Multi-Factor Authentication
Use Case Report

Process

To reduce security vulnerability, the GoHealth system provides our end users with an additional layer of protection by utilizing a two-factor authentication process.

Our authentication process is automatically initiated at the first login of each day. The first level of authentication is accomplished via the entry of the username and password. It is then followed by a system generated email that delivers an authentication code (OTP) to the end user's email address on file within the personnel profile. This automatically generated code is a numeric string and authenticates a user for a single transaction or login session and must be entered before access is granted to the GoHealth system.

This added level of authentication prevents unauthorized access to the GoHealth system via comprised login credentials.

Steps

1. The user navigates to the login form.
2. The user enters the username for authentication to begin.
3. The user enters a password corresponding to the information given in step 2.
4. The application prompts for an OTP that is sent to the user's email address.
5. The OTP is retrieved by the user and the user manually enters the authentication code.
6. The correct OTP will grant access to the GoHealth system.

Use cases to test:

1. A user sends a request for OTP, the app sends the OTP via email, OTP gets verified for successful authentication.
2. The user enters a wrong OTP and the authentication fails
3. The user enters the right OTP but later than the specified expiry time, authentication fails
4. Users enter the OTP after a long time (expiration time) – the authentication fails