US-15402 Glassbeam apps security implementation

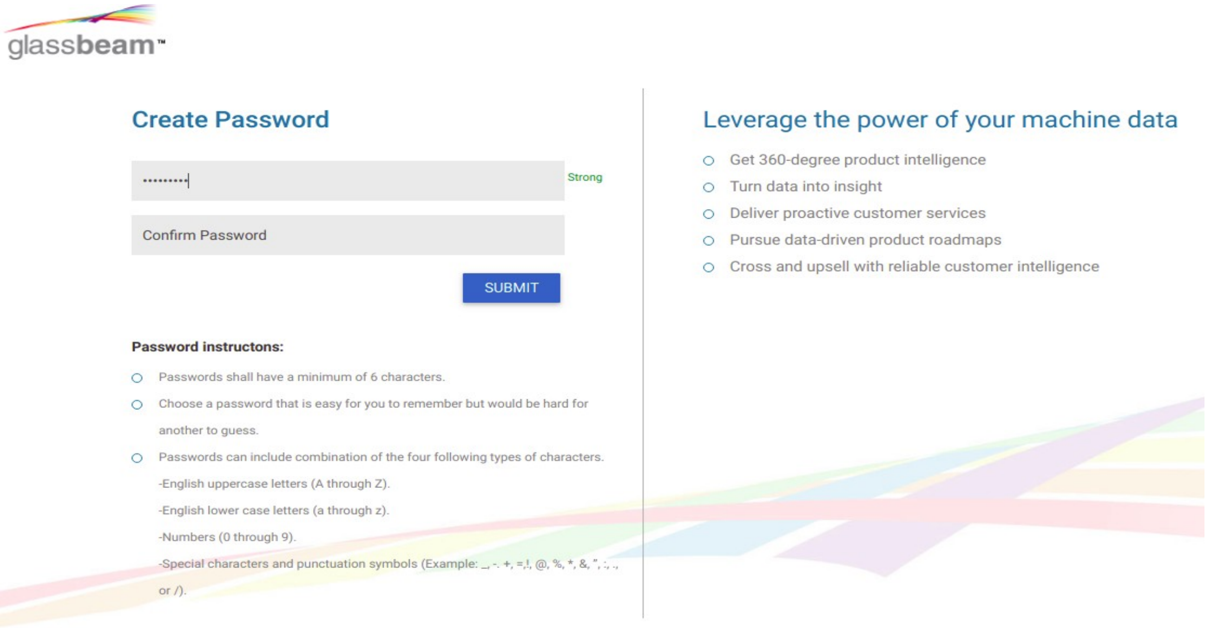
As per proposed document I have designed the mockups for the features as follows.

Password Policies:

Password Strength:

We need to rely on some kind of an indicator to indicate the strength of the password to the user during registration. The indicator serves as a good reminder for the user as to the level of difficulty to crack the password.

The below figure shows how the strength of the password is shown to the user.



Create Password

Confirm Password

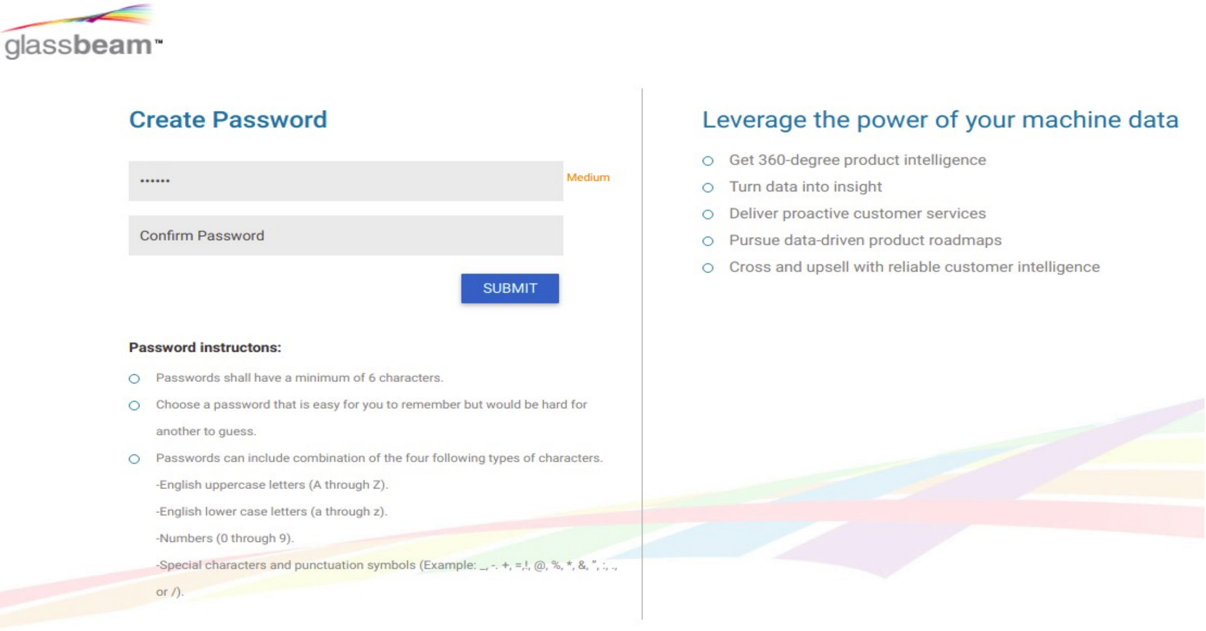
Password instructons:

- ○ Passwords shall have a minimum of 6 characters.
- ○ Choose a password that is easy for you to remember but would be hard for another to guess.
- ○ Passwords can include combination of the four following types of characters.
  - -English uppercase letters (A through Z).
  - -English lower case letters (a through z).
  - -Numbers (0 through 9).
  - -Special characters and punctuation symbols (Example: _, -. +, =,!, @, %, *, &, ", :, ., or /).

Leverage the power of your machine data

- ○ Get 360-degree product intelligence
- ○ Turn data into insight
- ○ Deliver proactive customer services
- ○ Pursue data-driven product roadmaps
- ○ Cross and upsell with reliable customer intelligence

Figure 1: Strong Password



Create Password

Confirm Password

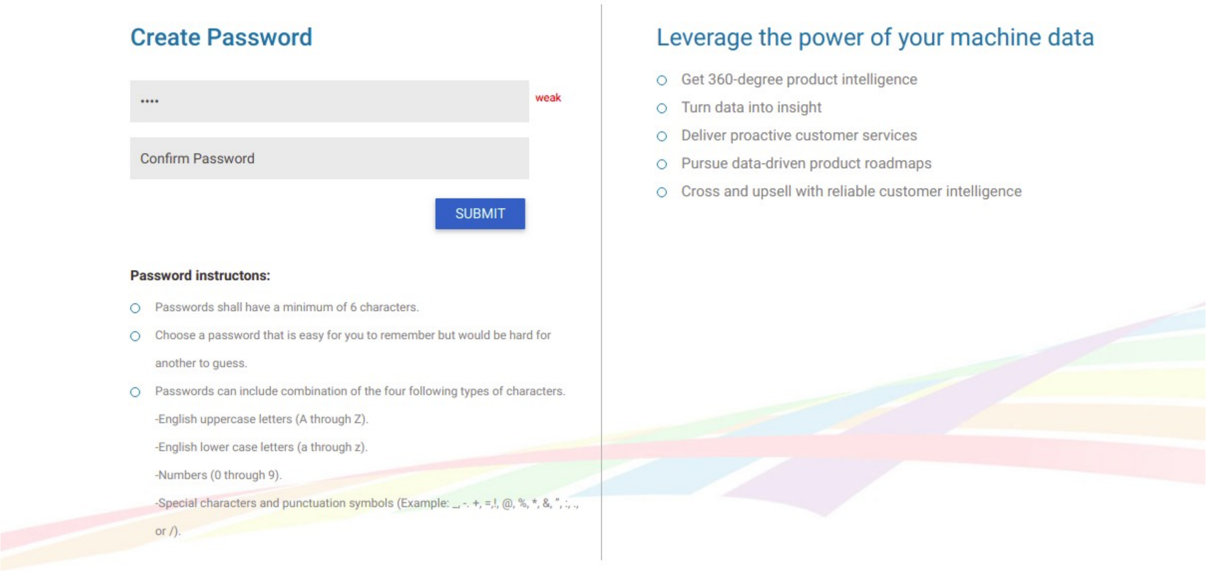
Password instructons:

- ○ Passwords shall have a minimum of 6 characters.
- ○ Choose a password that is easy for you to remember but would be hard for another to guess.
- ○ Passwords can include combination of the four following types of characters.
  - -English uppercase letters (A through Z).
  - -English lower case letters (a through z).
  - -Numbers (0 through 9).
  - -Special characters and punctuation symbols (Example: _, -. +, =,!, @, %, *, &, ", :, ., or /).

Leverage the power of your machine data

- ○ Get 360-degree product intelligence
- ○ Turn data into insight
- ○ Deliver proactive customer services
- ○ Pursue data-driven product roadmaps
- ○ Cross and upsell with reliable customer intelligence

Figure 2: medium Password



Create Password

....

weak

Confirm Password

Password instructons:

- ○ Passwords shall have a minimum of 6 characters.
- ○ Choose a password that is easy for you to remember but would be hard for another to guess.
- ○ Passwords can include combination of the four following types of characters.
  -English uppercase letters (A through Z).
  -English lower case letters (a through z).
  -Numbers (0 through 9).
  -Special characters and punctuation symbols (Example: _, -. +, =,!, @, %, *, &, ", :, ., or /).

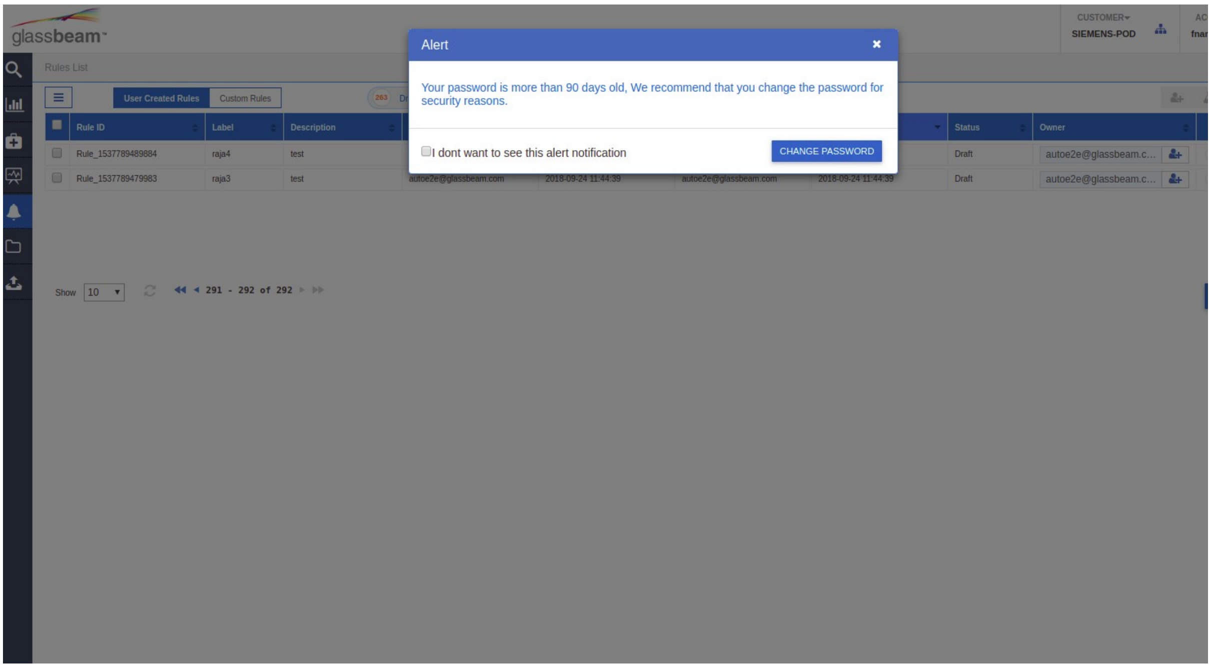
Leverage the power of your machine data

- ○ Get 360-degree product intelligence
- ○ Turn data into insight
- ○ Deliver proactive customer services
- ○ Pursue data-driven product roadmaps
- ○ Cross and upsell with reliable customer intelligence

Figure 3: Weak Password

Password Expiry/Duration:

After a certain period of time 60 to 90 days, we can alert the user once he logs in saying that the password is greater than 90 days, In addition, we can provide an option to not show the alert and a checkbox stating that he doesn't want to change his password.



Alert ×

Your password is more than 90 days old, We recommend that you change the password for security reasons.

□ I dont want to see this alert notification

□	Rule ID	Label	Description					Status	Owner
□	Rule_1537789489884	raja4	test					Draft	autoe2e@glassbeam.c...
□	Rule_1537789479983	raja3	test	autoe2e@glassbeam.com	2018-09-24 11:44:39	autoe2e@glassbeam.com	2018-09-24 11:44:39	Draft	autoe2e@glassbeam.c...

Show 10 ▾ 291 - 292 of 292

Figure 4: Password Expiry

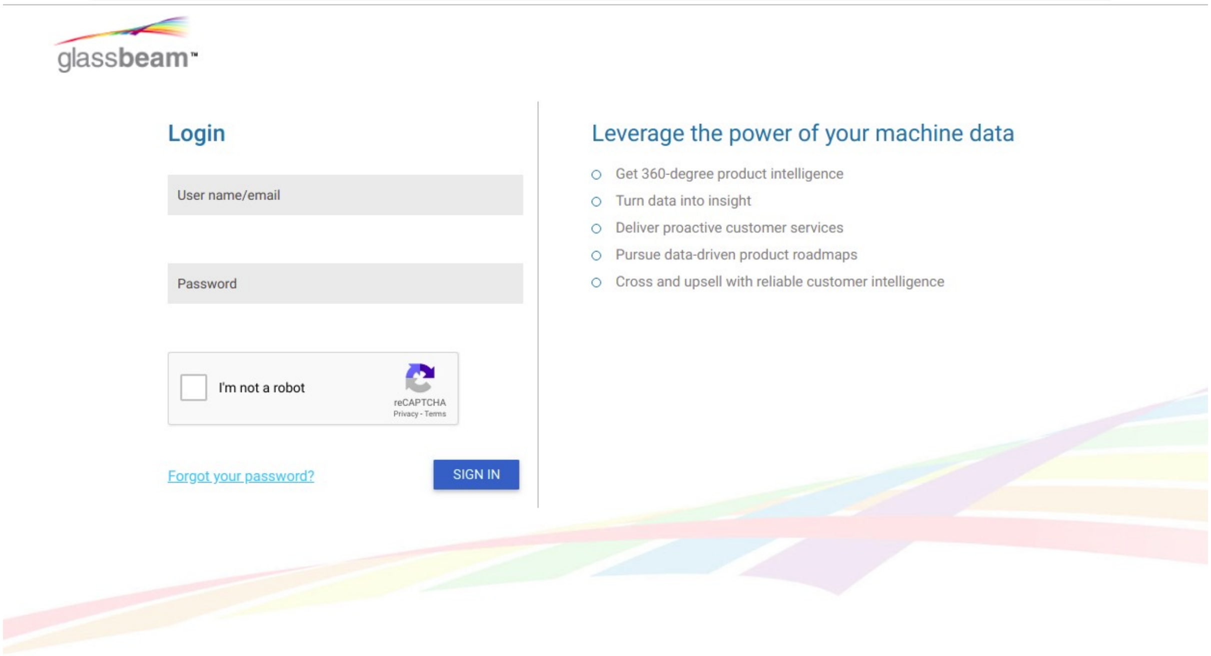
The user has an option to opt out from this notice if he doesn't want to change his password. The change password will work as per the existing process.

Login/Logout Policies:

Login Captcha:

Google reCaptcha V2 is used for this implementation which is a free captcha service provided by Google.

The captcha will appear on the login screen after sequential failed login attempts. This would reduce automated brute force attempts. The user would need to solve the captcha in order to login after failed attempts.



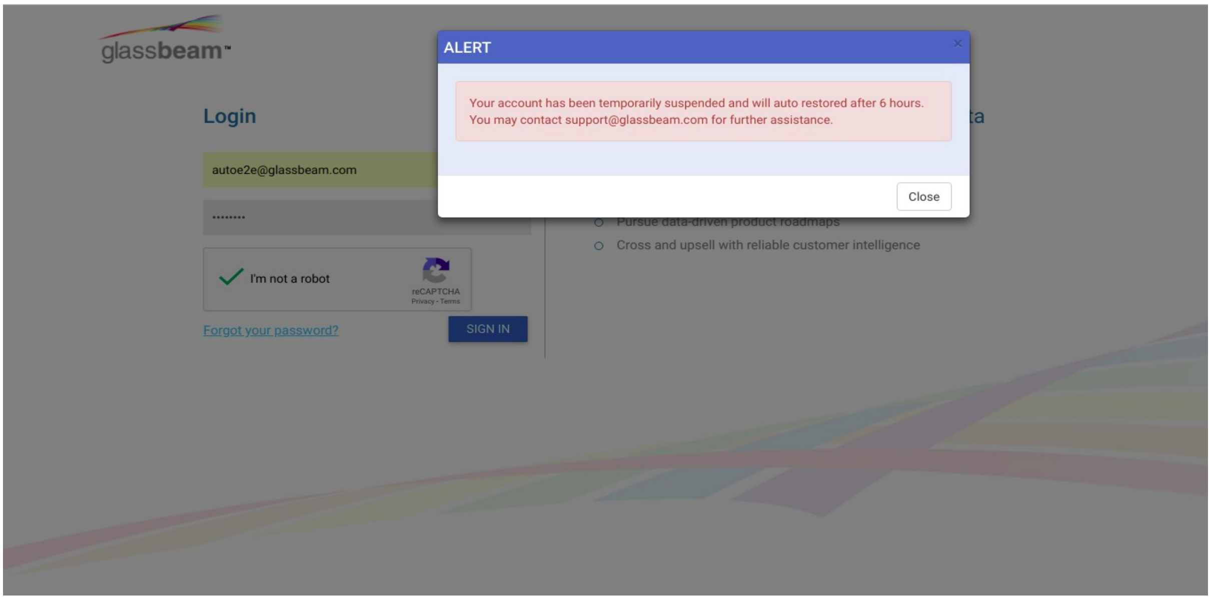
Leverage the power of your machine data

- Get 360-degree product intelligence
- Turn data into insight
- Deliver proactive customer services
- Pursue data-driven product roadmaps
- Cross and upsell with reliable customer intelligence

Figure 5: Login Captcha

Failed & Limit login attempts:

Limiting the number of times a user can attempt to log in to your application helps reduce the risk of brute force attack. A brute force attack happens when an attacker tries to gain access by guessing your username and password through the process of cycling through combinations. To help protect against brute force attacks, you want to limit the number of times any user can try to log in to your website. After ‘n’ number of attempts, the account can be temporarily blocked for few minutes.



Your account has been temporarily suspended and will auto restored after 6 hours. You may contact support@glassbeam.com for further assistance.

- Pursue data-driven product roadmaps
- Cross and upsell with reliable customer intelligence