

Specifications

US001 - Login Time Rule

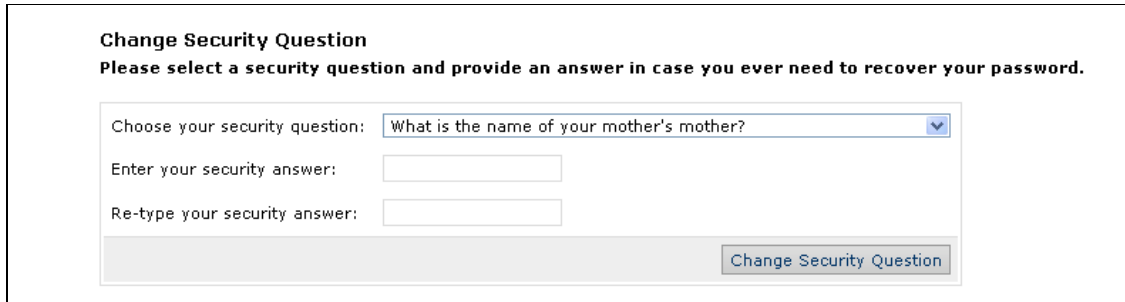
As a system, I want to enforce when users can login into the application.

Login Time Rule		
Rule Name:	<input type="text"/>	
Rule Description:	<input type="text"/>	
Rule Type:	Login Time Rule ▼	
Apply to Payee:	<input type="checkbox"/>	
Apply to Users:	<input type="checkbox"/>	
Login Time Details		
The time the working day begins:	00 ▼	00 ▼
The time the lunch hour begins:	00 ▼	00 ▼
The time the lunch hour ends:	00 ▼	00 ▼
The time the working day ends:	00 ▼	00 ▼
Sunday:	<input type="checkbox"/>	
Monday:	<input type="checkbox"/>	
Tuesday:	<input type="checkbox"/>	
Wednesday:	<input type="checkbox"/>	
Thursday:	<input type="checkbox"/>	
Friday:	<input type="checkbox"/>	
Saturday:	<input type="checkbox"/>	

Note: Fields in yellow are mandatory.

US002 - First time provisioning of username/ password after platform user sync

As a system, I want to send a notification (via email) with specific instructions (e.g. provisioning link) to users when they are created for the first time in the portal so that they can login into the portal with minimum overhead to system administrators



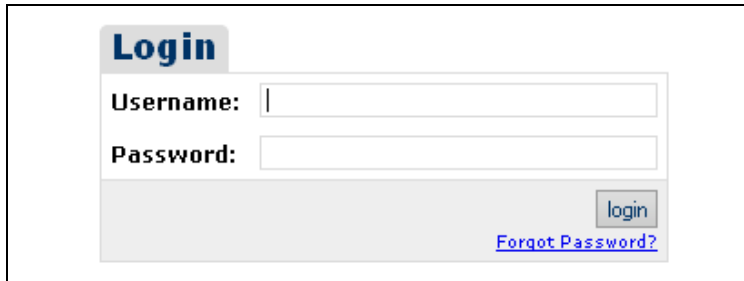
The screenshot shows a web form titled "Change Security Question". Below the title is a instruction: "Please select a security question and provide an answer in case you ever need to recover your password." The form contains three input fields: a dropdown menu for "Choose your security question:" with the selected option "What is the name of your mother's mother?", a text box for "Enter your security answer:", and another text box for "Re-type your security answer:". A "Change Security Question" button is located at the bottom right of the form.

Acceptance Criteria

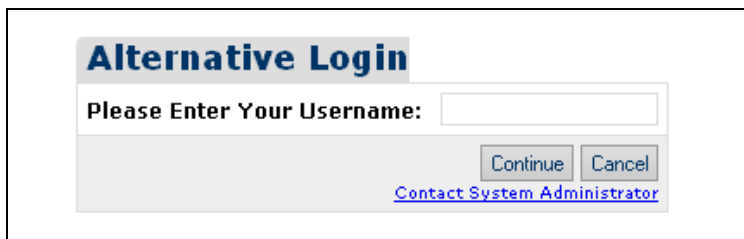
1. Email sent to users when they are created for the first time in the portal.
2. The email must provide the username/account name as well as a web link to self service create password and answers to security questions
3. The web link should launch a form that requires the user to specify a password. The user must be required to input the password twice. The two entries must be matched. The password must be validated against password strength rules. Warning message must be provided if the password does not match and/or the password strength criteria are not met.
4. The form must also present pre-defined security questions. The text box for the responses must be able to accept 255 characters. Validation must be performed to ensure that non-null responses are provided for all security questions.
5. User should not be allowed to create password if account is locked

US003 - Self service password change via "forgot password" link

As user, I want the ability to reset my password without requiring the system administrator to manually reset my account so that I can save time.



The Login form features a title 'Login' in a blue box. Below it are two input fields: 'Username:' and 'Password:'. A 'login' button is positioned to the right of the password field. At the bottom right, there is a blue hyperlink labeled 'Forgot Password?'.



The Alternative Login form has a title 'Alternative Login' in a blue box. It contains a single input field with the label 'Please Enter Your Username:'. To the right of the field are 'Continue' and 'Cancel' buttons. At the bottom right, there is a blue hyperlink labeled 'Contact System Administrator'.



This image shows the Alternative Login form with pre-filled data. The 'Username:' field contains 'acody'. The 'Security Question:' is 'What is the first letter of the alphabet?'. The 'Security Answer:' field is empty. Below this is a list of five password requirements: 1. Password must contain at least 4 character(s). 2. Password must contain at least 1 numeric value(s). 3. Password must not contain the username. 4. Password must not match any of the 5 previous passwords. 5. Passwords expire in 60 days. At the bottom are 'New password:' and 'Re-type new password:' fields, followed by 'login' and 'Cancel' buttons, and the 'Contact System Administrator' link.

Acceptance Criteria

1. Link on portal page corresponding to 'Forgot Password' (Image 1) - clicking on link should refresh the page to show a form to collect the required information. (Image 2)
2. If the username field in the Login page was filled, the same username should be pre-populated in the Alternative Login page. (Image 2)

3. The 'Alternative Login' form must require answers the secret question (previously setup) corresponding to the user.(Image3)
4. If the answer match and the new password meets the strength rules, the user is allowed to start a session in the portal (clicking on Login button). The Home page is displayed.
5. If security answer does not match, provide a message "Your answer does not match. Please try again". If the number of attempts exceed the pre-defined limit, the account must be locked and a message stating "You account is locked. Contact system administrator" must be provided.
6. The new password must be validated against password strength rules. If the new password doesn't meet any of the rules a corresponding error message will be displayed.
7. User must not be able to change password if account if locked
8. The flow can finish in any point clicking on the Cancel button.