254450

Contents

1 254450

Ready for **What's Next, Now**™

2 254450 ID-7HSD79 Add Change Remove password management

Ready for **What's Next, Now**™

3 FUNCTIONAL OVERVIEW

3.1 Client Requirement

A person using the web should also be able to change their password themselves. This has been requested by Aramco to conform to their security policy. I assume passwords need to expire after a xxx time-out period, where the users can login 1 time and are forced to change the password to something else. This timeout should be configurable on the system as a global value, and alterable per person by the admin staff, if needed. If an admin changes a password, the first login should cause a password change by the user. We can NOT use the standard MTS password policy. We need to create a standard password management system, just like MS Windows, where the user themselves changes the password, or an Admin resets a password to a known value.

3.2 Solution

1.A new username profile table (MTS_OWNER.TRACKING_TOOL_USERS) will be created in MTS database specifically for authentication into the Tracking Tool web application. The new table will hold data in a similar way to as defined below

UserName	Password	Name	Company	Based At	Last Logged in	Last Password Change	Password Expires next on	Force Password Change on next log	User Locked
SANDUS	sdfgds445	Suk Sandhu	DHL	Hams Hall	21/10/08 09:32	01/10/08 10:00	31/12/08 00:00	N	
KARIMA	dsfbnsb5	Abdul Karim	Saudi Aramco	Damman	18/10/08 15:45	01/06/08 09:00	28/10/08 17:00	Y	N
MTS_OWNER	sb5b1	OBS	OBS	Speke	21/10/08 12:55	01/10/08 09:00	31/12/99 23:59	N	

2.An ORACLE forms front end screen will be developed to allow central administration of this data through MTS. The form will look rather like the above with actions NEW, EDIT, CHANGE PASSWORD, DELETE, SAVE, CLOSE

3.The Tracking Tool application will be changed to connect to the MTS database using the oracle username MTS_TRACKING and a secure password.

4.The user will be authenticated as normal via the login screen. However the username and password will also be authenticated via the above table.

5.If the username and password entered is valid, check that the user is not locked (TRACKING_TOOL_USERS.LOCKED = ?N?) - fail the login if the user is locked (TRACKING_TOOL_USERS.LOCKED = ?Y?).

6.Check whether the user has been set to force password change (TRACKING_TOOL_USERS.FORCE_PSWD_CHANGE = ?Y?) or if the password has expired (TRACKING_TOOL_USERS.PSWD_EXPIRY <= SYSDATE) - if so go through to the new change password screen.

7.Once successfully logged on, set the last logged on date to the current system date and time. (TRACKING_TOOL_USERS.LAST_LOGIN = SYSDATE).

8.There will be a new button available on the Tracking Tool application to allow individual users to change their password manually. If clicked it will go through to the new change password screen

9.The new change password screen will display 3 text boxes. One for the user to re-enter their old password, one for the new password and one to confirm the new password. The entries will be validated as follows:

```
?Old password must match the current password that the user entered when logging in.
?New password must contain a combination of numbers and letters. The password must not start or end in a nu
?New password can not be the same as old password.
?Confirm New Password must match the entry in the New Password field. The case of the letters must also mat
```

If successfully validated then the following updates will occur:

```
?Reset the force password change to N (TRACKING_TOOL_USERS.FORCE_PSWD_CHANGE = ?N?)
?Set the password expires next date to the current date + [a configurable number] of days (TRACKING_TOOL_US
?Update the Last Password Change Date to the current date and time. (TRACKING_TOOL_USERS.PSWD_CHANGED = SYS
?Update the Password to the new value ((TRACKING_TOOL_USERS.PASSWORD = [password entered]).
```

Ready for **What's Next, Now™**

3.3 Scope

This change will be applied to system version 10.6.

Ready for **What's Next, Now**™

4 SET-UP

4.1 Data

The current user information will need to be imported into the new table. This will include

```
Username
Name
Company
Based At
```

This information is available from ADM_USER for existing user in the Group WEBTRACKING.

Ready for **What's Next, Now**™

5 FUNCTIONAL DESCRIPTION

5.1 MTS

A new table will be created in MTS to store the user password details for Webtracking. This table will contain

```
USERNAME
PASSWORD
NAME
COMPANY
BASED_AT
LAST_LOGGED_IN
LAST_PASSWORD_CHANGE
PASSWORD_EXPIRES_ON
FORCE_PASSWORD_CHANGE
USER_LOCKED
```

The existing users for webtracking will be loaded into this table from ADM_USERS. The initial password for each user will be set to a default value. The user will then be prompted to change this when they first login to the system.

A new maintenance screen will be created for the entry and maintenance of the webtracking users. The screen will be similar in format to the existing user maintenance screen.

The screen will allow users to be entered, edited and deleted. The passwords for users will also be maintained from this screen.

An option to lock the user will be added, allowing superusers to force a user to change their password. This will be in the form of a check box against the user.

5.2 Tracking Tool Web Application

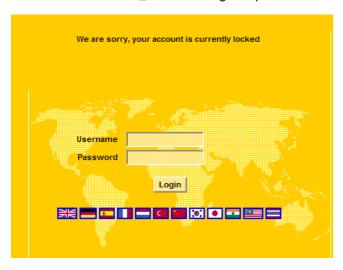Changes to the Tracking Tool application are detailed below:

The web application will connect to the MTS database using a generic username (MTS_TRACKING) and password (TBC).

The login screen will validate the username and password entered against the new table TRACKING_TOOL_USERS. If the username/password combination entered does not exist on this table then an error will be displayed:
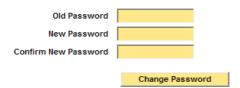

If the username/password combination is valid, the USER_LOCKED flag on the TRACKING_TOOL_USERS table will be checked. If the USER_LOCKED flag is equal to ?Y? then the following error will be displayed:

If the user is not locked (USER_LOCKED = ?N?) then the TRACKING_TOOL_USERS table?s LAST_LOGGED_IN date should be changed to the current date.

The system will now check to see if the user?s password needs to be reset (FORCE_PASSWORD_CHANGE = ?Y?) or if the password has expired (PASSWORD_EXPIRES_ON <= SYSDATE) - if so go through to the new change password screen:

Ready for **What's Next, Now**™

The new change password screen will display 3 text boxes as above. Entries made into these fields will be masked so that the password isn?t visible on screen. These fields will be validated as follows:

```
?Old password must match the current password that the user entered when logging in.
?New password must contain a combination of numbers and letters. The password must not start or end in a nu
?Confirm New Password must match the entry in the New Password field. The case of the letters must also mat
```

If successfully validated then the following updates will occur:

```
?Reset the force password change to N (FORCE_PASSWORD_CHANGE = ?N?)
?Set the password expires next date to the current date + [a configurable number] of days (PASSWORD_EXPIRES
?Update the Last Password Change Date to the current date and time. (LAST_PASSWORD_CHANGE = SYSDATE).
?Update the Password to the new value ((PASSWORD = [password entered]).
```

If the user arrived at this screen via the login screen (i.e. password expired or user forced to change password) then no system options will be available until the password has been successfully changed (e.g. user will not be able to search for example).

The password change screen can also be accessed manually by a user, should they wish to change their password at any time:

This option will be available on the left hand side of the screen near the ?Logout? button.

Ready for **What's Next, Now**™

6 Document History

Version	Date	Status	Reason	Initials
1a	22/01/09	Draft	Initial version (MTS Changes)	DNG
1b	27/01/09	Draft	Added Web application changes	NA
1	27/01/09	Issue	Reviewed and Issued	MJC

Ready for **What's Next, Now**™

7 Authorised By

7.1 Matt Crisford

Development Manager

7.1.1 Suk Sandhu

TMSCC MTS Product Mgr

Ready for **What's Next, Now**™