MULTI-FACTOR AUTHENTICATION

6/25/2021

Table of Contents

Revision History

Date	Version	Reason for Change
6/25/2021	1.0	Initial draft of the use case document

Trademark Notice

Software License Notice

Introduction:

blueEHR supports multi-factor authentication. The document describes briefy the use cases of multi-factor authentication. blueEHR has three methods for multi-factor authentication.

- Login using Email OTP,
- Login using SMS OTP.
- Login using Google Authenticator code.

Multi-factor Authentication:

Use Case for Email authentication:

Multi-factor authentication using email can be setup by the administrator as well as the user. While logging into blueEHR application after successfully authenticating the username and password provided by the user, the user will get the input section where OTP can be provided. OTP will be received in the email, the user can input the OTP and successfully login to the system.

User Case for SMS authentication:

Multi-factor authentication using SMS can be setup by the administrator as well as the user. While logging into the blueEHR application after successfully authenticating the username and password provided by the user, the user will get the input section where OTP can be provided. OTP will be received as SMS, the user can input the OTP and successfully login to the system.

User Case for Google Authenticator:

Multi-factor authentication using Google Authenticator can be setup by the administrator as well as the user. While logging into the blueEHR application after successfully authenticating the username and password provided by the user, the user will get the input section where the Google Authenticator code can be provided. Once the code is provided and the authentication is successful the user can enter the application.

Use Case for multiple Multi-factor authentication:

Users can enable multiple methods of multi-factor authentication. If there are multiple methods enabled and when a user logs into the system, user can choose the multi-factor authentication and provide the OTP/Code accordingly.