

Alameda County Continuum of Care

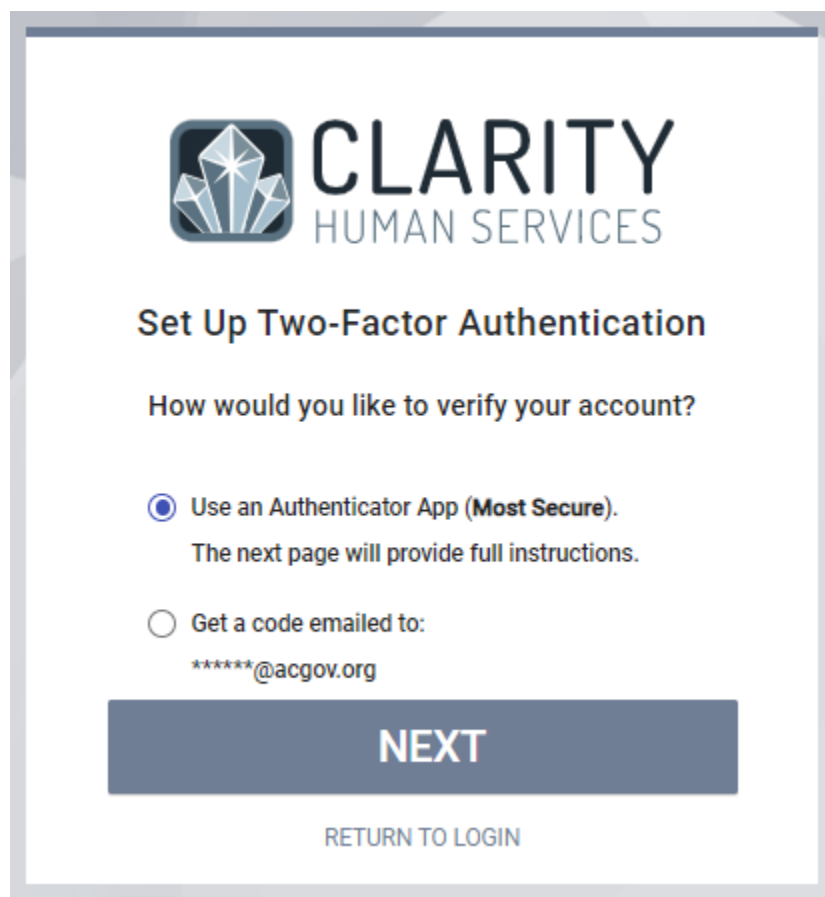
HMIS Two-Factor Authentication (2FA)

Purpose: Two-Factor Authentication (2FA) is a form of multi-factor authentication that requires two separate pieces of information to confirm the identity of a user attempting to log in to the system. When 2FA is enabled, you must enter both a password and a 6-digit verification code to log in to Clarity Human Services. You can receive the verification code through your email account or through an Authenticator App.

There are several authenticator applications available for mobile devices. It is recommend installing Google Authenticator for Android/iOS and Microsoft Authenticator for Windows Phone.


Set-up:

When you log in for the first time with 2FA enabled, you will need to set up your 2FA after entering your username and password.



The screenshot shows a web interface for setting up Two-Factor Authentication. At the top is the Clarity Human Services logo, which consists of a stylized diamond icon and the text "CLARITY HUMAN SERVICES". Below the logo is the heading "Set Up Two-Factor Authentication". The main question is "How would you like to verify your account?". There are two radio button options: "Use an Authenticator App (Most Secure)." which is selected, and "Get a code emailed to:" with the email address "*****@acgov.org" displayed below it. At the bottom of the form is a large blue button labeled "NEXT" and a smaller link labeled "RETURN TO LOGIN".

Use Authenticator App:




CLARITY
HUMAN SERVICES

Set Up Two-Factor Authentication

Download an Authenticator App

Android, iOS and Blackberry – **Google Authenticator**
Windows Phone – **Microsoft Authenticator**

Scan this code with the app



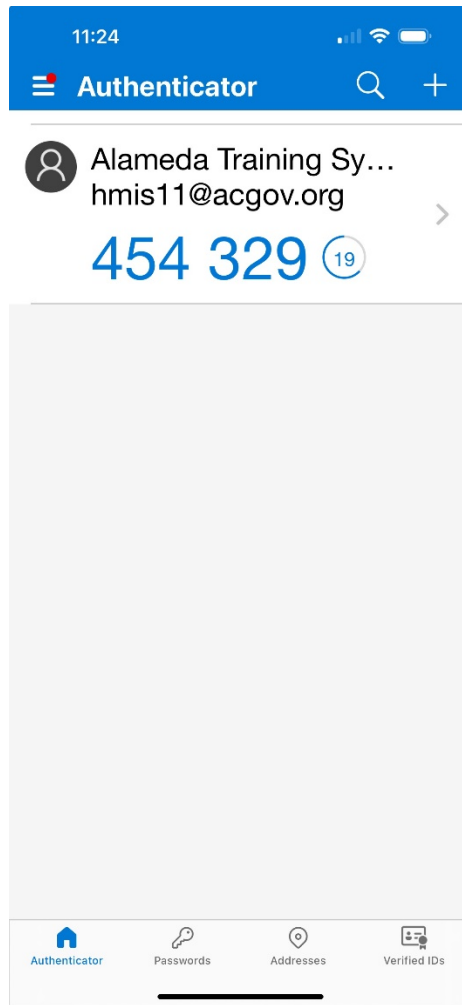
Enter the 6-digit code generated by the app

VERIFY CODE

[RETURN TO CHOOSE METHOD](#)

[RETURN TO LOGIN](#)

From the Microsoft Authenticator:

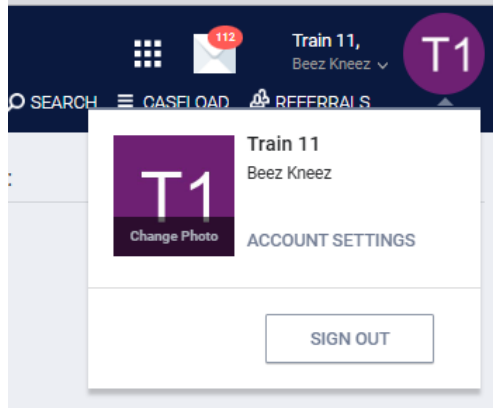


The 6-digit code generated for the user must be entered before it expires. The expiration time frame is 30 seconds on the App Authenticator.

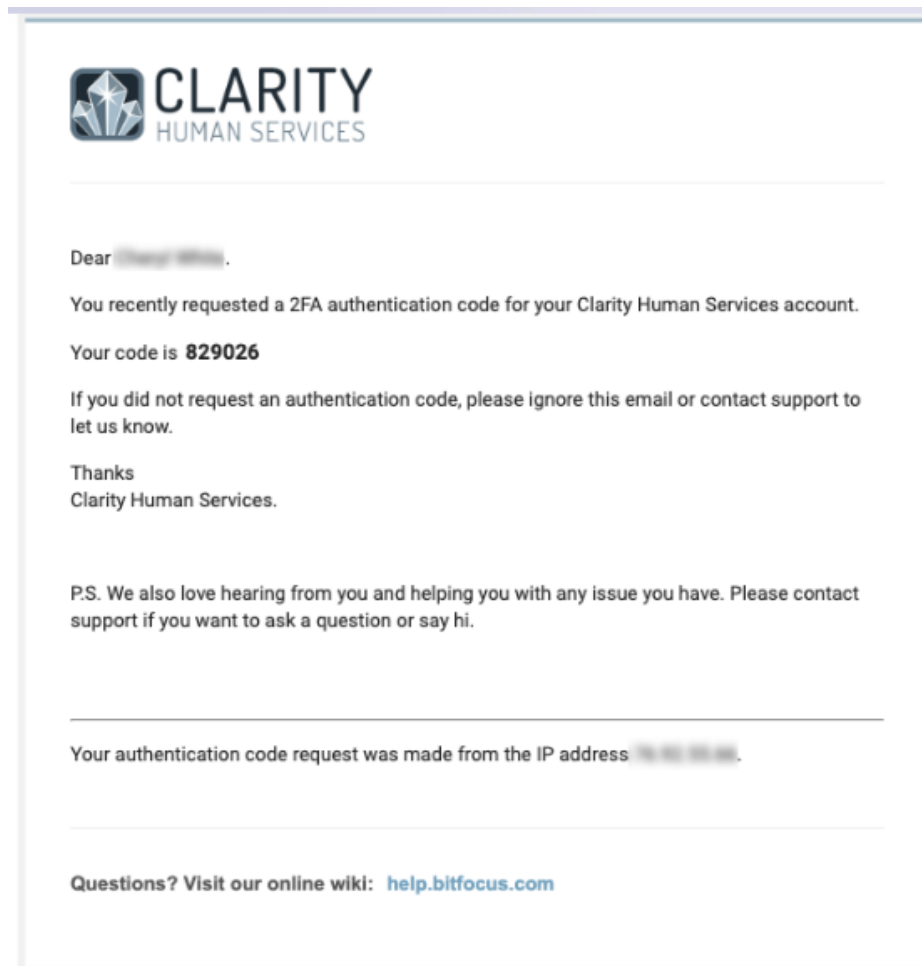
Users who enter an incorrect code more than 5 times in a minute will be locked out of their account.

Code emailed:

The system sends an email containing a 6-digit code to the email address associated with your account. To verify the email address in Clarity:



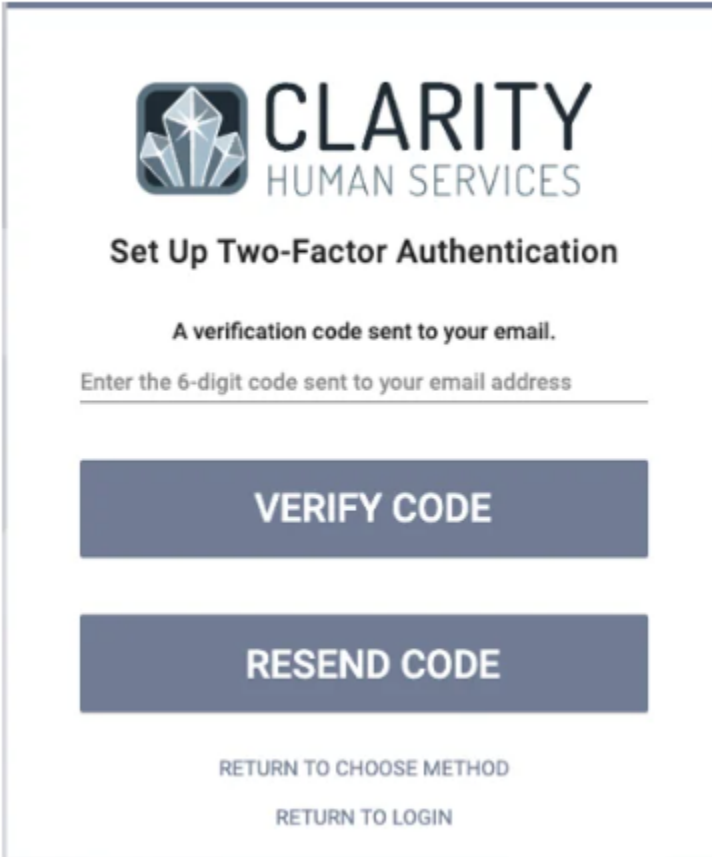
Select Account Settings. Email will display under My Info.



Once you receive the email, enter the code into the dialog box and click *VERIFY CODE* to complete the login process. You may also click *RESEND CODE* to have a new code sent to your email address.

The 6-digit code generated for the user must be entered before it expires. The expiration time frame is between 10 and 20 minutes, depending on the timing of the request.

Users who enter an incorrect code more than 5 times in a minute will be locked out of their account.



The image shows a screenshot of a web interface for setting up two-factor authentication. At the top left is the Clarity Human Services logo, which consists of a stylized diamond icon and the text "CLARITY HUMAN SERVICES". Below the logo is the heading "Set Up Two-Factor Authentication". Underneath the heading is the text "A verification code sent to your email." followed by a prompt "Enter the 6-digit code sent to your email address" with a horizontal line for input. There are two large, dark blue buttons: "VERIFY CODE" and "RESEND CODE". At the bottom of the screen are two smaller, light blue links: "RETURN TO CHOOSE METHOD" and "RETURN TO LOGIN".

If you are unable to receive the email code, please ask your IT department to whitelist the incoming email address (alert@notifications.clarityhumanservices.com) so that it will be marked as a safe sender. Once your IT department has whitelisted the incoming email address, log on and have the code re-sent to your email address.

Unable to access Authenticator/Not receiving emails:

Contact alameda@bitfocus.com