

 Benefits Technology, Powered by People

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

Businesssolver 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 image displays two overlapping screenshots of the Benefitsolver web application interface, illustrating the Multi-Factor Authentication (MFA) setup process.

Left Screenshot: Shows the user's profile at the top right as "Matthew Corsman". Below the header, a section titled "Multi-Factor Authentication" is visible, followed by a sub-section "Set Up Multi-Factor Authentication". Under this, there are two informational boxes: "Why multi-factor authentication?" (stating it protects the account even if a password is hacked) and "How does Multi-Factor Authentication Work?" (explaining the two-step login process: 1. Enter Username and Password, 2. Complete second form on personal device).

Right Screenshot: Shows the "Multi-Factor Authentication Method" selection screen. It offers two primary options, each with a "Setup" button: "Setup Multi-Factor Authentication with your Preferred Authenticator App" (accompanied by icons for Google Authenticator, Microsoft Authenticator, and others) and "Setup Multi-Factor Authentication Through Text Message" (accompanied by a smartphone icon). A note for the text message option states "A verification code is sent by text message." and includes a link "Click here" for users without a phone.



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.
2. **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.


The image displays three overlapping screenshots illustrating the Multi-Factor Authentication (MFA) process:

- Top Screenshot (Multi-Factor Setup):** A window titled "Multi-Factor Setup" with a close button (X). It prompts the user to "Enter phone number" with a text input field containing "555-555-1234". Below the input, it states: "We will only use this number for device security. Message and Data rates may apply." There are "Cancel" and "Save" buttons at the bottom right.
- Bottom Left Screenshot (Code Sent):** A window titled "Multi-Factor Authentication" with a lock icon. It says "Code Sent" and "Please enter the code sent to your device." Below this is an "Enter Code" label and a text input field containing "123456". At the bottom, it provides links: "Did not receive code? [Send new code](#)" and "Still not receiving code? [Authenticate with Security Questions](#)". There are "Cancel" and "Continue" buttons at the bottom right.
- Bottom Right Screenshot (Text Message):** A simulated text message from "Benefitsolver" with a profile icon and phone number "+1 (224) 276-5837". The message says: "Enter this code for Benefitsolver access: **327511**". It also includes the text "The sender is not in your contact list." and a "[Report Junk](#)" link.






What are the authentication types?

Email, SMS and Authenticator App

 Multi-Factor Authentication


Multi-Factor Authentication Method

	Setup Multi-Factor Authentication with your Preferred Authenticator App	Setup
	Setup Multi-Factor Authentication Through Text Message A verification code is sent by text message. Don't have a phone? Click here	Setup
	Setup Multi-Factor Authentication Through Email A verification code is sent by email.	Setup



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.

 Multi-Factor Authentication

Multi-Factor Authentication Method




Setup Multi-Factor Authentication Through Text Message
A verification code is sent by text message.

Setup

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.

Multi-Factor Setup






Enter phone number

555-333-4444
We will only use this number for device security
Message and Data rates may apply

Cancel Send Code

Verizon 10:19 AM 85%


  

(224) 276-5837

Text Message
Today 10:18 AM

Enter this code for
Benefitsolver access:
[973182](#)

Verify Code



Enter Code


123456
Did not receive code? [Send new code](#)

Cancel Verify Device




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.

 Multi-Factor Authentication

Multi-Factor Authentication Method




Setup Multi-Factor Authentication Through Email
A verification code is sent by email.

Setup





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.



Multi-Factor Setup X



MFA Email Label

Cancel Send Code


 verification 

Verification Code

Phish Alert

Enter this code for Benefitsolver access: 385983

Verify Code X



Enter Code

123456


Did not receive code? [Send new code](#)

Cancel Verify Device




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.



Multi-Factor Authentication

Multi-Factor Authentication Message



Setup Multi-Factor Authentication with your Preferred Authenticator App

Setup



9:21
Search
LTE

Authenticator

Benefitsolver

968 767

Verify Code



Open your Authenticator App and add an account. Then scan the QR Code with the App.

Enter Code

123456

Cancel Verify Device



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