret Key** displayed above OR scan the QR code
  - You don't need to provide your e-mail address in the app. You can just type 'piee' or
  - For MS Authenticator with Passkey - when adding account, choose 'Other' as type c
- You can use the code from this mobile app whenever there is a need to login or sign a docu
- When it's time for a signature, you will also receive the OTP via e-mail. You will have optionobile application.
- You do not need an internet connection on your mobile device in order to use these apps.
- **NOTE: The PIEE Help Desk does not handle troubleshooting for mobile application issu**

Your QR Code



 Download QR Code

 Home

### Buttons:

- Download QR Code
- Home

Email notification will be sent once user successfully sets up the authenticator app as shown in the screenshot below.

## PIEE Authenticator App Setup



To

This email was generated in MoonPiee - CACI Development environment. If you are a PRODUCTION user, then please ignore it.

Your PIEE - Authenticator App has been set for User ID [REDACTED].

If you did not make these changes please contact your Group Administrator or the DISA Help Desk.

Please contact your Group Administrator or the Ogden Help Desk if you have any questions or concerns.

THIS IS A SYSTEM GENERATED EMAIL MESSAGE, PLEASE DO NOT RESPOND TO THIS EMAIL.

### Step 5: Setting Up an Account in the Authenticator App:

1. **Open the App:** Launch any of authenticator apps that is mentioned above on a mobile device or tablet.
2. **Add an Account:** Follow the app's instructions to add a new account. Typically, it can be done this by tapping the '+' icon.
3. **Configure the Account:**
  - a. **Manual Input:** Enter the Secret Key provided.
  - b. **QR Code Scan:** Alternatively, scan the QR code to configure the account automatically.
4. **Check the Profile:** Ensure a profile labeled with the PIEE username is visible.
5. **Start Generating TOTP:** The app will begin generating TOTP Passwords for secure access.

## Email

Email-based Multi-Factor Authentication (MFA) enhances account security by requiring both a password and a One-Time Password (OTP) sent to a registered email address. This OTP, valid for 15 minutes, ensures that even if the password is compromised, unauthorized access to the account is prevented.

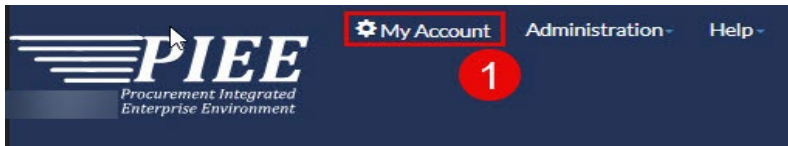
**Pros:** Simple to set up, user-friendly, no app required, cost-effective

.

**Cons:** Email account vulnerability, delay delivery issues, Internet access required.

### How to update Email Address:

1. Log in to **PIEE**.
2. Navigate to **My Account > User**.



My Account

Profile

User  
View/Edit the user profile information.

EB POC  
View the user's EB POC information.

Company  
View/Edit the user's company information.

3. Update Email address, click the **Submit** button.

Email \* Confirm Email \*

Commercial Telephone ! Extension Intl Country Code and Phone !

Citizenship \*

US

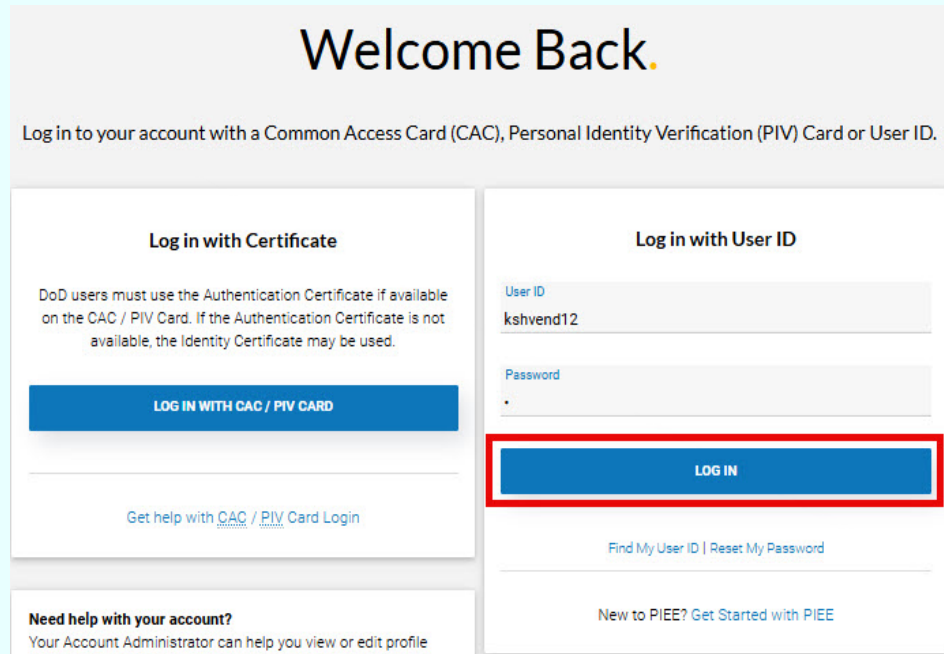
Submit Cancel Help Justification/Attachments

*Buttons:*

- Submit
- Cancel
- Help
- Justifications/Attachments

## MFA Login Process

1. **Initiate Login:** Navigate to the **PIEE** login page.
2. **Input Credentials:** Enter the username and password in the specified fields, click the **LOG IN** button.



The screenshot shows the PIEE login interface. At the top, it says 'Welcome Back.' followed by 'Log in to your account with a Common Access Card (CAC), Personal Identity Verification (PIV) Card or User ID.' Below this are two main login sections. The left section is titled 'Log in with Certificate' and contains text about DoD users and a blue button labeled 'LOG IN WITH CAC / PIV CARD'. The right section is titled 'Log in with User ID' and contains input fields for 'User ID' (with the value 'kshvend12') and 'Password' (with a masked character). Below these fields is a blue button labeled 'LOG IN', which is highlighted with a red rectangular border. At the bottom of the right section, there are links for 'Find My User ID | Reset My Password' and 'New to PIEE? Get Started with PIEE'. At the bottom left, there is a section titled 'Need help with your account?' with the text 'Your Account Administrator can help you view or edit profile'.

### Buttons:

- LOG IN
3. **MFA Prompt:** Upon successful entry of credentials, a prompt will appear requesting a second form of authentication. Users will be asked how they would like to receive the OTP. Options typically include:
    - Email
    - Authenticator App



## Multifactor Authentication(MFA)

### How would you like to receive your one-time code?

We are going to send you a temporary code for security. Choose how you want to receive the code.



Email:



Authenticator App

Help

Close

#### Buttons:

- Email
- Authenticator App
- Help
- Close

4. **Email-based Method:** If the user selects **Email** as his or her preferred factor for MFA, the system will send an OTP to the email address that is linked to the user's account and will not prompt the user for a code from the authenticator application. Retrieve the OTP from the user's registered email, enter it in the designated field, and click the **LOG IN** button to complete the authentication process.

## PIEE - OTP

1



To

This email was generated in MoonPiee - CACI Development environment. If you are a PRODUCTION user, then please ignore it.

Your OTP:

Use the code above to perform multi-factor authentication in PIEE suite.

This is a one-time code and will expire in 15 minutes.

This code was generated at 2024/12/05 15:35:15UTC

THIS IS A SYSTEM GENERATED EMAIL MESSAGE, PLEASE DO NOT RESPOND TO THIS EMAIL.

## Multifactor Authentication(MFA)

2

Info: As of 2024/11/26 19:46:12 UTC, an email was sent to your email account with a One-Time Password (OTP). This password will expire in 15 minutes.



OTP \*

\*\*\*\*\*

We have sent you the OTP to email:

Please wait seconds to resend OTP.



LOG IN

Go Back

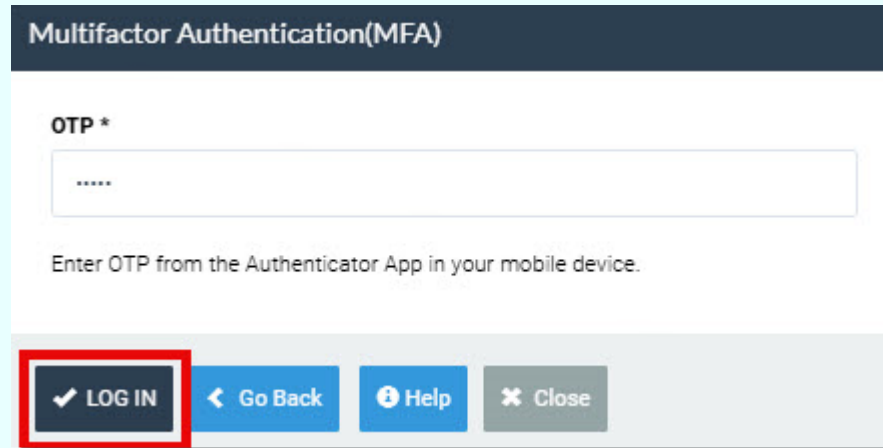
Help

Close

*Buttons:*

- *LOG IN*
- *Go Back*
- *Help*
- *Close*

5. **Authenticator app-based Method:** If the user selects the **Authenticator App** as their preferred MFA method, the system will prompt them to enter the **OTP** from the approved Authenticator App, and no email-based OTP will be sent. Retrieve the OTP from the selected app and enter it in the designated field. Click the **LOG IN** button to complete the authentication process.



*Buttons:*

- *LOG IN*
- *Go Back*
- *Help*
- *Close*

6. **Access Account:** After successful verification of the authentication code, access to the user's PLEE account will be granted.
7. **Troubleshooting:** If the code is not received, verify the network connection, check the Spam, or junk folder, and ensure that the email information is correct. Alternatively, click on **Re-send the OTP via Email** link for a new OTP, or reinstall the authenticator app.