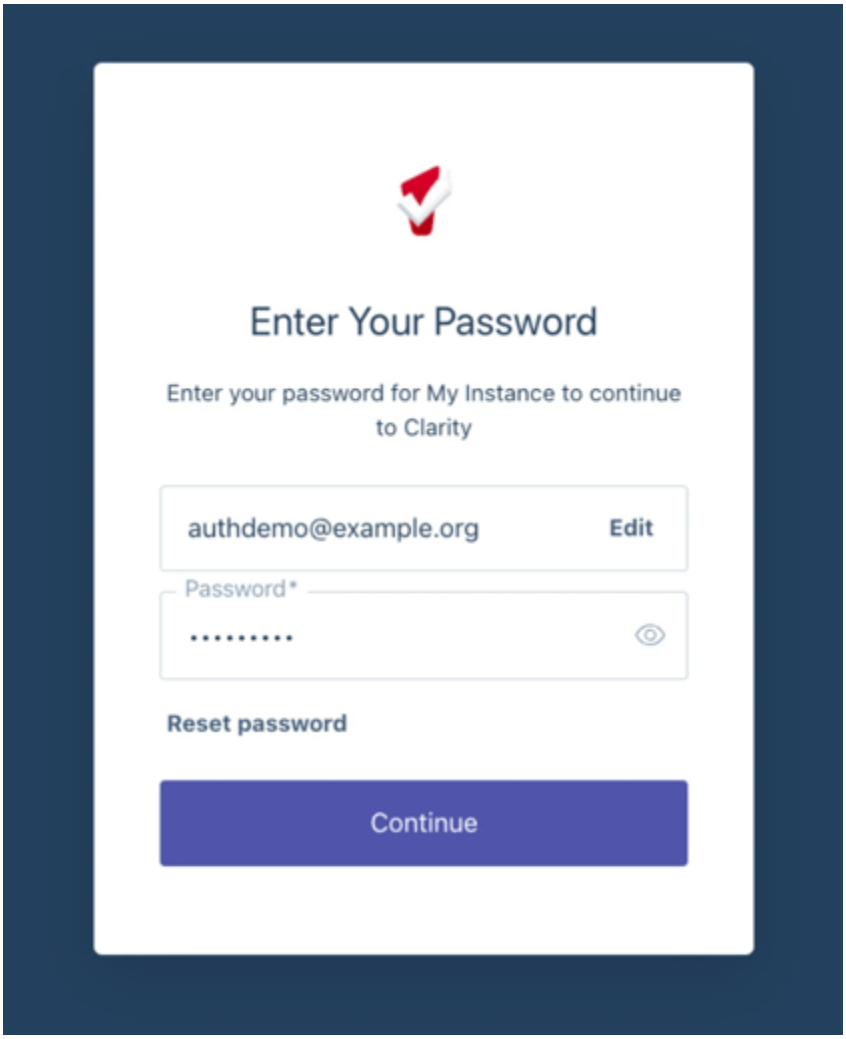
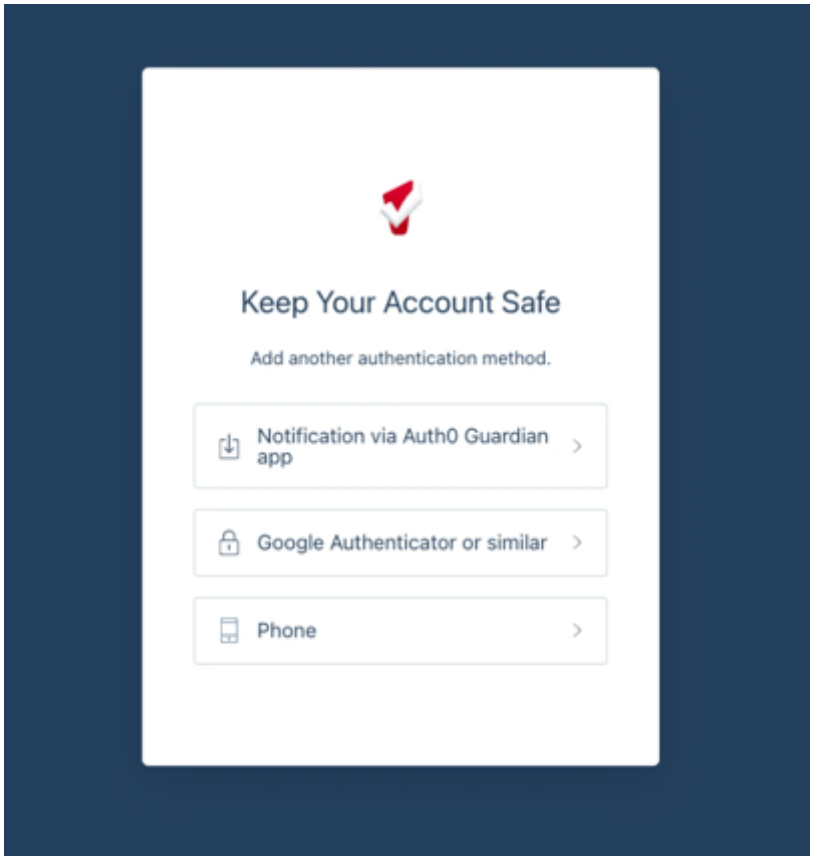
Multifactor Authentication (MFA) Enrollment Steps and FAQ

Step 1: Users enter their email address on the Clarity sign-in page:

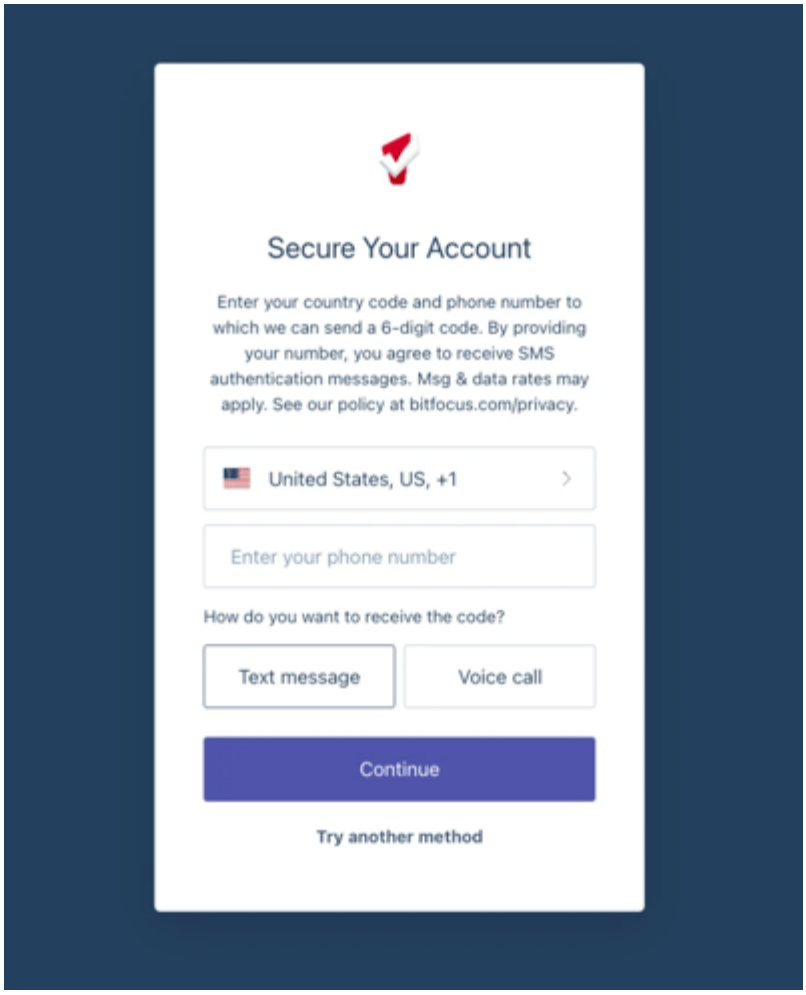
Step 2: Users are redirected to the Auth0 login page, where they enter their Bitfocus account password:



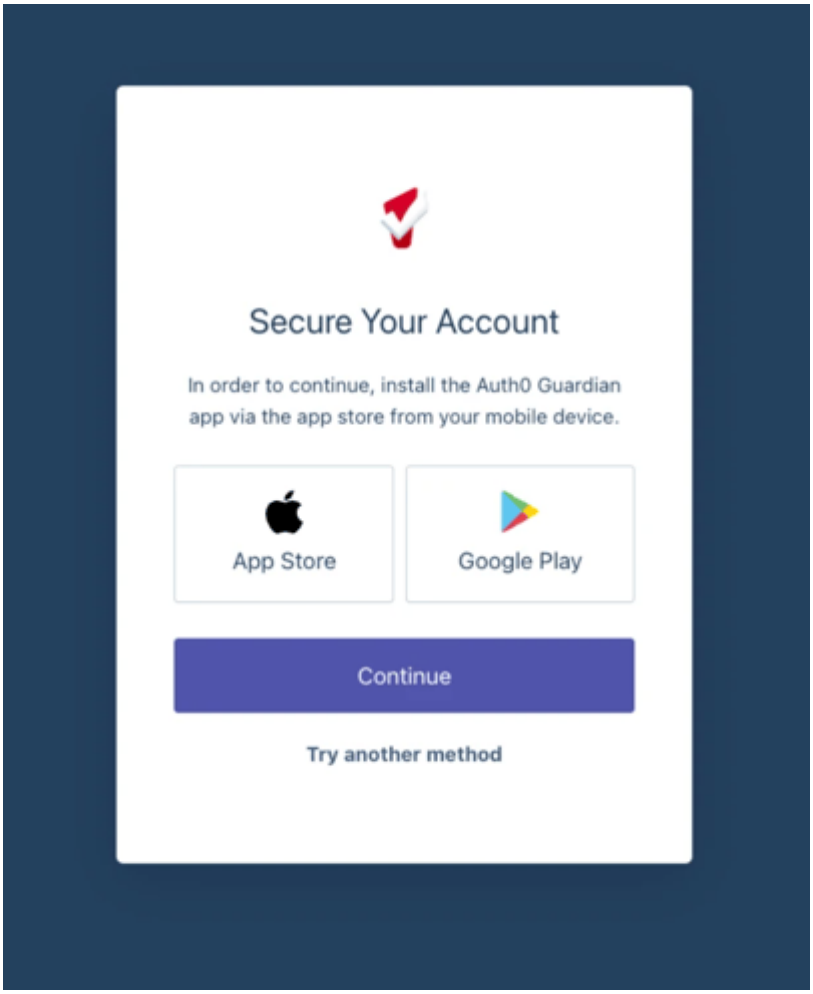
Step 3: Upon first SSO login with Auth0, the user will be prompted to select their authentication method:



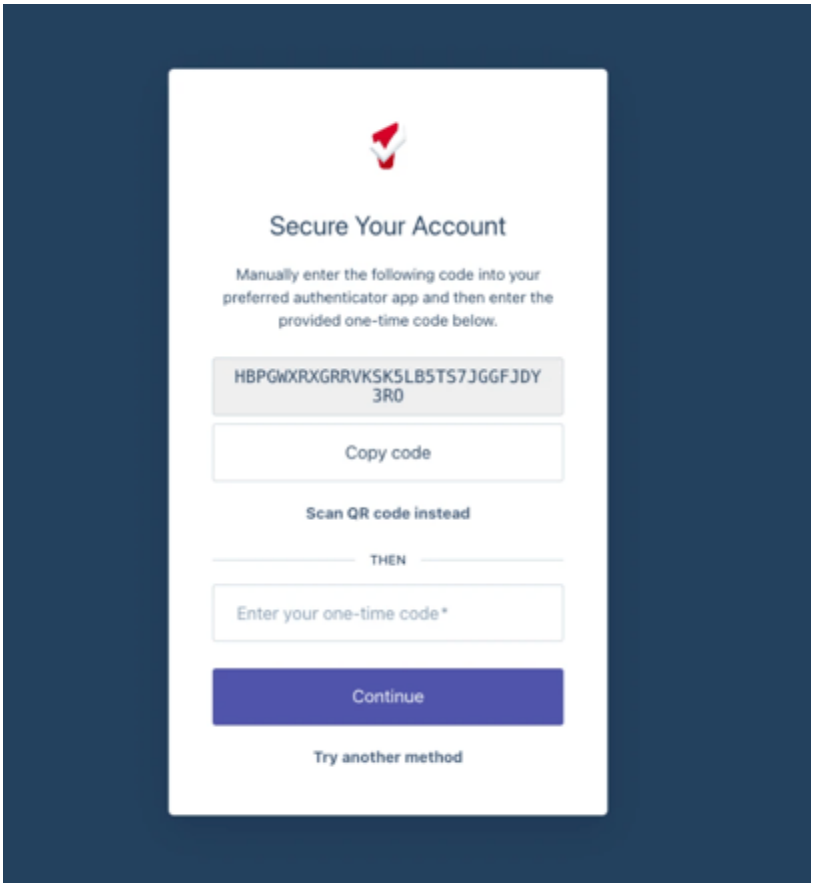
Authentication Methods



Phone Authentication

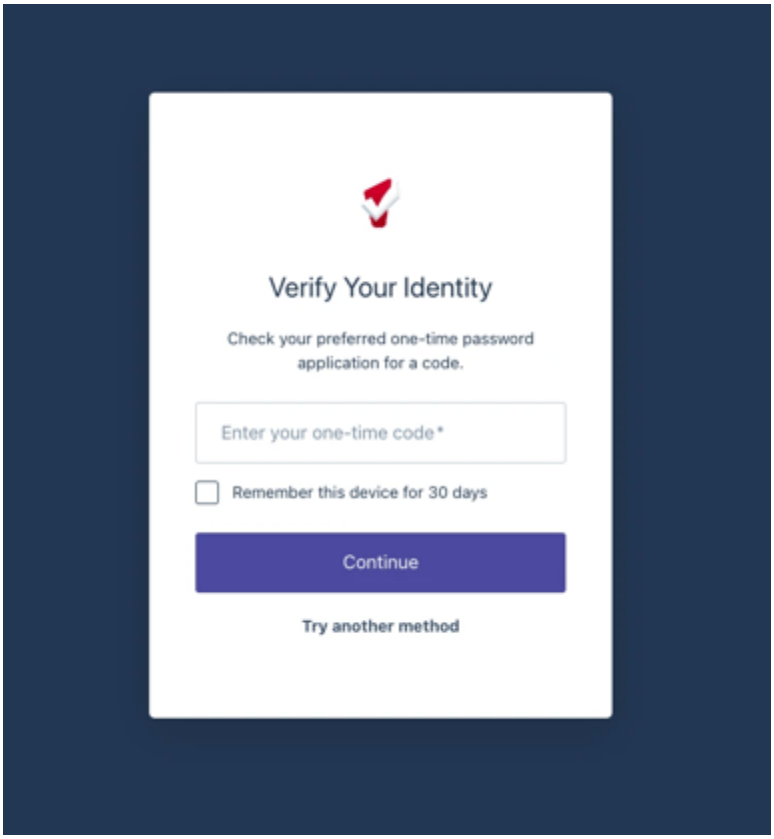


Auth0 Guardian App Authentication



Other Authenticator Apps Authentication

Step 4: Once the authentication method is set up, users will be prompted the next time they need to re-authenticate when they log in:

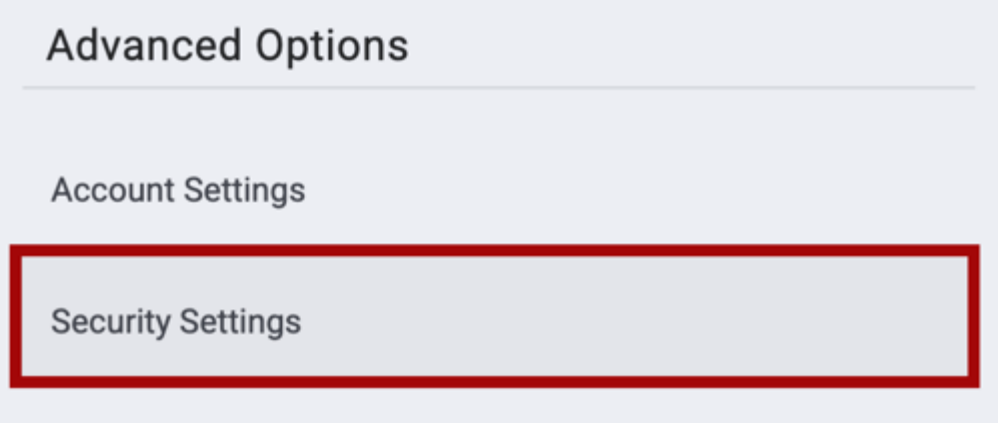


If the **Remember this device for 30 days** option is checked, an MFA challenge will only be presented after a 30-day grace period. If the **Remember this device for 30 days** option is not checked, you will be challenged every time you log in.

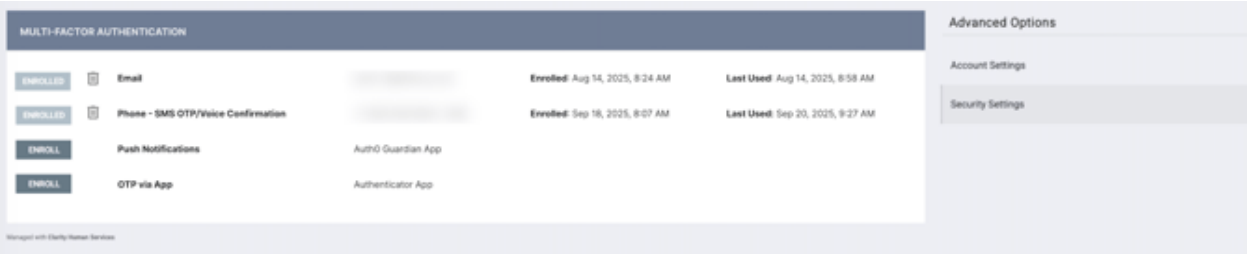
MFA Management for Users

Users can manage their MFA in their staff member Account Settings.

Once the user has logged in, they will click the staff member icon in the upper-right corner, then select **ACCOUNT SETTINGS**. Then they will click **Security Settings** under Advanced Options on the right side panel.



The user will then be on the **MULTI-FACTOR AUTHENTICATION** page. On this screen, they will see all of the available MFA options for them.



If **ENROLLED** is shown next to a factor, a **Delete** icon is provided to delete the factor. Then they can reconfigure that MFA option upon login.

If **ENROLL** is shown next to a factor, the **ENROLL** button will be clickable, and when they click it, a new **Auth0** tab will open, walking them through the enrollment/configuration for that option.

Frequently Asked Questions for Users

Why do I use my email to sign in now?

Email is globally unique and doesn't require users to invent or remember a separate identifier. It also enables built-in account recovery via password reset links sent to your inbox.

What is this new login screen? Why was I redirected to another website?

Users now enter their email on the Clarity sign-in page, which has the same URL as before. They'll then be temporarily redirected to Auth0, which handles the rest of the sign-in process. Once authentication completes, users are automatically sent back to Clarity.

Why am I being asked to register an MFA device?

MFA is now required for all users authenticating to Clarity Human Services and approved third-party applications. On first sign-in after migration, users will be prompted to enroll.

Where did the 2FA toggle in my user settings go?

The per-user 2FA enable/disable option has been removed. MFA is now centrally managed with Auth0, and users can manage their enrolled factors in their Clarity account settings.

What if I've already set up 2FA in Clarity?

Users who had 2FA enabled with Clarity before the change will need to set up their MFA again with Auth0.

What if the phone number on my Clarity user profile is different than the number I use for MFA?

This will not be an issue. Auth0 does not look at the Clarity user profile and only sees the phone number the user provides during login.

How long does "Remember this device" last?

30 days. A single 30-day option has replaced the previous 7/14/30/90-day selector.

Does the new Clarity interface require a separate login?

No. The new Clarity interface continues to authenticate via Clarity, sharing a single Auth0 session so that customers won't see two logins.

Can I use my email address for MFA?

Email can only be used if another authentication method is set up first, and the user does not have access to the phone or authenticator app they set as their primary recovery method. Email cannot be the only/primary authentication method.