APAR: IV08054

Symptom: NEW FUNCTION ENHANCEMENT
Provide the ‘Minimum Password Age’ Rule in password policy.

A new password rule, ‘Minimum Password Age’, has been introduced that will allow administrators to limit how frequently a user can change the password on their account.

By default, this new rule is disabled and will not be visible to the customers. Please execute the following steps to configure and enable this rule in your environment. If you have a clustered environment then please repeat the below steps on each node of the cluster.

1) Stop the application server.

2) Enable the new rule by un-commenting the following property in $ITIM_HOME/data/passwordrules.properties files.

```
password.rule.com.ibm.passwordrules.standard.MinAgeConstraint=true
```

3) A new label, “Minimum Password Age”, is added in $ITIM_HOME/data/CustomLabels.properties file. This is the label that will be displayed on the ‘Password Policies’ page for the new rule. If you have installed a language pack then please edit the appropriate $ITIM_HOME/data/CustomLabels_nn.properties (where nn stands for two letter language code) file. Add the following line at the end of the file after replacing the text on the right of the equals sign “=” with appropriate messages for that language. Do not change the text in English on the left of the equals “=” sign.

```
com.ibm.passwordrules.standard.MinAgeConstraint=Minimum Password Age
```

4) The next step is to add a new message in tmsMessages.properties file. This is the message that will be displayed to the end user when this rule is violated.

a. Take a backup of $ITIM_HOME/data/tmsMessages.properties file.

b. Open $ITIM_HOME/data/tmsMessages.properties file in any text editor.

c. Add the following line at the end of this file.

```
com.ibm.passwordrules.MinAgeConstraint.MIN_AGE_VIOLATED=Attempting to set the password within minimum age of password.
```

d. Save the file and quit the editor.

If you have a language pack installed, then please repeat the above steps (a to d) on each of the $ITIM_HOME/data/tmsMessages_nn.properties (where nn stands for two letter language code) file. In these files you can add the above line after replacing the text on the right of the equals “=” sign with appropriate message for that language. Do not change the text in English on the left of the equals “=” sign.

5) Start the application server.

Now you should able to see ‘Minimum Password Age’ rule under Manage Password Policies>Rule Tab and you can specify appropriate value for the minimum password age.

Please note the following salient features of this new rule:

1. ‘Minimum Password Age’ Rule accepts only Integer value that specifies the minimum period of time, **in hours**, a password changed by a user on their account must be used before the user can change it again.
2. The integer value specified for the rule will be interpreted by ITIM application as the number of **hours**. When a negative value or 0 or no value is specified, ITIM will not evaluate the rule; In other words this will allow the user to change the password on their account immediately.
3. This rule will be evaluated only when a user tries to change the password on any of the accounts owned by them and the previous password change on that account was successfully executed by the same user (owner of the account). In other words this rule will not be evaluated if the previous password change on the account was performed by someone else other than the owner of the account (like helpdesk or administrator or system).
4. This rule will not be evaluated when users change the password on accounts that are not owned by them. For example, this rule will not be evaluated when a help desk personnel or an administrator tries to change the password on some other user’s account. Also this rule will not be evaluated if the password change is initiated by the system (e.g. password change initiated by lifecycle rule or from a workflow initiated by automatic provisioning request etc).
5. ITIM maintains the information of who executed the last password change and at what time was the password change executed, in the directory server on each account object. If this data gets corrupted or these attributes get wiped off the account object due to some reasons then the rule will not get evaluated properly.
6. ITIM can only store the information about the password changes performed using ITIM application, SSUI or using ITIM APIs. So any information about password changes performed directly on the resource or using some other tool will not be used while evaluating this rule.