Team Firewall

Two-step Authentication Login

Written Requirements

Revision History

Authors	Description of Change	Sections	Rev	Date
Team Firewall	Initial Release		1.0	3/13/18
Ivan	Grammar corrections and requirement addition	3.1.1-3.1.8	1.1	3/20/18

Table of Contents

2nd level authentication   10

    The System will call for a 2 Step Authentication   10

    Validate 2 Step Authentication Code   10

Reset password   10

    Request Password Reset   10

1   Team Description

Team Member Name	Email Address
Gyromee Hatcher	gyromee@csu.fullerton.edu
Gabriel Varela	gabrielv@csu.fullerton.edu
Ivan Rosales	irosales@csu.fullerton.edu
Mevin Chen	mevin.chen@csu.fullerton.edu
Meng-Shen Kuan	mengkuan@csu.fullerton.edu

2   Terminology

The following table defined terms used within this document.

Term	Definition
User	A person operating the software
System	The website and database hosted on a server
Database	SQL database to store user data
opt in/out	Choose whether or not to have a feature. In = yes, Out = no.
2-step authentication	A second form of authentication after entering a password to login to an account.
Valid password	At least four and at most fifteen ascii characters.

3   Two-step Authentication Login
System Login utilizing a two factor authentication.

3.1   Overview
The program simulates a system login that allows basic account creation, deletion and modification that is protected by a two factor authentication system.

3.1.1   Create Account

Shall allow the user to create an account in order to being using the system

3.1.1.1   Email Validation
The system **shall** only accept a unique email that is not already in the database. **ID: 0001**

3.1.1.2   Password Creation and Confirmation.
The system **shall** only accept a valid password. **ID: 0002**

The system **shall** only create the account if both password inputs are verbatim. **ID: 0003**

3.1.1.3   Account Authentication
According to the steps above, when the account is created the system **shall** send an authentication email in order to access the homepage **ID: 0004**

3.1.2   Login

Users will be able to access content in the system after providing valid credentials to login.

3.1.2.1   Check Credentials
The system **shall** take the email and password and confirm with the database on the system. If this is the first time the user has logged in from this computer, "2nd level authentication" as specified in section 3.6.1 shall be required. **ID: 0005**

If they have, the system **shall** move onto "Allow Access to internal system", otherwise the system shall move onto 3.1.6. **ID: 0006**

3.1.2.2   Allow Access to internal system
The system **shall** redirect the user with correct credentials to the homepage that is provided to all valid users. **ID: 0007**

3.1.2.3   Edit Account Info

Requirement: User shall be logged in.

The user **shall** be able to change the information stored in their account. **ID: 0008**

3.1.2.4   Change Password
The user **shall** be able to change their password to another unique one with at least four and at most fifteen ascii characters. **ID: 0009**

3.1.2.5   Change Email Address
The user **shall** be able to change the email address associated with their account to a different valid email address. **ID: 0010**

3.1.3   Delete Account

The system **shall** allow the user to delete their account. **ID: 0011**

3.1.3.1   Request Account Deletion
The user **shall** request the system to delete their account from the database. **ID: 0012**

3.1.4   Opt in/out of 2-step authentication

Requirement: User shall be logged in.

The user **shall** be able to opt in/out of a 2-step authentication. **ID: 0013**

3.1.4.1   Opt in

If the user desires, the system **shall** allow the user to opt in of the 2-step authentication. **ID: 0014**

3.1.4.2   Opt out

If the user decided to opt in of the 2-step authentication system, the system **shall** allow the user to opt out of the 2-step authentication. **ID: 0015**

3.1.5   2nd level authentication

Requirement: User shall be logged in.

Shall allow the authenticate their account by clicking on the verification link upon account creation. **ID: 0016**

3.1.5.1   The System will call for a 2 Step Authentication

The system **shall** dictate when the user must perform a 2 Step Authentication. 2 Step Authentication will happen when the user first logs in by using the verification link and every time the user logs in if they have chosen to opt in our 2 Step Authentication. **ID: 0017**

3.1.5.2   Validate 2 Step Authentication Code

The system **shall** update the database showing that the user has successfully passed the 2 Step Authentication step on their account or computer. **ID: 0018**

3.1.6   Reset password

Requirement: User shall be logged in.

The user **shall** be able to reset their password by clicking a link on their homepage. **ID: 0019**

3.1.6.1   Request Password Reset

Upon request, the user **shall** be required to enter their email and a link to reset their password will be sent to the entered email. **ID: 0020**