

Clarity HMIS Training

NEW MULTI-FACTOR AUTHENTICATION (MFA)

Link to the training video:

COMING SOON

Link to Bitfocus Help Desk Article: <https://help.bitfocus.com/auth0-for-clarity-human-services-toolkit>

Overview

Bitfocus is moving to a new multi-factor authentication that requires two separate pieces of information to confirm the identity of a user attempting to log in to the system. Just like 2FA, when MFA is enabled, you must enter both a password and then verify your identity with one of the following methods:

- One Time Password – Receive a 6-digit verification code from an Authenticator App like Google Authenticator or Microsoft Authenticator.
- Phone – Receive a 6-digit verification code via text message or voice call. You must have a valid cell phone to receive text messages. You may use a landline to receive the code via voice call.
- Push Notification via Auth0 Guardian App - Provide permission through an app's push notification to log in to Clarity Human Services (HMIS). The app push notification will require installing the Auth0 Guardian App on an individual's cell phone (See below for more information).

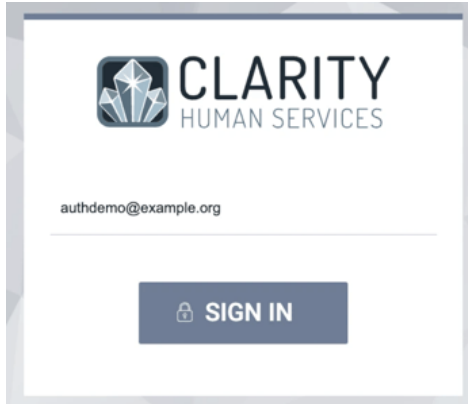
Users will only be required to set up one of these identity verification methods in addition to entering their username and password.

MFA will be enabled for all BRCoC Clarity HMIS users on the LIVE SITE beginning TUESDAY, JULY 14, 2026. MFA is already active on the Clarity HMIS Training Site as of July 1, 2026, so users can practice logging in and setting up MFA before July 14.

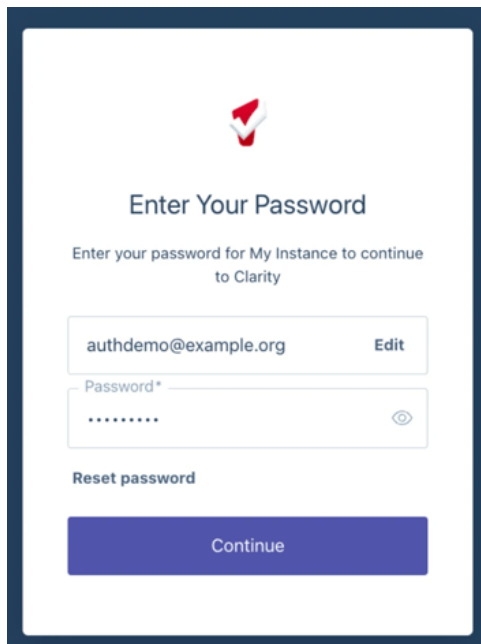
Signing in with Multi-Factor Authentication (MFA) for the First Time

The first time you sign into the Training or Live Site after MFA has been enabled, you will see a new log-in prompt. Please follow the MFA enrollments steps below:

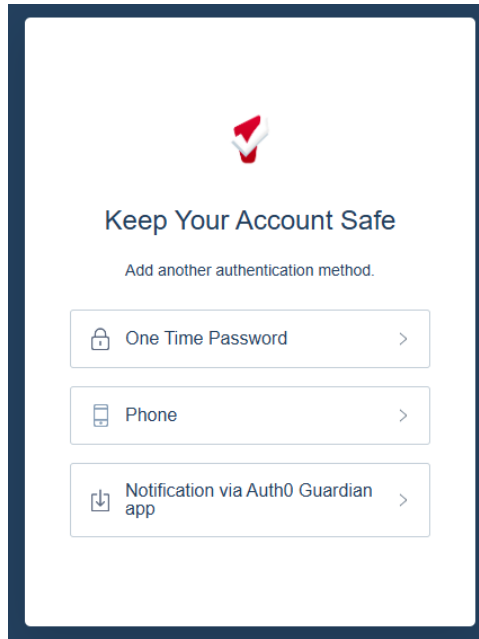
STEP 1: Enter your email address on the Clarity sign-in page:

The image shows the Clarity Human Services sign-in page. At the top, there is a logo for Clarity Human Services. Below the logo, the email address "authdemo@example.org" is entered into a text field. A "SIGN IN" button with a lock icon is positioned below the text field.

STEP 2: Users are redirected to the MFA log-in page, where you will enter your HMIS account password and click “Continue”:

The image shows the "Enter Your Password" page. At the top, there is a red and white logo. Below the logo, the text "Enter Your Password" is displayed. Underneath, it says "Enter your password for My Instance to continue to Clarity". There is a text field for the email address "authdemo@example.org" with an "Edit" link. Below that is a password field labeled "Password*" with a masked password "....." and a toggle icon. A "Reset password" link is located below the password field. At the bottom, there is a large blue "Continue" button.

STEP 3: The first time you log-in, you will be prompted to select your authentication method:



STEP 4: Choose the authentication method you would like to use. Follow the instructions for each method below to set up it up:

1. One Time Password from an Authenticator Apps for Mobile Devices

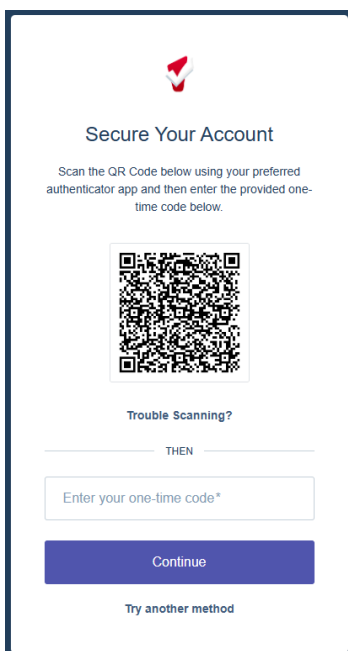
- a. If you choose to generate the one-time 6-digit verification code using an authenticator app, we recommend you install *Google Authenticator* or *Microsoft Authenticator* from your device's app store prior to signing in to Clarity HMIS on the start date. Which one you choose could depend on which email service your organization uses (Google or Microsoft). Please contact your internal IT administrator for their recommendations.
- b. Make sure you have downloaded your chosen authenticator app and signed in with your Google or Microsoft account as applicable.
- c. Click the option for “🔒 One Time Password” in the dialogue box.
- d. Clarity will then display a new dialog box with a QR Code on the screen:



Google Authenticator

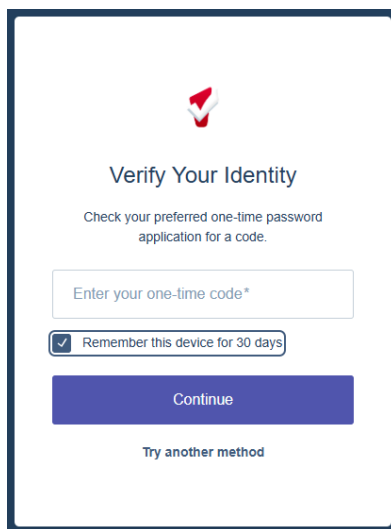


Microsoft Authenticator



The screen displays the BRCoC logo at the top. Below it, the heading "Secure Your Account" is centered. A sub-header reads: "Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below." A square QR code is centered below the text. Underneath the QR code is a link: "Trouble Scanning?". Below this is a horizontal line with the word "THEN" in the center. Underneath the line is a text input field with the placeholder text "Enter your one-time code*". Below the input field is a blue "Continue" button. At the bottom of the screen is a link: "Try another method".

- e. In the authenticator app on your phone, there will be a QR code button or camera button that will open up your camera so you can scan the QR code.
- f. After scanning the QR code, the app will display a 6-digit code. Enter this code in the box that says "Enter your one-time code."
- g. If you would like to skip MFA for 30 days at a time, then check the box next to "Remember this device for 30 days" before you click "Continue." Please only use this feature on laptops, desktops, or mobile devices that are NOT for public use.



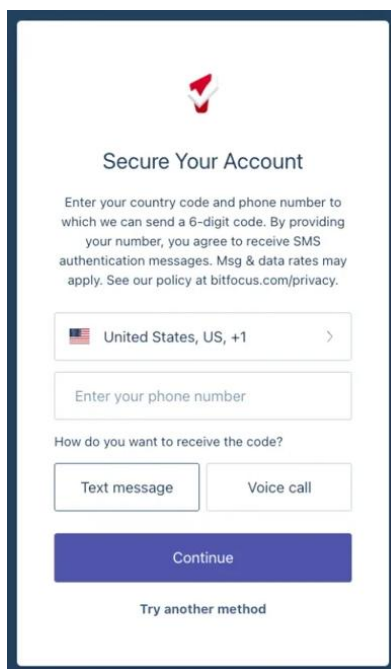
The screen displays the BRCoC logo at the top. Below it, the heading "Verify Your Identity" is centered. A sub-header reads: "Check your preferred one-time password application for a code." Below this is a text input field with the placeholder text "Enter your one-time code*". Underneath the input field is a checkbox that is checked, with the label "Remember this device for 30 days". Below the checkbox is a blue "Continue" button. At the bottom of the screen is a link: "Try another method".

h. This completes your login to Clarity HMIS.

2. Phone

a. Click the option for “Phone” in the MFA dialogue box.

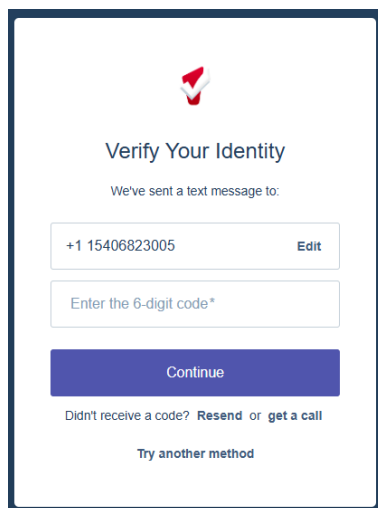
b. Clarity will then display a new dialog box where you can enter the phone number



The screenshot shows a mobile-style dialog box titled "Secure Your Account" with a red logo at the top. Below the title, there is a paragraph of text: "Enter your country code and phone number to which we can send a 6-digit code. By providing your number, you agree to receive SMS authentication messages. Msg & data rates may apply. See our policy at bitfocus.com/privacy." Below this text is a dropdown menu showing "United States, US, +1" with a right arrow. Underneath is a text input field labeled "Enter your phone number". Below the input field is the question "How do you want to receive the code?" followed by two buttons: "Text message" and "Voice call". At the bottom is a large blue "Continue" button and a smaller link "Try another method".

c. After entering your phone number, select whether you would like to receive a 6-digit code via text message or voice call then click “Continue.”

d. A new dialog box will open where you will enter the 6-digit code. Click “Continue.”

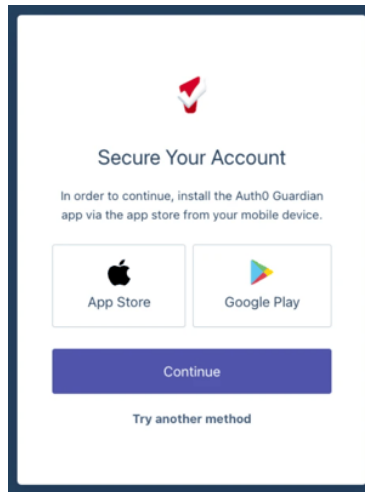


The screenshot shows a mobile-style dialog box titled "Verify Your Identity" with the same red logo. Below the title, it says "We've sent a text message to:". Below this is a text input field containing "+1 15406823005" with an "Edit" link to its right. Underneath is another text input field labeled "Enter the 6-digit code*". At the bottom is a large blue "Continue" button and a smaller link "Try another method". Above the "Continue" button is a link "Didn't receive a code? Resend or get a call".

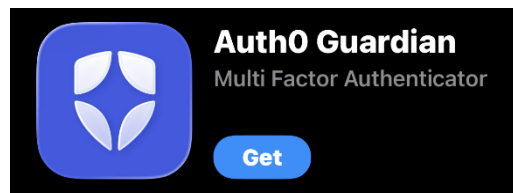
e. This completes your login to Clarity HMIS.

3. **Notification via Auth0 Guardian App**

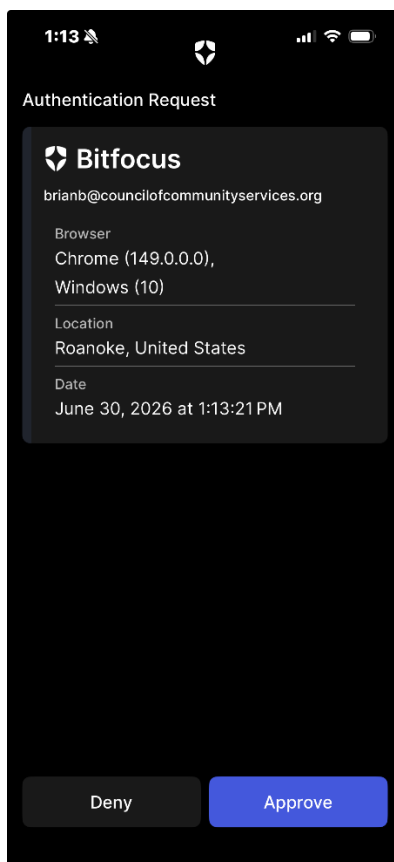
- a. Click the option for “Notification via Auth0 Guardian App.”
- b. Clarity will open a dialog box and ask you to install the “Auth0 Guardian App” from either the Apple App Store or Google Play, depending on what device you have.



- c. Before you click “Continue,” go to the app store on your device and search for the “Auth0 Guardian App.” The app icon will look like the picture below:



- d. After the app is installed on your phone, go back to your browser window and click “Continue.” Clarity will then display a new dialog box with a QR Code displayed.
- e. In the Auth0 Guardian app, click “+Add” in the top right corner. Then click “Scan QR Code” to open your phone’s camera. Use the camera to scan the QR code and Clarity will complete your log-in.
- f. The next time you log in using this method, you will receive a push notification like this:

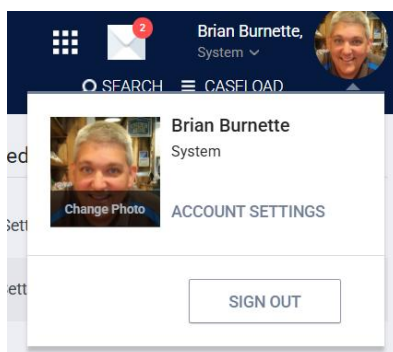


- g. Click “Approve” to complete your log-in to HMIS.

ADDING OR CHANGING MULTI-FACTOR AUTHENTICATION METHODS

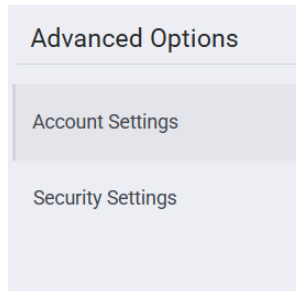
After you have MFA set up, follow the steps listed below if you would like to add or change any of your MFA methods:

1. While logged into HMIS, click on your initials (or profile photo) in the top right corner of the screen:



2. Click “ACCOUNT SETTINGS” to open up your user settings.

3. On the right side of the screen, click “Security Settings” to access your MFA methods:



4. The MFA screen will list the four methods for authenticating your identity during log-in. If you have already set up one of the methods, it will display “ENROLLED” next to that option:

MULTI-FACTOR AUTHENTICATION					
ENROLLED		Email	bria**@coun*****	Enrolled: Jun 30, 2026, 11:07 AM	Last Used:
ENROLLED		Phone (SMS or Voice Call)	XXXXXXXX3005	Enrolled: Jun 30, 2026, 2:31 PM	Last Used: Jun 30, 2026, 2:31 PM
ENROLL		One-Time Password (Authenticator App)	Authenticator App		
ENROLLED		Push Notification (Auth0 Guardian App)	iPhone	Enrolled: Jun 30, 2026, 2:32 PM	Last Used:

5. If you would like to add another MFA method, click “ENROLL” next to the new method and refer to the steps listed above to complete set-up.
6. If you no longer wish to use one of the listed MFA methods, click the  icon next to method to delete it.

If you have any questions or are having trouble logging in or setting up an MFA method, please submit an [HMIS Help Desk Ticket](#).