Test Case Document for

Strengthening the password policies

(Security Module Enhancement)

Version 1.0

By Visolve ViCare Team

Prepared by

ViSolve Inc.,

Contact: 408.666.4320

EMail: vicare_engg@visolve.com

www.visolve.com

25th November 2009

Revision History

Version	Date	Author	Reviewed By
1.0	11/25/09	ViCare Team	Team

I. Password must be eight character length or more and must contain 3 of the following 4 items:

- a lowercase letter
- an uppercase letter
- an integer
- a special character

Test the following test cases in **"User and Group Administration** (Administration->Users)**" and** "**User Administration** (Administration->Users->edit)" and "**Password Change** (Miscellaneous->Password)" pages.

1. Enter the username in username textbox and click add button. An alert "Please enters the password" is displayed

2. Enter the username and password which is less than eight characters in "Password" textbox and click add button. The following alert is displayed.

"The password must be at least 8 characters, and should contain at least three of the four following items:

- A number
- A lowercase letter
- An uppercase letter
- A special character (not a letter or number).

For example: healthCare@09".

3. Enter the username and a non-strong password (Example: HealthCare) and click add button. The following alert is displayed. "The password must be at least 8 characters, and should contain at least three of the four following items:

- A number
- A lowercase letter
- An uppercase letter
- A special character (not a letter or number).

For example: healthCare@09".

4. Enter the username and password(Example: Healthcare123) which does contains minimum of eight characters, any of three items from the list (a number, a lowercase letter, an uppercase letter, a special character) and click add button. Corresponding username is listed below with edit option. Check the database "users" table where the entered values are stored properly.

II. Passwords need to be changed on a regular basis (6 months) and the grace login period must be given for another 30days to reset the password.

Test the following test cases after successful login by users**.**

1. If the user logins, prior to <7 days of 'Password Expiration Date, the warning message "Welcome <<UserName>>, Your Password Expires on <<YYYY-MM-DD>>. Please change your password" is displayed.
2. If the user logins with password expiration date > current date + 7, the warning message "Welcome <<UserName>>, Your Password Expires on <<YYYY-MM-DD>>. Please change your password" is displayed.
3. If the user logins with password expiration date = current date + 4, the warning message "Welcome <<UserName>>, Your Password Expires on <<YYYY-MM-DD>>. Please change your password" is displayed
4. If the current date is equal to password expiration date then "Welcome <<UserName>>, Your Password expires today. Please change your password" message is displayed.
5. If the user logins with password expiration date = current date - 5, the warning message "Welcome <<UserName>>, You are in Grace Login period. Please change your password before <<YYYY-DD-MM>>".
6. If the user logins with password expiration date = current date - 90, their user account is locked and the user will not be able to login and user account is moved to 'Inactive' state.
7. If the "Password Expiration Date" is date empty or default value of "0000-00-00". The warning message "Welcome <<UserName>>, Your Password Expired. Please change your password" is displayed.
8. Password expiration page is loaded only once after successful login at the top frame (instead of calendar).
9. "Invalid username or password" message displayed when inactive username and password are used for login.
10. To active the inactive user, change the "password" and check the "active" field of particular user in **"User Administration**". If the password is not changed a warning message "Please reset the password" is displayed.

III. Test the following test cases in "User and Group Administration (Administration->Users)**" and "User Administration** (Administration->Users->edit)".

1. Default value for "Password Expiration" is 180.
2. Password Expiration field is configurable and text box accepts numbers.
3. Password Expiration value is added with current date and stored in "pwd_expiration_date" of "users "table. Check the date is calculated correctly.
4. Check values are stored correctly in" pwd_exp_duration" of "users" table.

IV. The system should log the last three passwords and prevent reuse.

Test the following test cases in "User Administration (**Administration**->Users->edit)" and "**Password Change (**Miscellaneous->Password**)**" pages.

1. Enter the new password for a user in "password" textbox and save it in database. This value is stored in "password" field of users table.Then enter the previous password in "password" textbox. Click add/save button. Now "Recent three passwords are not allowed" is displayed.
2. Repeat the previous step by entering last three passwords and the same alert message will be displayed.

3. Enter another new password and save it. Check the users table that new password is stored in “password” field and pervious password is stored in “pwd_history1”.
4. Enter another new password and save it. Check the users table that new password is stored in “password” field and password is stored in “pwd_history1” is moved to pwd_history2 and password is stored in “password” is moved to “pwd_history1”.

V. CCHIT Security Criteria and Test cases

CCHIT Criteria #	CCHIT Criteria
SC 03.02	When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.
SC 03.09	When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rules (SC 03.02)
SC 03.10	When passwords are used, the system shall support case sensitive passwords that contain typeable alpha and numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).
SC 03.12	When passwords are used, the system shall prevent the reuse of passwords previously used within a specific (configurable) timeframe (i.e., within the last X days, etc. - e.g. "last 180 days"), or shall prevent the reuse of a certain (configurable) number of the most recently used passwords (e.g. "last 5 passwords").
SC 06.02	When passwords are used, the system shall not display passwords while being entered

VI. Check above functionality in all type of browsers (Firefox, IE, chrome etc).