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

1 Team Description

Team Member Name	Email Address
Gyromee Hatcher	gyromee@csu.fullerton.edu
Gaberiel 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 Username Creation

The system **shall** only accept a unique username with at least four and at most fifteen ascii characters. The user must enter their username twice to confirm that they are verbatim.

3.1.1.2 Password Creation and Confirmation.

The system **shall** only accept a valid password.

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

3.1.1.3 Email and Email confirmation

The user **shall** input their email address twice to confirm they are verbatim. If they are not verbatim, the system will not allow the creation of the account.

3.1.1.4 Security Questions

The system **shall** require the user to input three security questions of their own choosing and three answers corresponding to the questions.

This will allow the user to recover their password by using the *Recover Password* option.

3.1.1.5 Account confirmation

According to the steps above, when the account is created the system **shall** send an account creation confirmation email in order to access the homepage

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 username 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.

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

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.

3.1.3 Edit Account Info

Requirement: User shall be logged in.

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

3.1.3.1 Change Username or Password

The user **shall** be able to change their username to another unique one with at least four and at most fifteen ascii characters.

The user **shall** be able to change their password to a valid password

3.1.3.2 Change Email Address

The user **shall** be able to change the email address associated with their account to a different valid email address.

3.1.3.3

2-Step authentication

After the user has logged in and verified their account, the system **shall** make the user opt in to the 2-step authentication service.

3.1.4 Delete Account

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

3.1.4.1 Request Account Deletion

The user **shall** request the system to delete their account from the database.

3.1.4.2 Required 2 Step Authentication

The system **shall** perform 2nd level Authentication in order to ensure the user is authenticated, regardless of opt out settings. Once 2nd Level Authentication is completed, the account **shall** be deleted.

3.1.5 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.

3.1.5.1 Opt out

By default, the user **shall** be automatically placed in our 2-step authentication system upon account creation. If the user desires, the system **shall** allow the user to opt out of the 2-step authentication.

3.1.5.2 Opt in

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

3.1.6 2nd level authentication

Requirement: User shall be logged in.

Shall allow the user to enter the code sent to them via email to authenticate.

3.1.6.1 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 and every time the user logs in on a new device, if they have not chosen to opt out.

3.1.6.2 Validate 2 Step Authentication Code

The system **shall** email the provided email a 4-digit code along with a link to provide the 4-digit code. The user **shall** access the link provided and enter their 4-digit code provided to them in the email. The system **shall** update the database showing that the user has successfully passed the 2 Step Authentication step on their there account or computer.

3.1.7 Recover username and password

Requirement: User shall be logged in.

The user **shall** be able to recover their username or password by clicking a link on their homepage.

3.1.7.1 Recover username

Upon request, the user **shall** receive an email with their current username.

3.1.7.2 Reset Password

Upon request, the user **shall** be required to answer one of their security questions. Upon correctly answering a security question, the user **shall** receive an email link to change their password to a valid password.