P: 757.213.5960 | F: 757.213.5965 | 5005 Colley Ave | Norfolk VA 23508

Welligent MU3: 2-Factor Authentication Use Case

Attestation

Welligent attests that the Welligent MU3 IT module supports authentication, through multiple elements, of the user's identity with the use of industry-recognized standards.

Introduction

The intent of two-factor authentication is to prevent unauthorized access to Welligent. A user can access the Welligent system only after their credentials are successfully verified by the two steps of authentication required by the system.

Description

Two-factor authentication in Welligent MU3 software is used to verify a user's credentials at the time of user login. Welligent uses both secure login and password credentials, as well as a four-digit code obtainable by cell phone text message or email to provide a second layer of credential verification. Once the code has been successfully entered and system verified, the user is granted access to their account in Welligent.

The four-digit verification code times out after five minutes if not entered on the verification screen, and the user is denied access to Welligent. The user must then request a new code via text or email to access Welligent.

Actors

The primary actor in this use case is the Welligent system user. The other entity included in the use case is the Welligent MU3 EHR system.

Goal

The goal of this test case is for the user to access their Welligent account securely.

Pre-Condition

To access Welligent, an approved user must have the following:

- An account set up in Welligent's User Maintenance
- Login name and password that meets the standards set by Welligent and the agency
- A login challenge question and response
- A working email address included in the user account
- A working cell phone number and indicator for cellular provider included in the account

P: 757.213.5960 | F: 757.213.5965 | 5005 Colley Ave | Norfolk VA 23508

Use Case 1

Token Submitted within Allotted Time Period

Actor/Entity	Step	Procedure	Expected Result
User	1	Clicks Welligent link	Welligent login screen displays
	2	Enters account login and password	Welligent verification screen displays requesting a token
System	3	Automatically creates four-digit token	Token is sent to user's email/text message
User	4	Checks text message or email	A four-digit token is provided
	5	Enters token on verification screen	Token is accepted
System	6	Automatically verifies token with account login/a match is made	The Welligent account is made available to the user

Use Case 2

Token Time Period Allowed to Expire

Actor/Entity	Step	Procedure	Expected Result
User	1	Clicks Welligent link	Welligent login screen displays
	2	Enters account login and password	Welligent verification screen displays requesting a token
System	3	Automatically creates four-digit token	Token is sent to user's email/text message
User	4	Checks text message or email	A four-digit token is provided
	5	Enters token on verification screen	Token is accepted
System	6	Automatically verifies token with account login/token has timed out	A message displays alerting the user that the verification has timed out and a new token request is required
User	7	Submits request for new token	A new four-digit token is provided
System	8	Automatically creates new four-digit token	Token is sent to user's email/text message
User	9	Checks text message or email	A four-digit token is provided
	10	Enters token on verification screen	Token is accepted
System	11	Automatically verifies token with account login/a match is made	The Welligent account is made available to the user