Version 2 | December 18, 2024

Confidential: For internal use only

CARES

Civil Adjudication and Response Solution

First Time Login Guide

ACCESSING THE SOLUTION

This section covers:

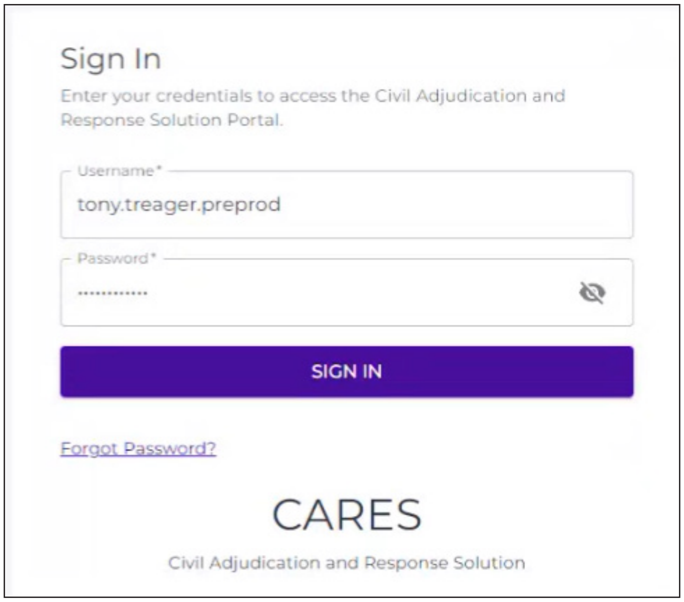
- First Time Login
- Multi-factor Authentication (MFA)
- Logging On
- Changing Your Password

First Time Login

The login process may vary by system configuration. Upon first receiving access, the user will receive an email with their login information and a temporary password.

- The first time user will use the temporary password they were provided to log in and receive a prompt to change their password.
- Temporary passwords set by administrators expire in 7 days
- Password requirements:
- Minimum length of 16 characters
  - Contains at least 1 number
  - Contains at least 1 special character
  - Contains at least 1 uppercase letter
  - Contains at least 1 lowercase letter
- Username is case sensitive.

1. On the login screen, enter the provided/assigned username and provided temporary password.



Sign In

Enter your credentials to access the Civil Adjudication and Response Solution Portal.

Username*: tony.treager.preprod

Password*: ············

2. During the first login, the user will be required to set up a new password.

3. After establishing a new password, the user will be returned to the login screen and is required to login with the newly established password.

4. The user will then complete the setup of multi-factor authentication (MFA) tools. *See the next section.*

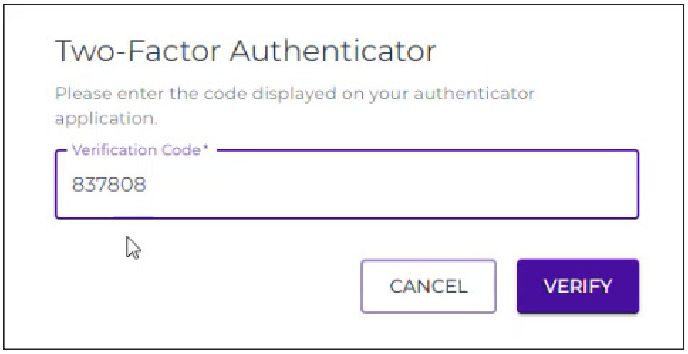
Multi-Factor Authentication (MFA)

After setting up a password, the user will be required to enable MFA. The user will set up MFA by scanning the displayed QR code with an authenticator application from a smartphone. *Note: An authenticator application is required to authenticate that the user is who they claim to be.*

1. After entering their username and password information, the user will be presented with a two-factor authentication (2FA) QR code.

2. The user will scan the QR code with their selected authenticator application. *See further information and example screenshots below.*

3. Once set up, the user may be required to login again. Each time the user logs in, the 2FA code will be required.



Two-Factor Authenticator

Please enter the code displayed on your authenticator application.

Verification Code*: 837808

GUIDANCE ON AUTHENTICATOR APPLICATION SETUP

An authenticator application is a software-based tool that provides an additional security layer to protect your online accounts from unauthorized access. It generates time-based one-time passwords (TOTP) or event-based codes used as a second factor in the MFA process — along with your regular password. This means that even if someone manages to obtain your password, they still need the unique code generated by the authenticator app to gain access to your account.

Downloading an authenticator application is easy. If you have a phone or tablet, follow the steps on the next page.

Select an Authenticator App

Recommended authenticator apps are listed below. Your selection will depend on your device and personal preferences.

- **Okta Authenticator**: As an identity management service available for Android and iOS devices, Okta connects any person with any application on any device. Features include provisioning, single sign-on (SSO), Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) integration; the centralized deprovisioning of users; MFA; mobile identity management and flexible policies for organization security and control.
- **Google Authenticator**: Developed by Google, this app is available for Android and iOS devices. Supports MFA for various online accounts, including Google accounts, social media and many other popular services.
- **Duo Mobile**: Developed by Duo Security, this trusted MFA solution provider available for Android and iOS devices supports MFA for Duo-protected accounts, as well as other services that use Time-based One-Time Password (TOTP) or event-based One-Time Password (OTP) protocols.
- **Microsoft Authenticator**: Available for Android and iOS devices, this app supports MFA for Microsoft accounts and other services that use the TOTP protocol.
- **Authy**: Available for Android or iOS, Authy allows you to synchronize your accounts across multiple devices.
- **LastPass Authenticator**: Available for Android and iOS devices, this app provides an additional security layer for LastPass accounts, as well as other services that support TOTP-based authentication.
- **YubiKey Authenticator**: Available for Android and iOS devices, this app is designed specifically for YubiKey hardware security keys, which are physical devices that provide an additional security layer. Supports TOTP and Hash-based Message Authentication Code One-Time Password (HOTP) protocols.

Download and Install the Authenticator App

If you have a smartphone, go to your device's app store, e.g., Google Play Store (Android) or App Store (iOS), search for the authenticator app of your choice and download and install the app on your phone.

Set up the Authenticator App

After installing the authenticator app on your device, open it and follow the setup instructions. Typically, to link your authenticator app to your account, you will need to scan a QR code or enter a secret key provided by the service for which you want to enable 2FA.

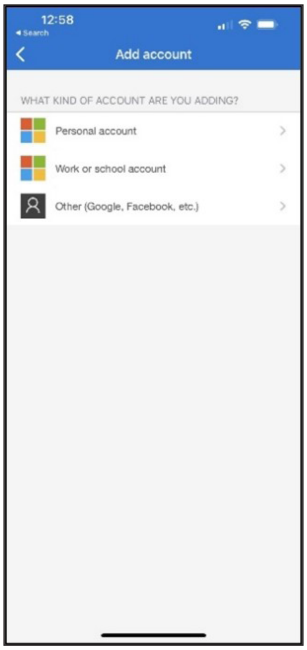
Verify the Authenticator App

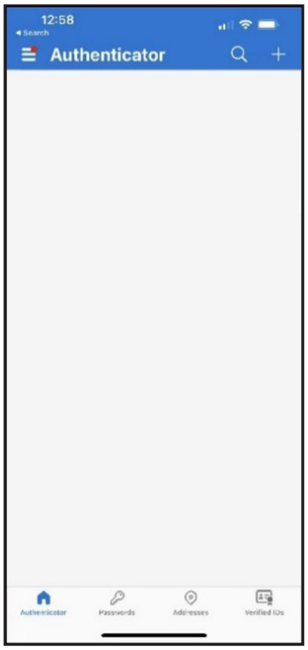
After setting up the authenticator app, you will need to verify the app to ensure it is working properly. This usually involves entering an app-generated code into the service you are trying to secure. This step confirms that the authenticator app is generating the correct codes and ready to be used as a second factor in the authentication process.

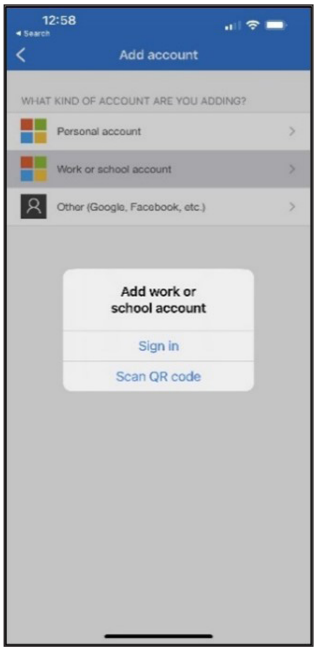
Use the Authenticator App

After setting up and verifying the authenticator app, it is ready to use. When you log into a 2FA-enabled account, you must enter the code generated by the authenticator app, in addition to your regular password. The app will generate a new code every few seconds or after each use, ensuring that the second factor is dynamic and constantly changing and adding an extra security layer to your accounts.

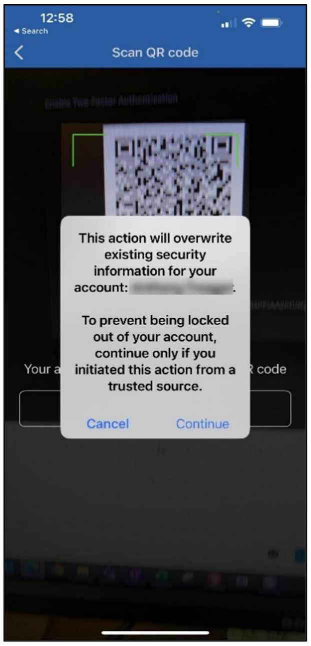
Example images from the Microsoft authenticator app are below. Please refer to the instructions on your specific app and follow the onscreen prompts. With the authenticator app open on your smartphone, select the **"+" Add Account** function:


12:58
◂ Search
Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)



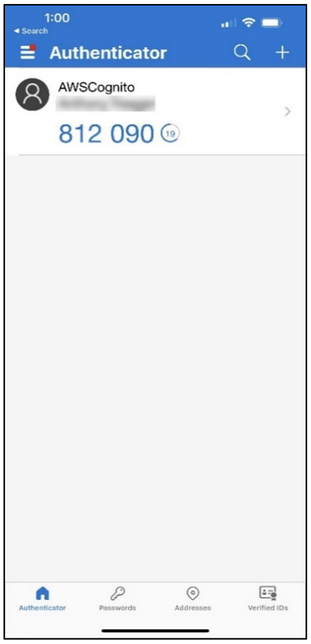

12:58
◂ Search
Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)
Add work or school account
Sign in
Scan QR code

Use the authenticator app to scan the provided QR code and obtain an access code:



This action will overwrite existing security information for your account: [redacted].

To prevent being locked out of your account, continue only if you initiated this action from a trusted source.



Enter the access code in the CARES portal to complete the setup of the account and MFA tool.

Logging On

The login procedure may vary by system configuration.

1. On the login screen, enter the assigned **Username**.

2. The user also will enter the established password in the appropriate box.

3. The user will complete the MFA process to confirm the user's identity.

SESSION TIMEOUT DUE TO INACTIVITY

1. For security purposes, if the user is inactive for a period of **15 minutes**, the system is configured to inform the user that they will be automatically logged out after a 5-minute countdown period.

2. The user has the option to interact with the prompt in order to maintain activity.

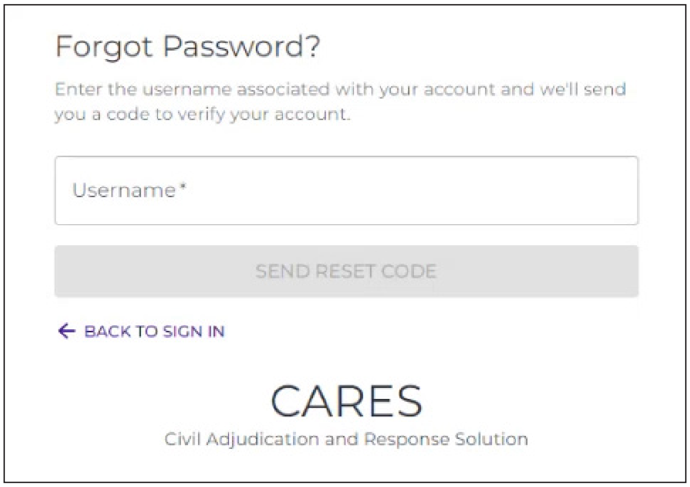
3. Once the 5-minute timer counts down without interaction, the system will log out the user and return them to the login screen where the user will be required to login again.

Changing Your Password

FORGOT PASSWORD

If a user forgets their set password, the solution offers a recovery process for the user to change the password from the main login page.

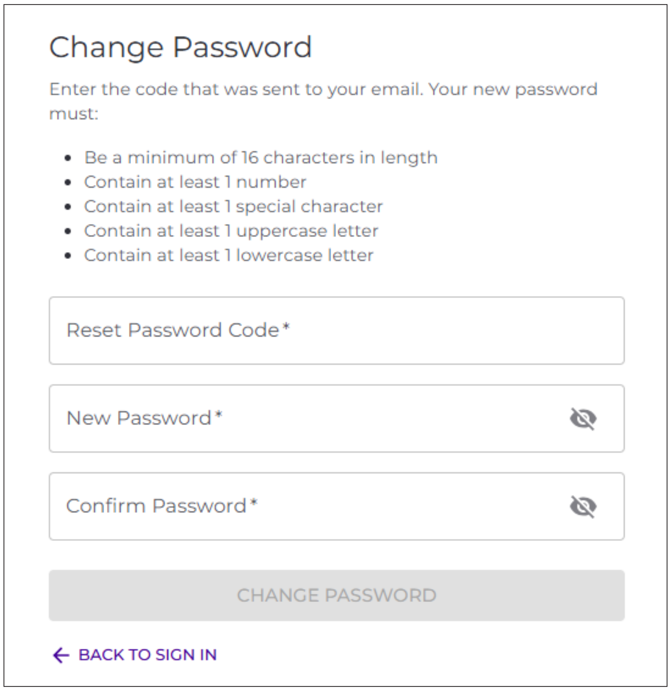
1. On the main login page, the user will select the **Forgot Password** link.



Forgot Password?

Enter the username associated with your account and we'll send you a code to verify your account.

2. The user will enter the provided/assigned username where prompted. *The user must still have access to the email address originally set up with the account.*



Change Password

Enter the code that was sent to your email. Your new password must:

- Be a minimum of 16 characters in length
- Contain at least 1 number
- Contain at least 1 special character
- Contain at least 1 uppercase letter
- Contain at least 1 lowercase letter

3. The CARES system will deliver a **Confirmation Code** to the email address on file.

4. The user will enter the **Confirmation Code** in the appropriate box as prompted on the screen. *See example screen above.*

5. The user will enter a new password with the following requirements:
   a. Minimum length of 16 characters
   b. Contains at least 1 number
   c. Contains at least 1 special character
   d. Contains at least 1 uppercase letter
   e. Contains at least 1 lowercase letter

6. The user will be required to re-enter the new password. The entered values must match.

7. The user will then proceed to log on to the system.