

Multi-Factor Authentication

Enabling for all clients starting August 1!





What is Multi-Factor Authentication?

Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Traditionally, when establishing someone's identity there are three basic factors that can be implemented:

- Something you know (Example: Passwords, Security Phrases, Personal Information, etc.)
- Something you have (Example: Cell Phone, key fob, badge, etc.)
- Something you are (Example: Fingerprint, palm print, iris scan, facial recognition)

Multi-factor authentication uses more than one of these factors to validate your identity and ensure you are who you say you are.

Authentication is a common part of our everyday digital lives—whether we're logging into a bank account, shopping online, or accessing personal health records.

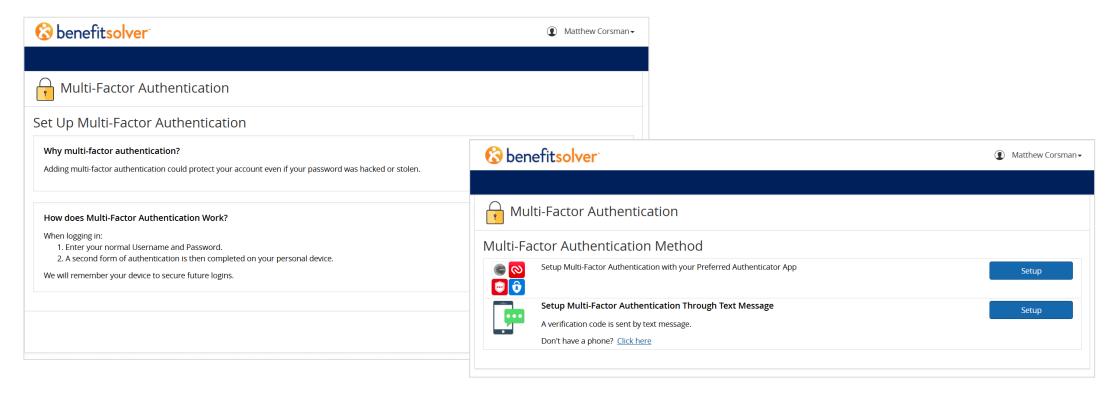




Strengthening Benefitsolver Security

Multi-Factor Authentication Coming for All

Businessolver is committed to safeguarding our customers' data and driving the highest standards for security within the benefits industry. In honor of that commitment, we will be enabling multi-factor authentication (MFA) for all members logging into Benefitsolver.



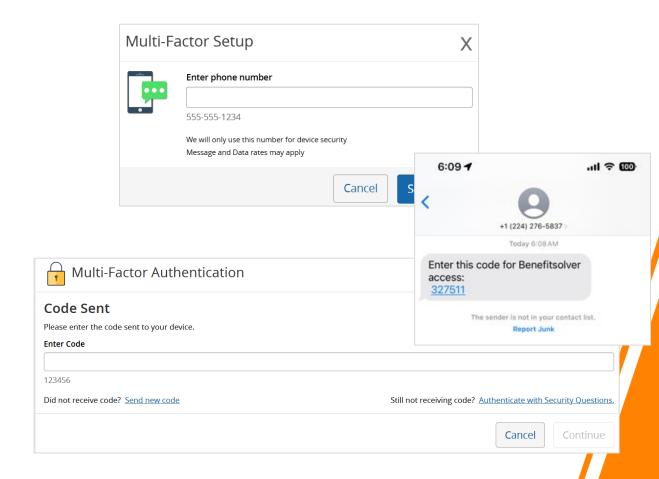


> The Details

Multi-Factor Authentication will be turned on for all clients on August 1!

As easy as...

- 1. **Initial Login**: Upon logging in with their credentials, members will be asked to set up authentication.
- Authentication Type: Email, Text Message, Authenticator App
- 3. Ongoing Logins: They will then use that authentication method each time after when they log in (including if they change benefit status). This does NOT impact those logging in through SSO.

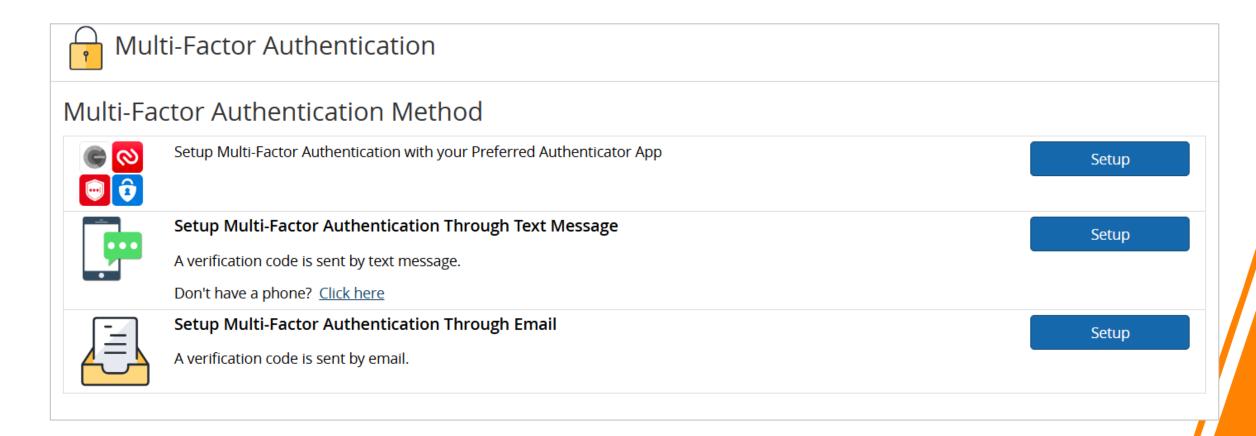






What are the authentication types?

Email, SMS and Authenticator App





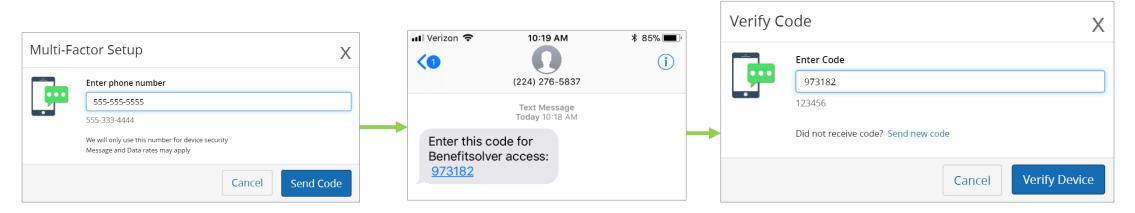


Using SMS authentication to log in to Benefitsolver

When logging in, members and admins will have the option to set up SMS Multi-Factor Authentication with their mobile phone number.



The user will provide their number and a code will be sent to their phone. They will then enter that code into Benefitsolver to log in. The messaging in the text is configurable.

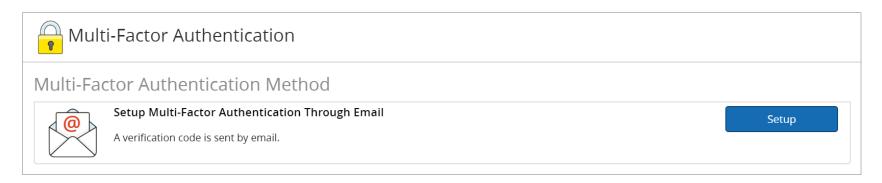




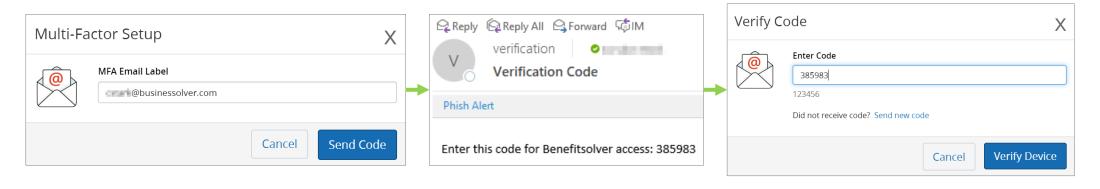


Using email authentication to log in to Benefitsolver

When logging in, members and admins will have the option to set up Multi-Factor Authentication with their email address.



The user will have a code sent to their inbox. Then, they will enter the code into Benefitsolver to log in. The messaging within the email is configurable.

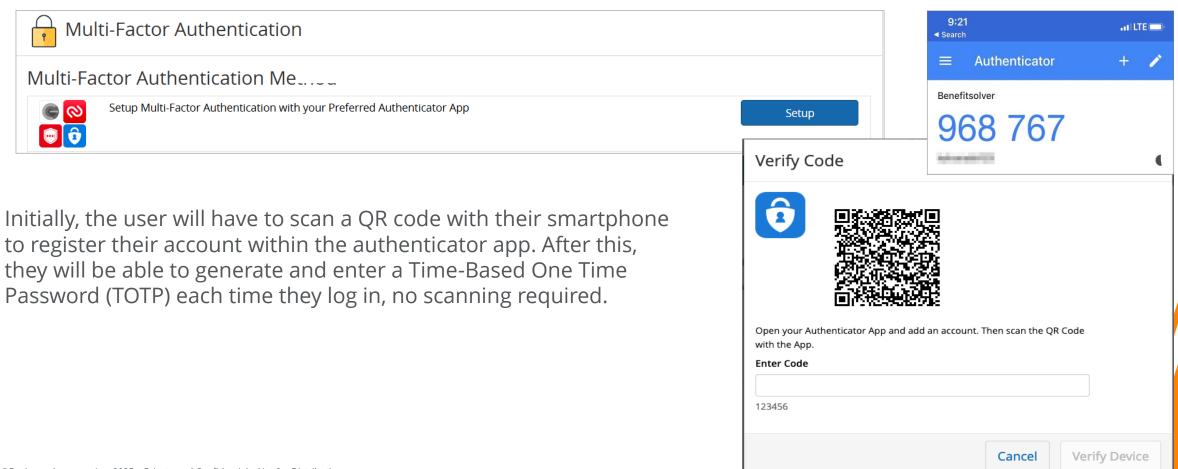






Using an authenticator app to log in to Benefitsolver

When logging in, members and admins will have the option to set up Multi-Factor Authentication with their desired authenticator application.



Frequently Asked Questions

We are not contracted for text messaging; can we still use the text authentication option? Yes. The text function within MFA is not part of the contracted text messaging service and is available for all clients within MFA specifically. For those who are contracted for text messaging, this will not impact your messaging count.

Is this a required setting for employees? This is required. Given heightened security concerns, we must enable MFA to safeguard member information ongoing.

Can we add MFA to our admin logins? Yes! This can also be turned on for your administrator logins. (But is not required)

Is the setup configurable? While our security team has set minimum thresholds of what must be in place (and will be launched with the update), if you wish to make the entry more restrictive, that is permitted. Additionally, most of the text within the experience is also configurable, including the email/text message that is sent as part of the experience.



Frequently Asked Questions

What are the required settings?

- MFA is required for members but still optional for admins.
- The types of devices that can be used are at your discretion. We will deploy the setting with all three options available, however, the you may update the devices allowed (email, authenticator and SMS).
- You can choose to make MFA only required when logging in from a new device, however best practice is to always require the authentication.
- Minutes to timeout will follow industry best practice which is 5 minutes.

Anything else? For MFA to work properly, personal preferences must be turned on. This allows us to collect the required information. The majority of clients (more than 95%) are already taking advantage of this experience!





Technology, Powered by People

Market Leader in Benefits Technology and Innovation

