

Oracle FLEXCUBE  
Security Management System User Manual  
Release 4.3.1.0.0  
Part No E52075-01

**ORACLE**  
FINANCIAL SERVICES

**ORACLE**

## Table of Contents (index)

<b>1. SMS.....</b>	<b>3</b>
1.1. 7011 - Event Log Inquiry .....	4
1.2. 752 - Reset Primary Password .....	7
1.3. 753 - Enable/Disable User .....	10
1.4. 755 - Modify Login Status .....	13
1.5. 756 - User Prohibited Passwords.....	15
1.6. 757 - Inquiry For Logged In Users .....	18
1.7. 758 - Inquiry For Password .....	20
1.8. 766 - Secondary Password Expiry Date .....	23
1.9. 767 - Reset Secondary Password.....	26
1.10. 768 - Change Primary Password .....	29
1.11. 769 - Change Secondary Password .....	32
1.12. AT002 - Audit Trail Financial Transactions Inquiry .....	35
1.13. BA777 - Audit Trail Inquiry for Non-Financial Txns* .....	40
1.14. BAM04 - BA Audit Tasks Maintenance-Inquire.....	48
1.15. BAM10 - Restricted Accounts Maintenance .....	51
1.16. SM11A - Inquiry On Logged In Users .....	54
1.17. SMM02 - User Profile Maintenance .....	56
1.18. SMM03 - Task Profile Maintenance .....	66
1.19. SMM09 - User Prohibited Password Maintenance .....	70
1.20. SMM12 - User Class Cross Reference Maintenance .....	73
1.21. SMM13 - Template Transaction Limits .....	76

## 1. SMS

The FLEXCUBE Retail Security Management System (SMS) provides a security envelope within which, all the FLEXCUBE Retail application modules are executed. SMS maintains and controls access to users in the FLEXCUBE Retail system and ensures that only authorized users are allowed to use the system. Security definitions are broadly categorized into two parts namely host security definition and branch security definition. For the purpose of security and centralized control, it is recommended that all the security related definitions users are created at the HO and branch security definitions are important attributes of the user are modified at HO and downloaded to the branches. All the users of the bank can be broadly classified depending upon their role and seniority. Such classification is represented in FLEXCUBE Retail using templates. All the FLEXCUBE Retail transactions are linked to one or more such templates to define the access to the transactions for the respective class of users. Each user needs to have a user profile defined in the system. This user profile is linked to one of the templates.

## 1.1. 7011 - Event Log Inquiry

User logged in from different computer under a core banking network is allowed (although concurrent user log-ins is not allowed).

Using this option you can log the IP's under which the user ID was entered in the posting date. The system displays the date, time and action performed. The system displays the date, time and action performed.

### Definition Prerequisites

Not Applicable

### Modes Available

Not Applicable

### To perform event log inquiry

1. Type the fast path **7011** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Inquiries > Event Log Inquiry**.
2. The system displays the **Event Log Inquiry** screen.

### Event Log Inquiry

Seq No	User ID	Date	Terminal IP	Action

**Field Description**

Field Name	Description
<b>User Name</b>	[Display] This field displays the name of the user who is logged in.
<b>From</b>	[Mandatory, dd/mm/yyyy] Type the date from which the event log inquiry is to be made.
<b>To</b>	[Mandatory, dd/mm/yyyy] Type the date till which the event log inquiry is to be made.

Column Name	Description
<b>Seq No</b>	[Display] This column displays the sequence number of the event.
<b>User ID</b>	[Display] This column displays the user id.
<b>Date</b>	[Display] This column displays the date and time of the event.
<b>Terminal IP</b>	[Display] This column displays the terminal IP from where the user had logged in.
<b>Action</b>	[Display] This column displays the action performed by the user.

3. Enter the from and to date.
4. Click the **Get** button. The system displays the event log details.

## Event Log Inquiry

Event Log Inquiry					
User Name:	TRITU	From:	12/02/2007	To:	31/08/2008
Seq No	User ID	Date	Terminal IP	Action	
1	TRITU	2008-07-19 09:38:21	IFLMUD5DL124G	Logged In	
2	TRITU	2008-07-18 14:44:53	IFLMUD5DL124G	Logged Out	
3	TRITU	2008-07-18 14:22:47	IFLMUD5DL124G	Logged In	
4	TRITU	2008-07-18 11:58:58	IFLMUD5DL124G	Logged In	
5	TRITU	2008-07-18 11:54:00	IFLMUD5DL124G	Logged Out	
6	TRITU	2008-07-18 11:10:54	IFLMUD5DL124G	Logged In	
7	TRITU	2008-07-18 11:06:05	IFLMUD5DL124G	Logged Out	
8	TRITU	2008-07-18 10:44:20	IFLMUD5DL124G	Logged In	
9	TRITU	2008-07-18 10:11:20	IFLMUD5DL124G	Logged Out	
10	TRITU	2008-07-18 09:39:38	IFLMUD5DL124G	Logged In	
11	TRITU	2008-07-15 15:31:29	IFLMUD5DL124G	Logged Out	
12	TRITU	2008-07-15 15:09:37	IFLMUD5DL124G	Logged In	
13	TRITU	2008-07-15 14:46:16	IFLMUD5DL124G	Logged Out	
14	TRITU	2008-07-15 14:32:03	IFLMUD5DL124G	Logged In	
15	TRITU	2008-07-15 14:05:55	IFLMUD5DL124G	Logged Out	
16	TRITU	2008-07-15 14:20:53	IFLMUD5DL124G	Logged In	
17	TRITU	2008-07-15 14:20:27	IFLMUD5DL124G	Logged Out	
18	TRITU	2008-07-15 14:19:15	IFLMUD5DL124G	Logged In	
19	TRITU	2008-07-15 14:19:05	SVSDOC	Admin Logged Out User	
20	TRITU	2008-07-15 14:18:40	IFLMUD5DL124G	Already Logged In	

5. Click the **Cancel** button.

## 1.2. 752 - Reset Primary Password

Using this option you can reset the password without entering the old one .This option is used by the system administrator to reset the password if the user has forgotten his password or if the SM does not want the user to log into the system. If the user knows the new password, he will be prompted to change it on login.

### Definition Prerequisites

- SMM02 - User Profile Maintenance

### Modes Available

Not Applicable

### To reset the primary password

1. Type the fast path **752** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Reset primary password**.
2. The system displays the **Reset Primary Password** screen.

### Reset Primary Password

**Field Description**

Field Name	Description
<b>Branch Code</b>	[Mandatory, Numeric, Four, Pick List] Type the branch code or select it from the pick list. The name of the branch is displayed in the adjacent field.
<b>User ID</b>	[Mandatory, Pick List] Select the user ID whose password you want to reset from the pick list. These user IDs are added and maintained in the <b>User Profile Maintenance</b> (Fast Path: SMM02) option.
<b>Password</b>	[Mandatory, Alphanumeric, 10] Type the password, for the selected user ID. The password should have a minimum of six characters. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.
<b>Verify Password</b>	[Mandatory, Alphanumeric, 10] Type the new password to verify it. It should be the same as entered in the <b>Password</b> field.

3. Select the user ID from the drop-down list.
4. Enter the required information in the various fields.

**Reset Primary Password**

Reset Primary Password\*

Branch Code :	11	...	MUMBAI
User ID :	TSUDEEP11	...	
Password :	*****		
Verify Password :	*****		

Card    Change Pin    Cheque    Cost Rate    Denomination    Instrument    Inventory    Pin Validation    Service Charge    Signature    Travellers Cheque

UDF    OK    Close    Clear

5. Click the **Ok** button.

### 1.3. 753 - Enable/Disable User

Using this option you can enable/ disable a user of any branch through single administrator log in. The user IDs are created in the **User Profile Maintenance** (Fast Path: SMM02) option.

**Note:** The system cannot disable the already logged in users.

#### Definition Prerequisites

- SMM02 - User Profile Maintenance

#### Modes Available

Not Applicable

#### To enable or disable a user

1. Type the fast path **753** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Enable / Disable user**.
2. The system displays the **Enable / Disable User** screen.

#### Enable / Disable User

The screenshot shows the 'Enable / Disable User' window. The window title is 'Enable / Disable User\*'. It contains the following fields:

- Branch Code :
- User ID :
- User Name :
- Status :  Permanently Disable :
- Logged in :

At the bottom of the window, there is a row of buttons:

- Card
- Change Pin
- Cheque
- Cost Rate
- Denomination
- Instrument
- Inventory
- Pin Validation
- Service Charge
- Signature
- Travellers Cheque
- UDF
- OK
- Close

**Field Description**

Field Name	Description
<b>Branch Code</b>	[Mandatory, Numeric, Four, Pick List]  Type the branch code or select it from the pick list.  The name of the branch is displayed in the adjacent field.
<b>User Id</b>	[Mandatory, Pick List]  Select the ID of the user, who has to be enabled or disabled, from the pick list.  These user ID's are maintained in the <b>User Profile Maintenance</b> (Fast Path: SMM02) option.
<b>User Name</b>	[Display]  This field displays the name of the user for the selected user ID.
<b>Status</b>	[Mandatory, Drop-Down]  Select the status from the drop-down list.  The options are: <ul style="list-style-type: none"> <li>• ENABLE</li> <li>• DISABLE</li> <li>• LOCK : Select this option to unlock a user ID.</li> </ul>
<b>Permanently Disable</b>	[Conditional, Check Box]  Select the check box to permanently disable a user.  This field is enabled only if <b>DISABLE</b> option is selected in the <b>Status</b> drop-down list.
<b>Logged in</b>	[Display]  This field displays the logged in status of the user.  The options are: <ul style="list-style-type: none"> <li>• Y: User is logged in.</li> <li>• N: User is not logged in.</li> </ul>

3. Select the branch code and user ID from the pick list.

## Enable / Disable User

Enable / Disable User\*

Branch Code : 12 ... MUMBAI

User ID : TSANGU12 ...

User Name : First Teller

Status :  ENABLE  Permanently Disable :

Logged in : N

Card Change Pin Cheque Cost Rate Denomination Instrument Inventory Pin Validation Service Charge Signature Travellers Cheque

UDF OK Close

4. If the user is disabled, the system displays the message "User is Disabled. Do You Want to Enable".
5. If the user is not logged in, the system displays the "User Not Logged in. Want to Disable?".
6. Click the **Ok** button.

## 1.4. 755 - Modify Login Status

Using this option you are forcibly logged out of the system. This option is used when you have logged into **FLEXCUBE** and the application/system crashes. When you try to login after the system is restored, it does not allow, as the system still maintains the user status as logged in. Also, the system will not permit a login more than once. In such cases this option is used to modify the login status.

### Definition Prerequisites

- SMM02 - User Profile Maintenance

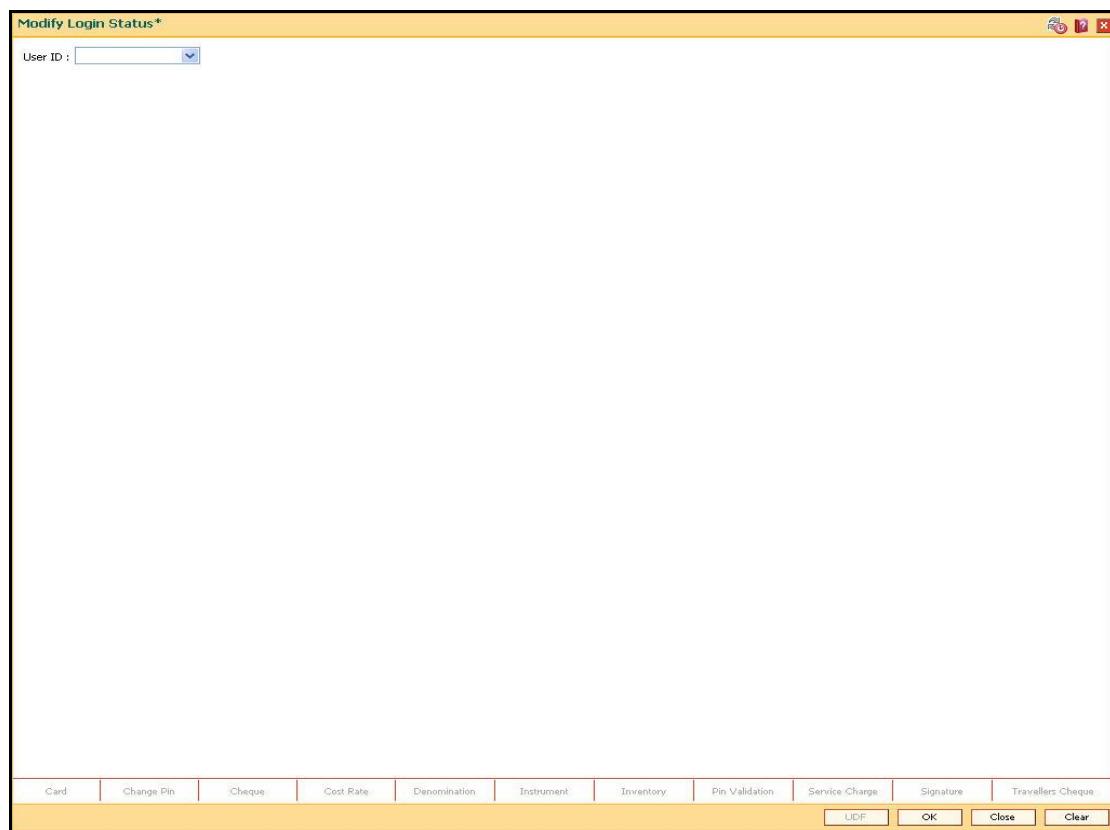
### Modes Available

Not Applicable

### To modify login status

1. Type the fast path **755** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Modify Login Status**.
2. The system displays the **Modify Login Status** screen.

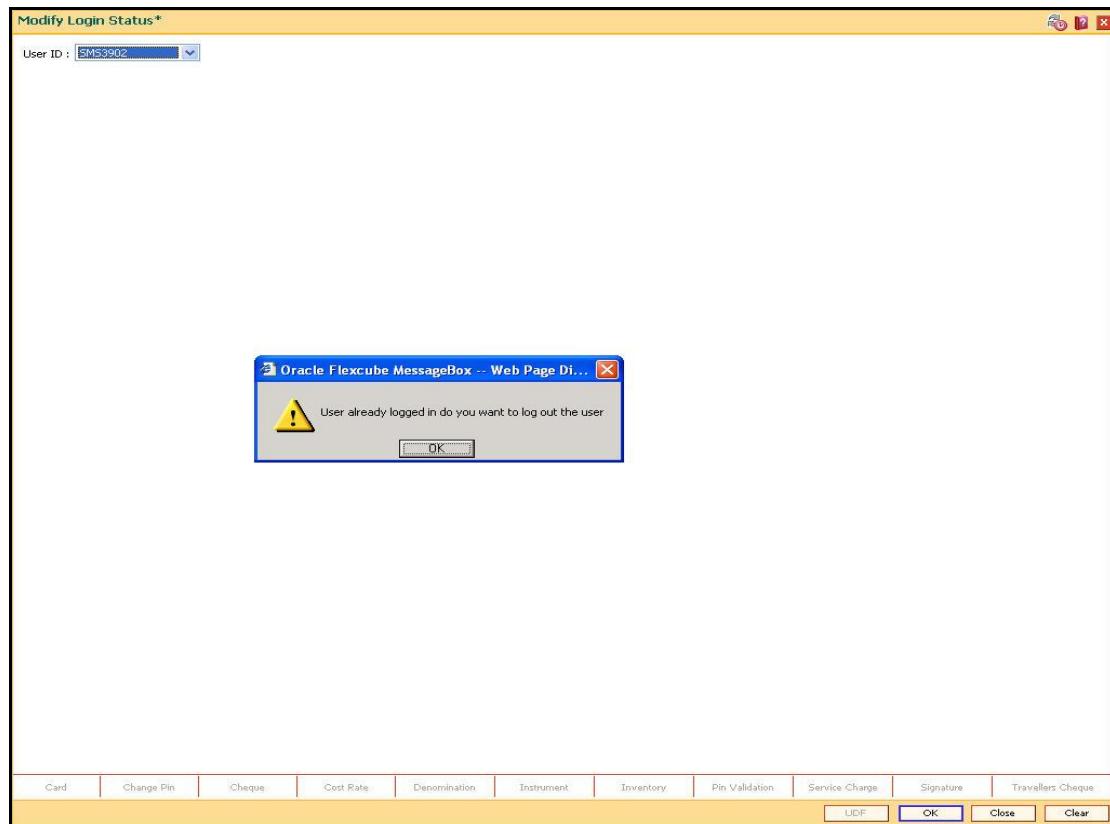
### Modify Login Status



**Field Description**

Field Name	Description
<b>User ID</b>	<p>[Mandatory, Drop-Down]</p> <p>Select the user ID of the user, whose login status is to be modified, from the drop-down list.</p> <p>These user ID's are maintained in the <b>Defining User Profile</b> (Fast Path: SMM02) option.</p>

3. Select the user ID from the drop-down list.

**Modify Login Status**

4. The system displays the message "User already logged in do you want to log out the user". Click the **OK** button.
5. Click the **OK** button.

## 1.5. 756 - User Prohibited Passwords

Using this option you can define those passwords which should not be used by particular user in the bank. These restrictions on using the password shall apply to only that user in the bank. These are commonly used words specific to the person such as place of residence, spouse name, name of son/daughters, etc.

### Definition Prerequisites

- SMM02 - User Profile Maintenance

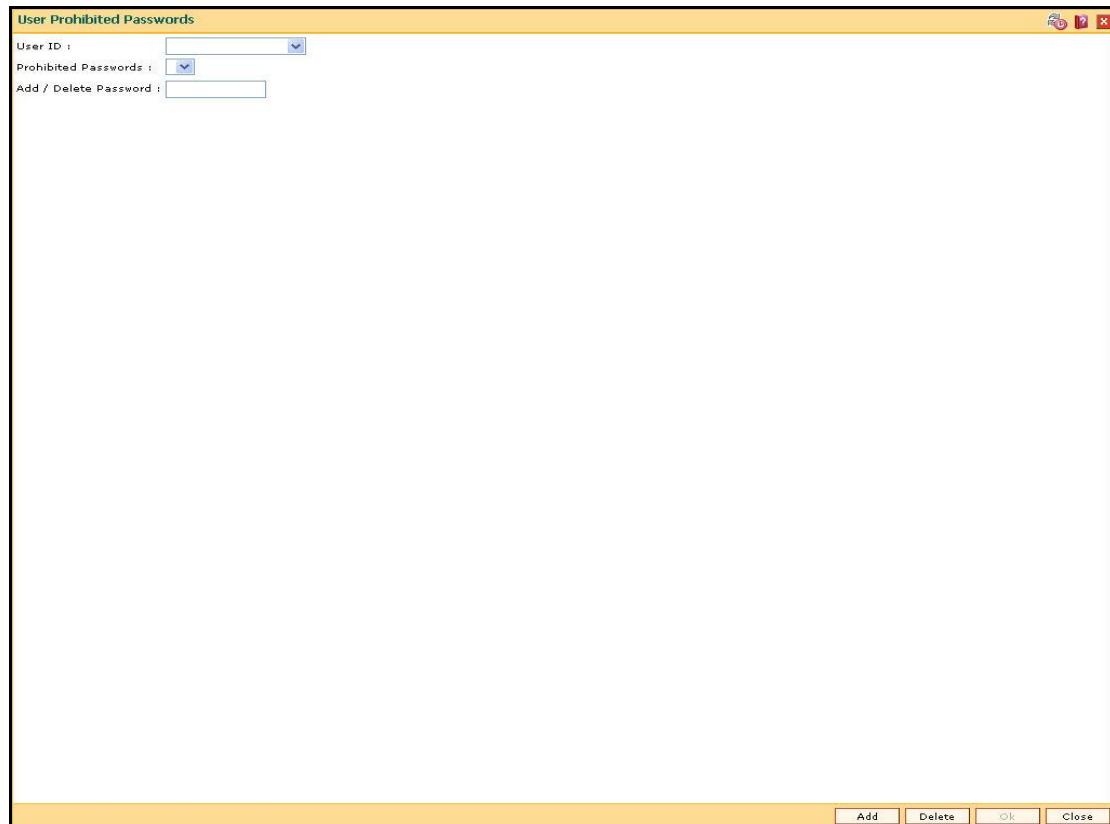
### Modes Available

Not Applicable

### To change the defined prohibited password

1. Type the fast path **756** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > User Prohibited Passwords**.
2. The system displays the **User Prohibited Passwords** screen.

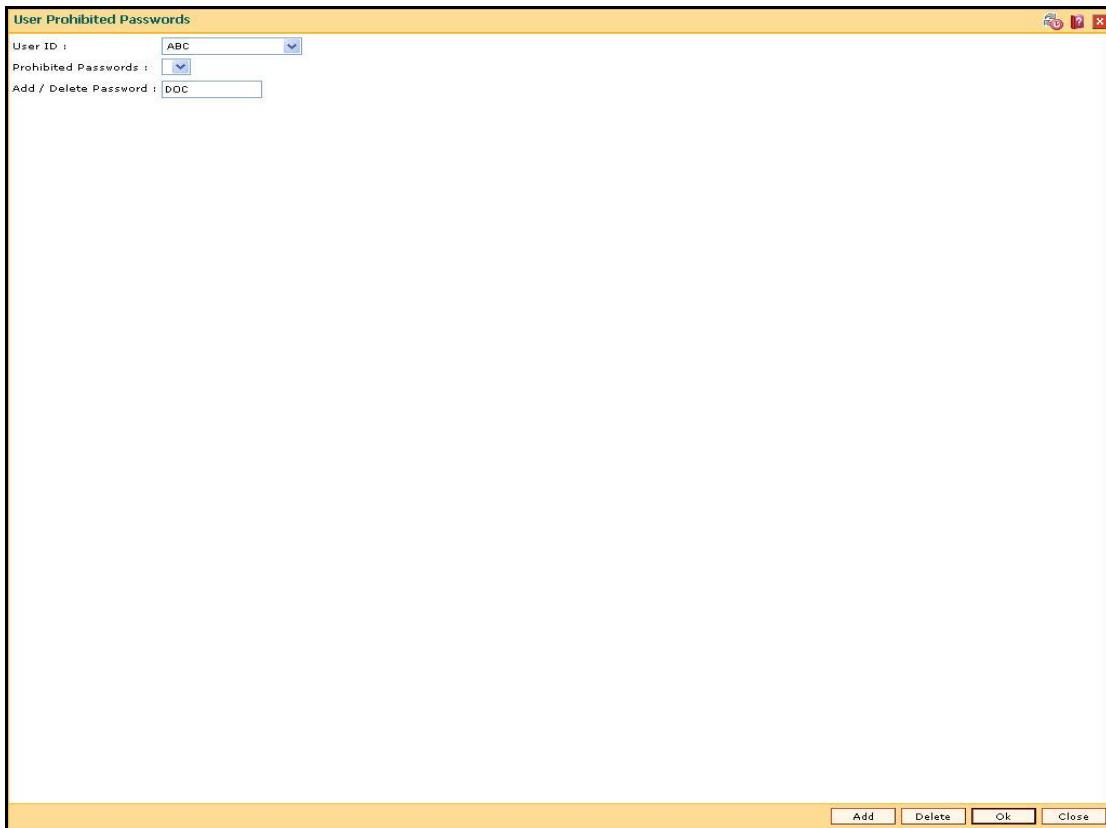
### User Prohibited Passwords



**Field Description**

Field Name	Description
<b>User ID</b>	[Mandatory, Drop-Down] Select the user ID from the drop-down list. These user IDs are added and maintained in the <b>Defining User Profile</b> (Fast Path: SMM02) option.
<b>Prohibited Passwords</b>	[Mandatory, Drop-Down] Select the prohibited password from the drop-down list. These prohibited passwords are added and maintained centrally in the <b>User Prohibited Password</b> option.
<b>Add / Delete Password</b>	[Mandatory, Alphanumeric, Eight] Type the password that is to be added or deleted. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.

3. Click the **Add** button.
4. The system displays the message "You are in Add option". Click the **OK** button.
5. The system displays the message "Data will be refreshed..Proceed?". Click the **OK** button.
6. The system refreshes the **User Prohibited Passwords** screen.
7. Select the user ID from the drop-down list.
8. Enter the prohibited password.

**User Prohibited Passwords**

9. Click the **Ok** button.
10. The system adds the prohibited password for that user ID.

## 1.6. 757 - Inquiry For Logged In Users

Using this option you can view the list of users that are logged in to the system in their own branch.

The system provides information on user ID, user name, the terminal ID in which the user has logged in and the login date and time. You can refresh the screen to get the latest status.

### Definition Prerequisites

Not Applicable

### Modes Available

Not Applicable

#### To view a list of currently logged in users

1. Type the fast path **757** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Inquiry For Logged In Users**.
2. The system displays the **Inquiry For Logged In Users** screen.

### Inquiry For Logged In Users

User ID	User Name	Terminal ID	Login Time
PGINA9999	First Teller	IFLNUIDSDLFT4G	16-DEC-2008 13:44:18
PRASA9999	First Teller	IFLNUIDSDLDX4G	16-DEC-2008 13:48:01
SDEVIDEA1	First teller	IFLEXPKW480	16-DEC-2008 15:18:03
SLIN9999	First Supervisor	IFLNUIDSDL5P4G	16-DEC-2008 15:56:24
SMATHIAS	First Supervisor	IFLNUIDSDLGP4G	16-DEC-2008 13:47:00
SMS3902	sms 39 test	IFLNUIDSIM0291	16-DEC-2008 14:47:08
SNELSON	First Supervisor	MyComputer	16-DEC-2008 16:02:01
SNISHIP	First teller	IFLNUIDSHP0162	16-DEC-2008 12:59:53
SPARAGP	First Supervisor	IFLNUIDSHP0885	16-DEC-2008 10:56:25
SRAJATC	First Supervisor	IFLNUIDSDL9X4G	16-DEC-2008 14:16:01
SROHIT	First Supervisor	IFLNUIDSHP0892	16-DEC-2008 14:26:46
SSAMEER	First Supervisor	MyComputer	16-DEC-2008 15:16:10
SSANDEEP	First Supervisor	IFLNUIDSIM0351	16-DEC-2008 13:54:34
SSENTHILV	First Supervisor	IFLNUIDSHP0716	16-DEC-2008 12:26:29
SVISHWAS	First Supervisor	IFLNUIDSHP0527	16-DEC-2008 11:20:09
SYLOAN	First System Administrator	IFLNUIDSHP2016	16-DEC-2008 15:46:52
TADITYAK	First teller	IFLNUIDSIM0249	16-DEC-2008 14:00:18
TAGARWAL	First teller	IFLNUIDSIM0303	16-DEC-2008 16:01:18
TBCHIT	First teller	IFLNUIDSDL174G	16-DEC-2008 14:12:55
TCHAITANYA	First teller	0	16-DEC-2008 15:47:10

1 3 1 2 3  
Refresh

Card | Change Pin | Cheque | Cost Rate | Denomination | Instrument | Inventory | Pin Validation | Service Charge | Signature | Travellers Cheque | UDF | Close

**Field Description**

Column Name	Description
<b>User ID</b>	[Display] This column displays the user ID for all those users who are currently logged into the system.
<b>User Name</b>	[Display] This column displays the list of users who are currently logged into the system.
<b>Terminal ID</b>	[Display] This column displays the identification code of the terminal where each user has logged into the system.
<b>Login Time</b>	[Display] This column displays the login date and time when the users have logged into the system.

3. The system displays the users who are currently logged in to the system.
4. Click the **Refresh** button to refresh the screen with the latest details.

## 1.7. 758 - Inquiry For Password

Using this option you can view the password details of the registered users . The system provides information on dual password facility available for the user IDs, primary password change due date, secondary password change due date, whether the system manger can reset the password, etc.

The inquiry about the passwords of the users will be useful for the supervisor mainly to keep track of the users for whom password reset is to be done, and if password change by Supervisor is allowed for the user.

You can change the primary/secondary passwords by using **Change Primary Password** (Fast Path: 768) and **Change Secondary Password** (Fast Path: 769) options.

### Definition Prerequisites

Not Applicable

### Modes Available

Not Applicable

### To view password details

1. Type the fast path **758** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Inquiry For Password**.
2. The system displays the **Inquiry For Password** screen.

## Inquiry For Password

Inquiry For Password						
User ID	Dual Pswd?	Change Pswd?	Pswd Reset?	Pri Password Change Due on	Sec Password Change Due on	
ABC	N	N	P	09-NOV-2008	01-JAN-1800	
ANANDVW	N	N	P	03-MAR-2009	01-JAN-1800	
API_SUPER	N	N	P	23-JUL-2008	23-JUL-2008	
API_USER	N	N	P	07-JUL-2008	07-JUL-2008	
ATM_USER	N	N	P	07-JUL-2008	07-JUL-2008	
CIFTEST01	N	N	P	11-FEB-2009	01-JAN-1800	
CIFTEST02	N	N	P	23-MAR-2008	01-JAN-1800	
GEFUONLY	N	N	P	22-JUN-2008	22-JUN-2008	
LSMS5306	N	N	N	15-FEB-2009	01-JAN-1800	
PCECILIA9999	N	N	N	08-JAN-2009	08-JAN-2009	
PGINA9999	N	N	N	08-JAN-2009	08-JAN-2009	
PRASA9999	N	N	N	08-JAN-2009	08-JAN-2009	
PVMT_USER	N	N	P	07-JUL-2008	07-JUL-2008	
REGTEST01	N	N	P	12-NOV-2008	01-JAN-1800	
SABHAY	N	N	N	13-FEB-2009	13-JUN-2008	
SABHAYP	N	N	N	06-FEB-2009	19-JUN-2008	
SABHDEET	N	N	N	16-MAR-2009	13-JUN-2008	
SADITYAK	N	N	N	11-FEB-2009	04-DEC-2008	
SAGARWAL	N	N	N	27-JAN-2009	13-JUN-2008	
SAMAR	N	N	N	15-FEB-2009	13-JUN-2008	
SAMIT	N	N	N	05-FEB-2009	13-JUN-2008	
SAMITESH	N	N	N	08-FEB-2009	13-JUN-2008	
SAMITS	N	N	P	05-JUL-2008	05-JUL-2008	
SAMLESH	N	N	P	13-JUN-2008	13-JUN-2008	
SANAND	N	N	N	23-FEB-2009	01-JAN-1800	
SANAND1	N	N	P	23-MAR-2008	01-JAN-1800	
SANILG	N	N	P	23-MAR-2008	01-JAN-1800	
SANIRBAN	N	N	N	11-MAR-2009	14-JUN-2008	
SANOOP	N	N	N	05-MAR-2009	13-JUN-2008	
SANUP	N	N	N	05-MAR-2009	14-JUN-2008	
SAPARNAR	N	N	N	09-FEB-2009	23-JUN-2008	
SASHISH	N	N	P	08-APR-2008	01-JAN-1800	
SASHWANI	N	N	P	29-JUN-2008	29-JUN-2008	
SASTI9999	N	N	N	05-JAN-2009	05-JAN-2009	
SAVADHESH	N	N	N	22-FEB-2009	05-JUN-2008	
SBABITA	N	N	N	10-FEB-2009	25-JUN-2008	
SBABU	N	N	P	16-MAR-2009	07-DEC-2008	
SBANDITA	N	N	N	04-FEB-2009	14-JUN-2008	
SBHAGWAT	N	N	N	16-FEB-2009	13-JUN-2008	
SBHARATH	N	N	P	13-JUN-2008	13-JUN-2008	
SBICHIT	N	N	N	27-JAN-2009	13-JUN-2008	
SCECILIA9999	N	N	N	05-JAN-2009	05-JAN-2009	
SCHAITANYA	N	N	N	08-FEB-2009	04-DEC-2008	
SCHUNDIGAR	N	N	P	08-APR-2008	01-JAN-1800	
SDARSINI	N	N	P	13-JUN-2008	13-JUN-2008	
SDEEPAK	N	N	N	01-FEB-2009	13-JUN-2008	
SDEEPAKM	N	N	P	28-JUN-2008	28-JUN-2008	
SDREVANAM	N	N	P	09-JUL-2008	09-JUL-2008	

### Field Description

Column Name	Description
<b>User ID</b>	[Display] This column displays the list of user IDs of the system.
<b>Dual Pswd?</b>	[Display] This column displays whether the user ID has dual password facility or not. The system displays: <ul style="list-style-type: none"><li>• Y: if the user ID has dual password facility.</li><li>• N: if the user ID does not have dual password facility.</li></ul>
<b>Change Pswd?</b>	[Display] This column displays whether the user can change his/her password or not. The system displays: <ul style="list-style-type: none"><li>• Y: if the user can change the password.</li><li>• N: if the user cannot change the password.</li></ul>

Column Name	Description
<b>Pswd Reset?</b>	[Display] This column displays the status of the user's password. The system displays: <ul style="list-style-type: none"><li>• P: if the security manager resets the user's password</li><li>• N: if the user logs in and changes the password</li></ul>
<b>Pri Password Change Due on</b>	[Display] This column displays the date on which the primary password is due for change.
<b>Sec Password Change Due on</b>	[Display] This column displays the date on which the secondary password is due for change.

3. Click the **Close** button.

## 1.8. 766 - Secondary Password Expiry Date

Using this option you can change the date on which a particular user's secondary password will expire.

While the users can view the password details like primary password change due date, secondary password change due date, etc. in **Inquiry For Password** (Fast Path: 758) option they can change the primary/secondary passwords by using **Change Primary Password** (Fast Path: 768) and **Change Secondary Password** (Fast Path: 769) options.

### Definition Prerequisites

- SMM02 - User Profile Maintenance

### Modes Available

Not Applicable

### To modify the secondary password expiry date

1. Type the fast path **766** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Secondary Password Expiry Date**.
2. The system displays the **Secondary Password Expiry Date** screen.

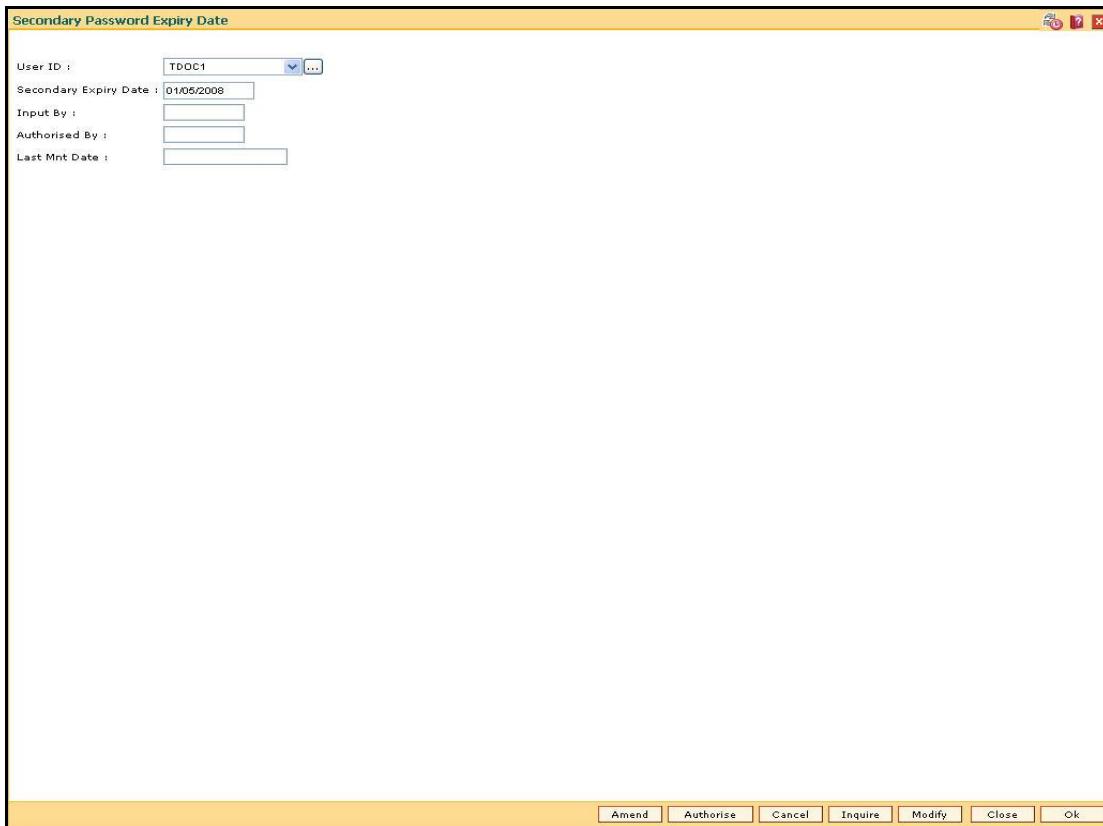
### Secondary Password Expiry Date

The screenshot shows the 'Secondary Password Expiry Date' screen. The title bar is yellow with the text 'Secondary Password Expiry Date'. The main area contains five input fields: 'User ID : TDOC1', 'Secondary Expiry Date : 01/05/2008', 'Input By : (empty)', 'Authorised By : (empty)', and 'Last Mnt Date : (empty)'. At the bottom is a yellow footer bar with buttons for 'Amend', 'Authorise', 'Cancel', 'Inquire', 'Modify', 'Close', and 'Ok'.

**Field Description**

Field Name	Description
<b>User ID</b>	[Mandatory, Pick List] Select the user ID from the pick list. These user IDs are added and maintained in the <b>Defining User Profile</b> (Fast Path: SMM02) option.
<b>Secondary Expiry Date</b>	[Mandatory, Numeric, dd/mm/yyyy] Type the new secondary expiry date for the password, which is greater than the current posting date. By default, this field displays the old expiry date. This date specifies the validity period of the password.
<b>Input By</b>	[Display] This field displays the user who has created the record. In the <b>Inquiry</b> mode, this field displays the user who had last maintained the record.
<b>Authorised By</b>	[Display] This field displays the user who has authorised the record.
<b>Last Mnt. Date</b>	[Display] This field displays the date and time when the record was last maintained.

3. Click the **Modify** button.
4. The system displays the message "Data will be refreshed..Proceed?". Click the **OK** button.
5. The system refreshes the **Secondary Password Expiry Date** screen.
6. Select the user id from the drop-down list or select it from the pick list.
7. Modify the relevant information in the various fields.

**Secondary Password Expiry Date**

8. Click the **Ok** button.
9. The system displays the message "The transaction completed successfully... Authorisation Pending". Click the **Ok** button.
10. The modified secondary password expiry date is reflected once the transaction is authorised.

## 1.9. 767 - Reset Secondary Password

Using this option you can reset the password without entering the old one . This option is used by the system administrator to forcibly to reset the password if the user has forgotten his password or if the SM does not want the user to log into the system. If the user knows the new password, he will be prompted to change it on login.

### Definition Prerequisites

- SMM02 - User Profile Maintenance

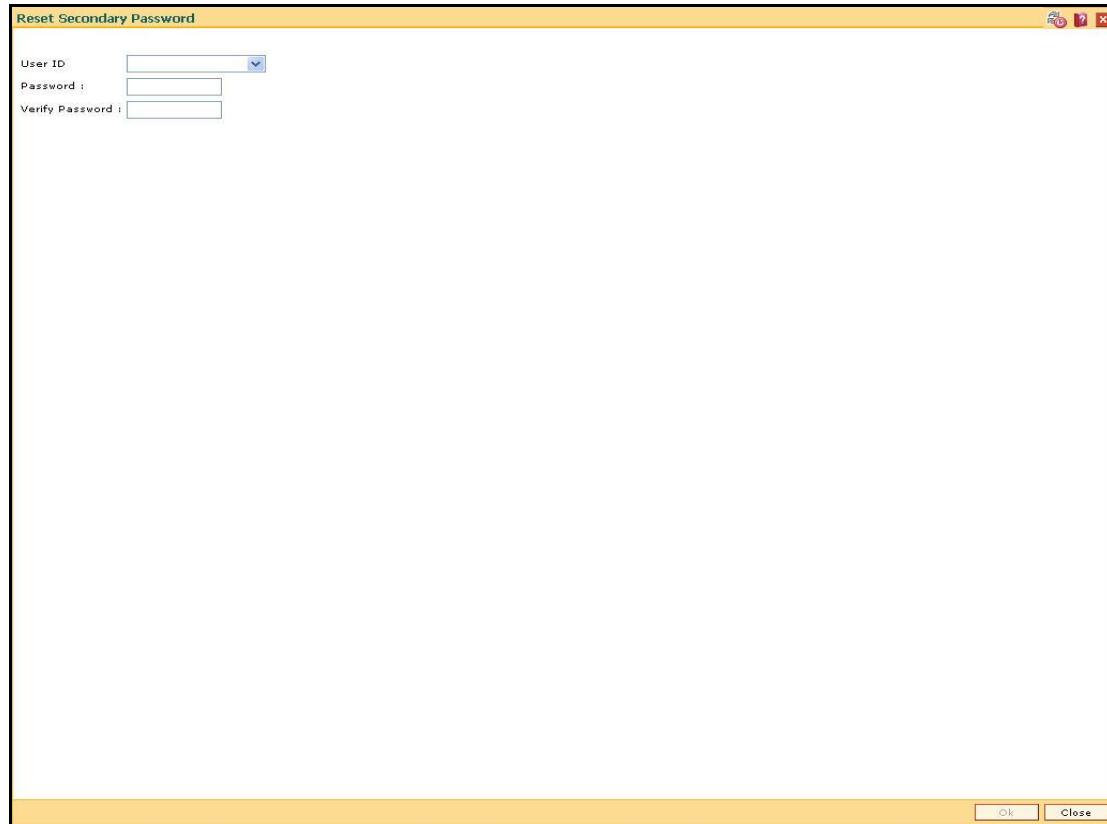
### Modes Available

Not Applicable

### To reset the secondary password

1. Type the fast path **767** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Reset Secondary Password**.
2. The system displays the **Reset Secondary Password** screen.

### Reset Secondary Password

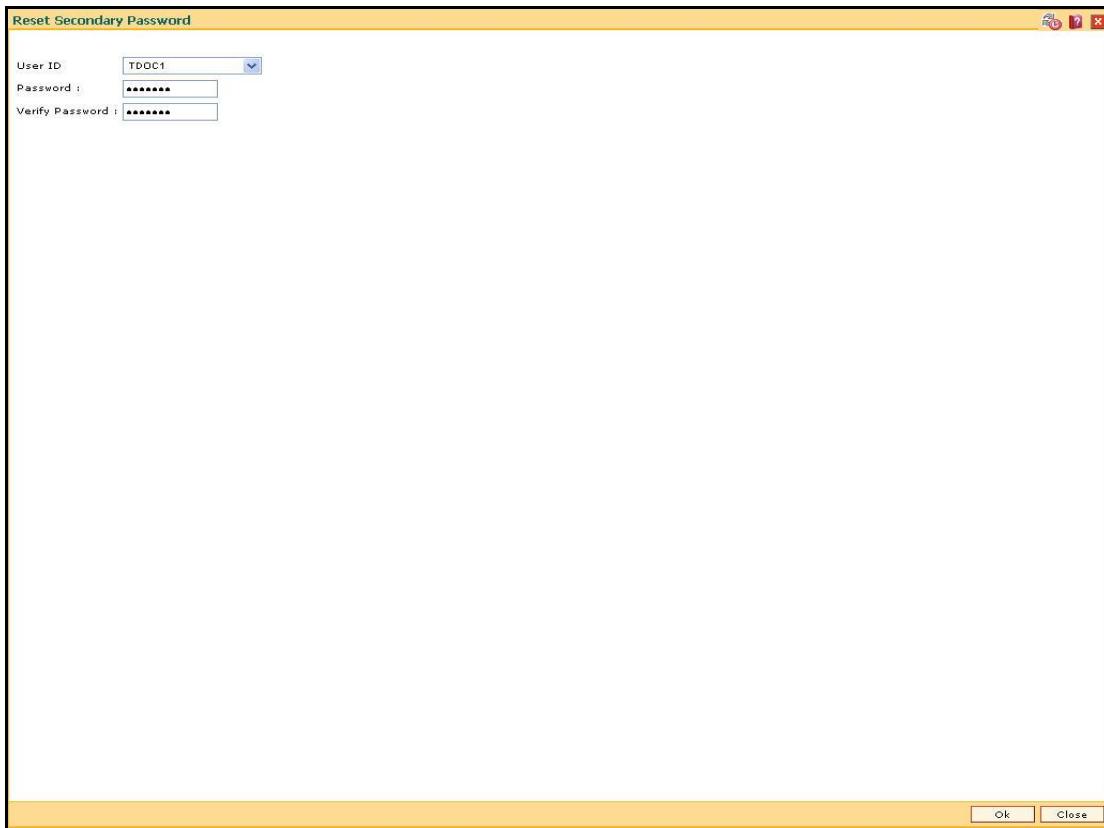


**Field Description**

Field Name	Description
<b>User ID</b>	<p>[Mandatory, Drop-Down] Select the user ID from the drop-down list. These user IDs are added and maintained in the <b>Defining User Profile</b> (Fast Path: SMM02) option.</p>
<b>Password</b>	<p>[Mandatory, Alphanumeric, 14] Type the new secondary password. It should have a minimum of eight characters. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.</p>
<b>Verify Password</b>	<p>[Mandatory, Alphanumeric, 14] Type the new password to verify it. It should be the same as entered in the <b>Password</b> field.</p>

3. Select the user ID from the drop-down list.
4. Enter the required information in the various fields.

**Reset Secondary Password**



5. Click the **Ok** button.

## 1.10. 768 - Change Primary Password

Using this option you can change your own password using the **Change Primary Password** option. You cannot use the passwords which are prohibited specifically in **User Prohibited Passwords** (Fast Path: 756) option. These are commonly used words specific to the person such as place of residence, spouse name, name of son/daughter, etc.

### Definition Prerequisites

Not Applicable

### Modes Available

Not Applicable

### To change primary password

1. Type the fast path **768** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Change Primary Password** .
2. The system displays the **Change Primary Password** screen.

### Change Primary Password

**Field Description**

Field Name	Description
<b>Old Password</b>	[Mandatory, Alphanumeric, 10] Type the valid current or old password.
<b>New Password</b>	[Mandatory, Alphanumeric, 10] Type the new password, which you would like to use. The password should have a minimum of six characters. It should be a combination of an uppercase and lowercase letter, and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.
<b>Verify Password</b>	[Mandatory, Alphanumeric, 10] Type the new password again to verify it.

3. Type the old password.
4. Type the new password and re-type it for confirmation.

**Change Primary Password**

5. Click the **Ok** button.
6. The system changes the primary password.

## 1.11. 769 - Change Secondary Password

Using this option you can change your own secondary password using the **Change Secondary Password** option. You cannot use the passwords which are prohibited specifically in **User Prohibited Passwords** (Fast Path: 756) option. These are commonly used words specific to the person such as place of residence, spouse name, name of son/daughter, etc.

### Definition Prerequisites

Not Applicable

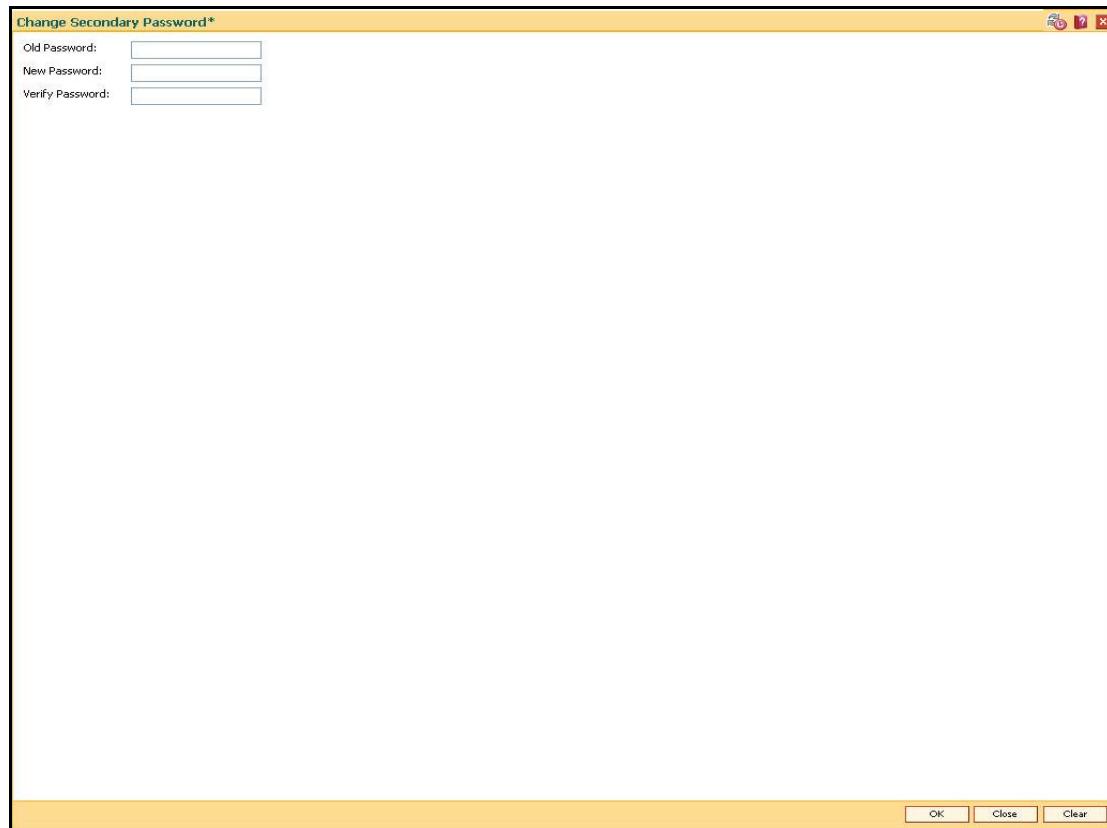
### Modes Available

Not Applicable

### To change secondary password

1. Type the fast path **769** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Change Secondary Password**.
2. The system displays the **Change Secondary Password** screen.

### Change Secondary Password

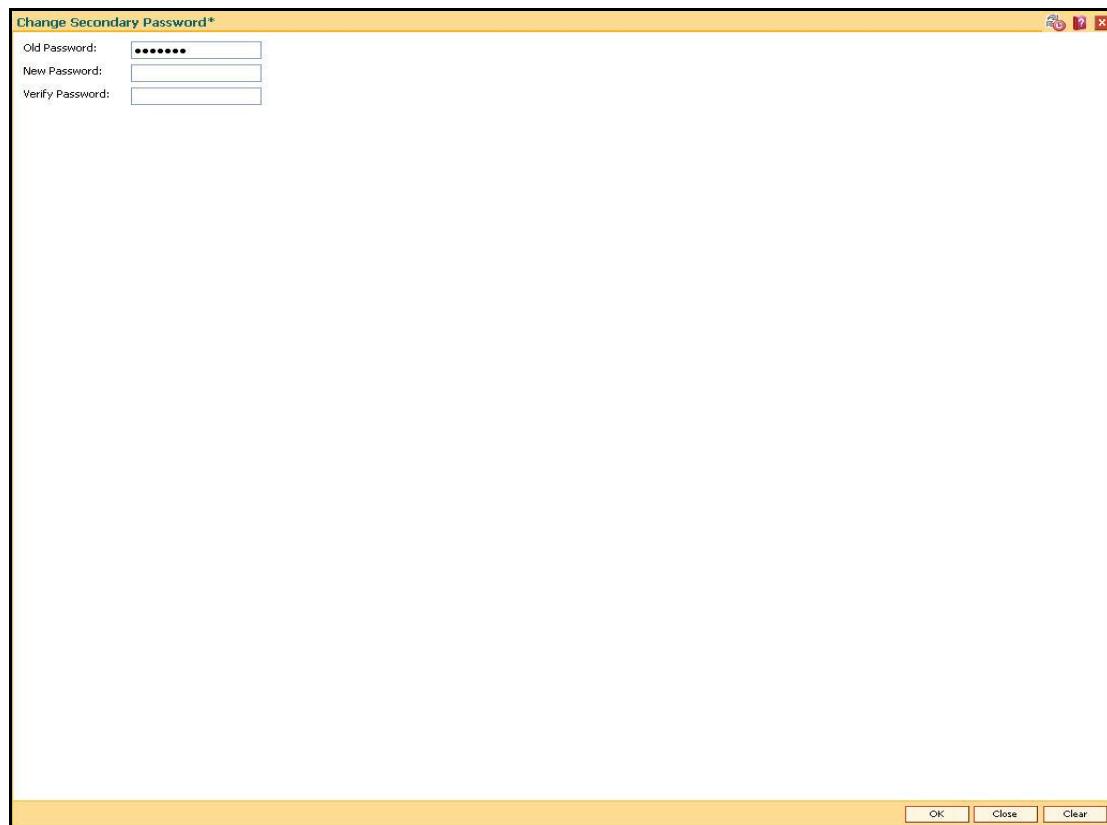


The screenshot shows a Windows-style dialog box titled "Change Secondary Password\*". Inside the dialog, there are three text input fields: "Old Password", "New Password", and "Verify Password". Each field has a small placeholder text "Enter password" inside it. At the bottom of the dialog, there is a horizontal bar with three buttons: "OK", "Close", and "Clear".

**Field Description**

Field Name	Description
<b>Old Password</b>	[Mandatory, Alphanumeric, 14] Type the valid current or old password.
<b>New Password</b>	[Mandatory, Alphanumeric, 14] Type the new password you would like to use. The password should have a minimum of eight characters. It should be a combination of an uppercase and lowercase letter, and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.
<b>Verify Password</b>	[Mandatory, Alphanumeric, 14] Type the new password to verify it.

3. Type the old password.
4. Type the new password and re-type it for confirmation.

**Change Secondary Password**


The screenshot shows a Windows-style dialog box titled "Change Secondary Password\*". Inside the dialog, there are three text input fields labeled "Old Password", "New Password", and "Verify Password". The "Old Password" field contains the masked password "\*\*\*\*\*". The "New Password" and "Verify Password" fields are empty. At the bottom of the dialog are three buttons: "OK", "Close", and "Clear".

5. Click the **Ok** button.
6. The system changes the secondary password.

## 1.12. AT002 - Audit Trail Financial Transactions Inquiry

Using this option you can view the audit trail of financial transactions performed on **Oracle FLEXCUBE**. The audit trail can be queried using this maintenance on any of the following parameters:

- Originating Branch
- Date Range
- Teller ID or Super ID
- Customer ID or Account Number
- Transaction mnemonic and/or Amount range
- Type of transaction, Transaction number

### Definition Prerequisites

- Financial Transactions should have been performed

### Modes Available

Not Applicable

### To inquire on audit trail

1. Type the fast path **AT002** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Inquiries > Audit Trail Financial Transactions Inquiry**.
2. The system displays the **Audit Trail Financial Transactions Inquiry** screen.

## Audit Trail Financial Transactions Inquiry

## Field Description

Field Name	Description
<b>Originating Branch</b>	[Mandatory, Drop-Down] Select the originating branch, for which the audit trail is required, from the drop-down list.
<b>Mnemonic</b>	[Optional, Pick List] Select the maintenance task code to be audited from the pick list.
<b>Date From</b>	[Mandatory, Pick List, dd/mm/yyyy] Select the date from which the data has to be retrieved from the pick list.
<b>Date To</b>	[Mandatory, Pick list, dd/mm/yyyy] Select the date up to which the data has to be retrieved from the pick list.
<b>Customer ID</b>	[Optional, Alphanumeric, 10] Type the id of the customer on whom the maintenance was done.

Field Name	Description
<b>Account Number</b>	[Optional, Numeric, 16] Type the account number on which the maintenance was done.
<b>Teller ID</b>	[Mandatory, Drop-Down] Select the id of the teller who has performed the maintenance from the drop-down list.
<b>Super ID</b>	[Optional, Drop-Down] Select the id of the authoriser who has authorised the maintenance from the drop-down list.
<b>Amount From</b>	[Optional, Alphanumeric, 13, Two] Type the minimum amount from which the records are to be displayed.
<b>Amount To</b>	[Optional, Alphanumeric, 13, Two] Type the maximum amount upto which the records are to be displayed.
<b>DR/CR</b>	[Optional, Character, One] Enter the type of transaction. You can type D or C to view the debit or credit transactions.
<b>Txn No</b>	[Optional, Alphanumeric, 40] Type the transaction number for which the records are to be displayed.

Column Name	Description
<b>Txn Date</b>	[Display] This column displays the date of transaction.
<b>Posting Date</b>	[Display] This column displays the posting date.
<b>Txn Type</b>	[Display] This column displays the type of transaction.
<b>Customer ID</b>	[Display] This column displays the id of the customer on whom the maintenance was done.
<b>Account No</b>	[Display] This column displays the account number on whom the maintenance was done.

Column Name	Description
<b>Amount</b>	[Display] This column displays the transaction amount.
<b>Dr/Cr</b>	[Display] This column displays the type of transaction i.e Debit or Credit.
<b>Currency</b>	[Display] This column displays the account currency.
<b>Mnemonic</b>	[Display] This column displays the transaction mnemonic.
<b>Narration</b>	[Display] This column displays the narration for the transaction.
<b>Tran No</b>	[Display] This column displays the transaction number.
<b>Teller ID</b>	[Display] This column displays the id of the teller who has performed the transaction.
<b>Auth ID</b>	[Display] This column displays the id of the authoriser who has authorised the transaction.

3. Select the originating branch and teller id from the drop-down list.
4. Enter the date range for which transactions are to be displayed.
5. Click the **Ok** button. The system displays the financial transactions based on the criteria entered.

## Audit Trail Financial Transactions Inquiry

**Audit Trail Financial Transactions Inquiry\***

Originating Branch :	HOHousingDevelopmentFinanceCorp	Mnemonic:	<input type="text"/>							
Date From :	31/03/2000	Date To :	31/03/2008							
Customer ID:	<input type="text"/>	Account Number:	<input type="text"/>							
Teller Id :	TNELSON	Super Id :	<input type="text"/>							
Amount From:	<input type="text"/>	Amount To:	<input type="text"/>							
DR/CR:	<input type="text"/>	Txn No:	<input type="text"/>							
Txn Date	Posting Date	Txn Type	Customer ID	Account No	Amount	Dr/Cr	Currency	Mnemonic	Narration	Tran no
31/12/2009	30/01/2008	Normal	606348	06063480000052	25,000.00	D		1001	Cash Withdrawal	000562008013000920
31/12/2009	30/01/2008	Normal	606348	99990111010011	25,000.00	C		1001	06063480000052;Cash Withdrawal	000562008013000920000
30/12/2009	30/01/2008	Normal	606348	06063480000039	50,000.00	D		1001	Cash Withdrawal	000562008013000920000
30/12/2009	30/01/2008	Normal	606348	99990111010011	50,000.00	C		1001	06063480000039;Cash Withdrawal	000562008013000920000
30/12/2009	30/01/2008	Normal	606348	99990111010011	50,000.00	C		1001	06063480000013;Cash Withdrawal	000562008013000920000
30/12/2009	30/01/2008	Normal	606348	99990111010011	50,000.00	C		1001	06063480000026;Cash Withdrawal	000562008013000920000
30/12/2009	30/01/2008	Normal	606348	06063480000026	50,000.00	D		1001	Cash Withdrawal	000562008013000920000

Card    Change Pin    Cheque    Cost Rate    Denomination    Instrument    Inventory    Pin Validation    Service Charge    Signature    Travellers Cheque

UDF    OK    Close    Clear

6. Click the **Close** button.

## 1.13. BA777 - Audit Trail Inquiry for Non-Financial Txns\*

A bank can view the trail of both financial and non-financial transactions performed on **FLEXCUBE**. Only those non-financial transactions for which audit trails are required can be inquired in this inquiry. This requirement is maintained in Audit Task Maintenance. The audit trail can be queried using this maintenance on any of the following parameters:

- Originating Branch
- Task ID
- Date Range
- Teller ID
- Authorizer ID
- Action

### Definition Prerequisites

- BAM04 - BA Audit Tasks Maintenance-Inquire

### Modes Available

Not Applicable

### To inquire on audit trail

1. Type the fast path **BA777** and click **Go** or navigate through the menus to **Global Definitions > Other > Audit Trail Inquiry for Non-Financial Txns**.
2. The system displays the **Audit Trail Inquiry for Non-Financial Txns** screen.

## Audit Trail Inquiry for Non-Financial Txns

## Field Description

Field Name	Description
<b>Originating Branch</b>	[Mandatory, Pick List] Select the originating branch, for which the audit trail is required, from the pick list.
<b>Task ID</b>	[Optional, Alphanumeric, Five] Type the maintenance task code being audited.
<b>From Date</b>	[Optional, Pick List, dd/mm/yyyy] Select the date from which the data has to be retrieved from the pick list.
<b>To Date</b>	[Optional, Pick list, dd/mm/yyyy] Select the date up to which the data has to be retrieved from the pick list.
<b>Teller ID</b>	[Optional, Alphanumeric, 16] Type the id of the teller who performed the maintenance.

Field Name	Description
<b>Authorizer ID</b>	[Optional, Alphanumeric, 36] Type the id of the authoriser who authorised the maintenance.
<b>Customer ID</b>	[Optional, Alphanumeric, 48] Type the id of the customer (if any) on whom the maintenance was done
<b>Account No.</b>	[Optional, Numeric, 16] Type the account number (if any) on which the maintenance was done.
<b>Action</b>	[Mandatory, Drop-Down] Select the maintenance action being audited from the drop-down list. The options are: <ul style="list-style-type: none"> <li>• Inquiry</li> <li>• Add</li> <li>• Modify</li> <li>• Delete</li> <li>• All</li> <li>• All Unauthorised</li> </ul> 3. Select the originating branch from the pick list. 4. Enter the required information. 5. Select the action from the drop-down list.

**Audit Trail Inquiry for Non-Financial Txns**

Originating Branch: 9999 ... Task ID: \_\_\_\_\_

From Date: 31/12/2007 To Date: 31/12/2007

Teller ID: TRAJI Authorizer ID: \_\_\_\_\_

Customer ID: \_\_\_\_\_ Account No: \_\_\_\_\_

Action : Inquiry

**Record Log** **Record Details**

Branch	Task ID	Posting Date	Teller ID	Authorizer ID	Action	Txn Date	Account No	Customer ID
--------	---------	--------------	-----------	---------------	--------	----------	------------	-------------

Inquire Close Clear Report Detail Report Exhaustive Report

6. Click the **Inquire** button.
7. The system displays the records matching the entered criteria.

## Record Log

Audit Trail Inquiry for Non-Financial Txns

Originating Branch:	9999	Task ID:																																																																									
From Date:	31/12/2007	To Date:	31/12/2007																																																																								
Teller ID:	TRAJI	Authorizer ID:																																																																									
Customer ID:		Account No.:																																																																									
Action :	Inquiry																																																																										
<input checked="" type="radio"/> Record Log <input type="radio"/> Record Details																																																																											
<table border="1"> <thead> <tr> <th>Branch</th> <th>Task ID</th> <th>Posting Date</th> <th>Teller ID</th> <th>Authorizer ID</th> <th>Action</th> <th>Txn Date</th> <th>Account No.</th> <th>Customer ID</th> </tr> </thead> <tbody> <tr><td>9999</td><td>CH021</td><td>31/12/2007</td><td>TRAJI</td><td></td><td>Inquiry</td><td>26/06/2008 14:46:50</td><td></td><td></td></tr> <tr><td>9999</td><td>CH021</td><td>31/12/2007</td><td>TRAJI</td><td></td><td>Inquiry</td><td>26/06/2008 14:45:32</td><td></td><td></td></tr> <tr><td>9999</td><td>BA078</td><td>31/12/2007</td><td>TRAJI</td><td></td><td>Inquiry</td><td>25/06/2008 11:03:30</td><td></td><td></td></tr> <tr><td>9999</td><td>CIM02</td><td>31/12/2007</td><td>TRAJI</td><td></td><td>Inquiry</td><td>24/06/2008 16:01:39</td><td></td><td></td></tr> <tr><td>9999</td><td>CHM01</td><td>31/12/2007</td><td>TRAJI</td><td></td><td>Inquiry</td><td>24/06/2008 10:43:22</td><td></td><td></td></tr> <tr><td>9999</td><td>CHM01</td><td>31/12/2007</td><td>TRAJI</td><td></td><td>Inquiry</td><td>24/06/2008 10:38:31</td><td></td><td></td></tr> <tr><td>9999</td><td>CHM01</td><td>31/12/2007</td><td>TRAJI</td><td></td><td>Inquiry</td><td>24/06/2008 10:38:10</td><td></td><td></td></tr> </tbody> </table>				Branch	Task ID	Posting Date	Teller ID	Authorizer ID	Action	Txn Date	Account No.	Customer ID	9999	CH021	31/12/2007	TRAJI		Inquiry	26/06/2008 14:46:50			9999	CH021	31/12/2007	TRAJI		Inquiry	26/06/2008 14:45:32			9999	BA078	31/12/2007	TRAJI		Inquiry	25/06/2008 11:03:30			9999	CIM02	31/12/2007	TRAJI		Inquiry	24/06/2008 16:01:39			9999	CHM01	31/12/2007	TRAJI		Inquiry	24/06/2008 10:43:22			9999	CHM01	31/12/2007	TRAJI		Inquiry	24/06/2008 10:38:31			9999	CHM01	31/12/2007	TRAJI		Inquiry	24/06/2008 10:38:10		
Branch	Task ID	Posting Date	Teller ID	Authorizer ID	Action	Txn Date	Account No.	Customer ID																																																																			
9999	CH021	31/12/2007	TRAJI		Inquiry	26/06/2008 14:46:50																																																																					
9999	CH021	31/12/2007	TRAJI		Inquiry	26/06/2008 14:45:32																																																																					
9999	BA078	31/12/2007	TRAJI		Inquiry	25/06/2008 11:03:30																																																																					
9999	CIM02	31/12/2007	TRAJI		Inquiry	24/06/2008 16:01:39																																																																					
9999	CHM01	31/12/2007	TRAJI		Inquiry	24/06/2008 10:43:22																																																																					
9999	CHM01	31/12/2007	TRAJI		Inquiry	24/06/2008 10:38:31																																																																					
9999	CHM01	31/12/2007	TRAJI		Inquiry	24/06/2008 10:38:10																																																																					
<input type="button" value="Inquire"/> <input type="button" value="Close"/> <input type="button" value="Clear"/> <input type="button" value="Report"/> <input type="button" value="Detail Report"/> <input type="button" value="Exhaustive Report"/>																																																																											

## Field Description

Field Name	Description
<b>Branch</b>	[Display] This column displays the originating branch for which the audit trail is required.
<b>Task ID</b>	[Display] This column displays the maintenance task code being audited.
<b>Posting Date</b>	[Display] This column displays the date from which the data has to be retrieved.
<b>Teller ID</b>	[Display] This column displays the id of the teller who performed the maintenance.
<b>Authorizer ID</b>	[Display] This column displays the id of the authoriser who authorised the maintenance.

## BA777 - Audit Trail Inquiry for Non-Financial Txns\*

Field Name	Description
<b>Action</b>	[Display] This column displays the maintenance action being audited.
<b>Txn Date</b>	[Display] This column displays the date of transaction.
<b>Account No</b>	[Display] This column displays the account number (if any) on whom the maintenance was done.
<b>Customer ID</b>	[Display] This column displays the id of the customer (if any) on whom the maintenance was done.

8. Double-click a record to view its details in the **Record Details** tab.

### Record Details

The screenshot shows the 'Audit Trail Inquiry for Non-Financial Txns' application window. The 'Record Details' tab is active. At the top, there are search fields for 'Originating Branch' (9999), 'From Date' (31/12/2007), 'Teller ID' (TRAJI), 'Customer ID' (empty), 'Task ID' (empty), 'To Date' (31/12/2007), 'Authorizer ID' (empty), and 'Account No.' (empty). Below the search fields are two tabs: 'Record Log' and 'Record Details' (which is highlighted). Under the 'Record Details' tab, there are fields for 'Originating Branch', 'Task Description', 'Posting Date' (01/01/1800), 'Teller ID', 'Authorizer ID', 'Customer ID', and 'Account No.'. Below these fields is a table with columns 'Type', 'Field', 'Old Value', and 'New Value'. The table contains the message 'NO DETAIL RECORDS AVAILABLE'. At the bottom of the window are buttons for 'Inquire', 'Close', 'Clear', 'Report', 'Detail Report', and 'Exhaustive Report'.

**Field Description**

Field Name	Description
<b>Originating Branch</b>	[Display] This field displays the originating branch for which the audit trail is required.
<b>Task Description</b>	[Display] This field displays the maintenance task description.
<b>Posting Date</b>	[Display] This field displays the date from which the data has to be retrieved.
<b>Teller ID</b>	[Display] This field displays the id of the teller who performed the maintenance.
<b>Authorizer ID</b>	[Display] This field displays the id of the authoriser who authorised the maintenance.
<b>Customer ID</b>	[Display] This field displays the id of the customer (if any) on whom the maintenance was done
<b>Account No</b>	[Display] This field displays the account number (if any) on whom the maintenance was done.

Column Name	Description
<b>Type</b>	[Display] This column indicates if this is a Key to identify the particular record in the <b>FLEXCUBE</b> database. Blank value indicates that this is not a <b>Key</b> field.
<b>Field</b>	[Display] This column displays the field name in the database which has changed. For a <b>Key</b> field, the actual value will also be indicated here.
<b>Old Value</b>	[Display] This column displays the previous value for the field being modified. This will be blank in case of <b>Add</b> option.

Column Name	Description
New Value	[Display] This column displays the new value for the field being modified. This will be blank in case of <b>Delete</b> option.
9.	Reports can be executed by clicking <b>Report</b> (Only Record Log Tab), <b>Detailed Report</b> (Only Record Details Tab for a particular selection) or <b>Exhaustive Report</b> (Complete details of all Record Log records).
10.	Click the <b>Close</b> button.
<b>Note:</b> The report output can then be viewed by navigating to the <b>Advice/Report Status Inquiry</b> option (Fast Path: 7778).	

## 1.14. BAM04 - BA Audit Tasks Maintenance-Inquire

Using this option you can decide the auditing matrix for a particular task. This option can be used to define whether an audit is allowed on a maintenance option, and the actions (add, modify, delete, etc.) from that window should be recorded in an audit log.

All online transactions with financial impact except for Voucher Entry transaction are recorded in the Electronic Journal (EJ) stored at the respective branch. This maintenance is used for auditing all the other transactions. The audit log is stored in the central host and is common to all the branches.

### Definition Prerequisites

- BAM15 - Transaction Mnemonic Codes

### Modes Available

Add By Copy, Add, Modify, Delete, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

### To add audit task details

1. Type the fast path **BAM04** and click **Go** or navigate through the menus to **Global Definitions > Other > BA Audit Tasks Maintenance-Inquire**.
2. The system displays the **BA Audit Tasks Maintenance-Inquire** screen.

### BA Audit Tasks Maintenance-Inquire

**Field Description**

Field Name	Description
<b>Task ID</b>	<p>[Mandatory, Pick List] Select the task ID from the pick list. Task ID lists all the transaction codes maintained in the <b>Transaction Mnemonic Codes</b> (Fast Path: BAM15) option. This ID acts like a fast path. The fast path is a mnemonic which allows the user to access the options.</p>
<b>Task Description</b>	<p>[Display] This field displays the description of the selected task code.</p>
<b>Maintenance Options</b>	
<b>Auditing Flag</b>	<p>[Mandatory, Check Box] Select the Auditing Flag check box, to enable the auditing flag. If the check box is selected, the details of the transaction will be recorded and stored for audit purposes. The maintenance options will also be enabled if the auditing flag is selected.</p>
<b>Inquire</b>	<p>[Conditional, Check Box] Select the Inquire check box, if you want the system to record the inquire actions and store the same for audit purposes. If the <b>Inquire</b> check box is selected it enables you to inquire about an authorised record. This field is enabled only if the <b>Auditing Flag</b> check box is selected.</p>
<b>Add</b>	<p>[Conditional, Check Box] Select the Add check box to enable you to add a new record to the selected task id. If the <b>Add</b> check box is selected, the system records the add actions and stores the same for audit purposes. This field is enabled only if the <b>Auditing Flag</b> check box is selected.</p>
<b>Modify</b>	<p>[Conditional, Check Box] Select the <b>Modify</b> check box to enable you to modify a record in the selected task id. If the Modify check box is selected, the system records the modify actions and stores the same for audit purposes. This field is enabled only if the <b>Auditing Flag</b> check box is selected.</p>

Field Name	Description
<b>Delete</b>	<p>[Conditional, Check Box]</p> <p>Select the Delete check box to enable you to delete a record from the selected task id.</p> <p>If the <b>Delete</b> check box is selected, the system records the delete actions and stores the same for audit purposes.</p> <p>This field is enabled only if the <b>Auditing Flag</b> check box is selected.</p>

3. Click the **Add** button.
4. Select the task ID from the pick list.
5. Select the auditing flag check box and the appropriate maintenance option check boxes.

### BA Audit Tasks Maintenance-Inquire

The screenshot shows the 'BA Audit Tasks Maintenance-Inquire' window. At the top, there are fields for 'Task ID' (1005) and 'Task Description' (Miscellaneous GL Transfer). Below these is a section titled 'Maintenance Options' with the following checkboxes:

- Auditing Flag:  (Y/N)
- Inquire:
- Add:
- Modify:
- Delete:

At the bottom of the window, there is a 'Record Details' section with fields for 'Input By', 'Authorized By', 'Last Mnt. Date', 'Last Mnt. Action', and 'Authorized'. Below this, there are buttons for 'UDF', 'Ok', 'Close', and 'Clear'. At the very bottom, there are buttons for 'Add By Copy', 'Add', 'Modify', 'Delete', 'Cancel', 'Amend', 'Authorize', and 'Inquiry'.

6. Click the **Ok** button.
7. The system displays the message "Record Added...Authorisation Pending..Click Ok to Continue". Click the **OK** button.
8. The audit task is added once the record is authorised.

## 1.15. BAM10 - Restricted Accounts Maintenance

Using this option you can restrict a particular teller from accessing the details of particular customer or GL accounts.

For example: If the bank decides to restrict the access to income and expenses accounts this option can be used. For a restricted account, the teller is not allowed to post any transaction, inquire, or maintain details.

### Definition Prerequisite

- SMM02 - User Profile Maintenance

### Modes Available

Add By Copy, Add, Modify, Delete, Cancel, Amend, Authorize, Inquire. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

### To add a teller restricted account

1. Type the fast path **BAM10** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Others > Restricted Accounts Maintenance**.
2. The system displays the **Restricted Accounts Maintenance** screen.

### Restricted Accounts Maintenance

The screenshot shows the 'Restricted Accounts Maintenance' screen. At the top, there are four input fields: 'User ID' (text box), 'Account Type' (dropdown menu set to 'Customer A/c'), 'Account No.' (text box), and 'Customer Name' (text box). Below these is a 'Remarks' text area. At the bottom, there is a toolbar with buttons for 'UDF', 'OK', 'Close', and 'Clear'. A status bar at the bottom shows 'Record Details' and buttons for 'Add By Copy' and other maintenance modes.

**Field Description**

Field Name	Description
<b>User ID</b>	<p>[Mandatory, Pick List] Select the user ID from the drop-down list. These user IDs are added and maintained in the <b>Defining User Profile</b> (Fast Path: SMM02) option. Once added, this field cannot be modified or amended.</p>
<b>Account Type</b>	<p>[Mandatory, Drop-Down] Select the account type on which restriction is to be imposed from the drop-down list. The options are:</p> <ul style="list-style-type: none"> <li>Customer A/C: It enables the <b>Account No</b> field in which you enter the customer account number.</li> <li>General Ledger A/C: It enables the <b>Account No</b> field in which you enter the GL account number.</li> </ul> <p>Once added, this field cannot be modified or amended.</p>
<b>Account No</b>	<p>[Mandatory, Alphanumeric, 16] Type the account number based on the selected account type. The system does not validate the status of the account.</p>
<b>Customer Name</b>	<p>[Display] This field displays the name of the customer if you select the <b>Customer A/C</b> option from the <b>Account Type</b> drop-down list.</p>
<b>Remarks</b>	<p>[Optional, Alphanumeric, 40] Type the reason for the restriction. This is for information purposes only.</p>

3. Click the **Add** button.  
 4. Select the user ID from the pick list and the account type from the drop-down list.  
 5. Enter the account number and press the **<Tab>** key.

## Restricted Accounts Maintenance

The screenshot shows the 'Restricted Accounts Maintenance' window. At the top, there are four input fields: 'User ID' (ABC), 'Account Type' (Customer A/c), 'Account No' (60000000006124), and 'Customer Name' (SURYA CHANDRATARE). Below these is a 'Remarks' field (Court Order). The window has a toolbar at the bottom with buttons for 'UDF', 'Ok', 'Close', and 'Clear'. A status bar at the bottom shows 'Record Details' and 'Input By'.

6. Click the **OK** button.
7. The system displays the message "Record Added...Authorisation Pending...". Click the **OK** button.
8. The teller restricted account is added once the record is authorised.

## 1.16. SM11A - Inquiry On Logged In Users

Using this option you can view the status of the currently logged in users for all the branches. The system provides information on user ID, user name, branch code and the terminal ID in which the user has logged in and the login date and time. You can refresh the screen to get the latest status.

### Definition Prerequisites

- SMM02 - User Profile Maintenance

### Modes Available

Not Applicable

### To inquiry on logged in users

1. Type the fast path **SM11A** and click **Go** or navigate through the menus to **Global Definitions > Security > Inquiry On Logged In Users**.
2. The system displays the **Inquiry On Logged In Users** screen.

### Inquiry On Logged In Users

User Id	User Name	Branch Code	Terminal Id	Login Time
PGINA9999	First Teller	9999	IFLMUD50LFT4G	16/12/2008 13:44:18
PRASA1000	First Teller	1000	IFLMUD50LDX4G	16/12/2008 13:46:05
PRASA9999	First Teller	9999	IFLMUD50LDX4G	16/12/2008 13:48:01
SDEVIDEA1	First teller	9999	IFLEXPKV480	16/12/2008 15:18:03
SLIN9999	First Supervisor	9999	IFLMUD50LSP4G	16/12/2008 15:50:12
SMATHIAS	First Supervisor	9999	IFLMUD50LGP4G	16/12/2008 13:47:00
SMS3902	sms 39 test	9999	IFLMUD50M0291	16/12/2008 14:47:08
SNELSON	First Supervisor	9999	IFLMUD50HP0316	16/12/2008 10:59:36
SNISHIP	First teller	9999	IFLMUD50HP0162	16/12/2008 12:59:53
SPARAGP	First Supervisor	9999	IFLMUD50HP0885	16/12/2008 10:56:25

**Field Description**

Column Name	Description
<b>User Id</b>	[Display] This column displays the user ID.
<b>User Name</b>	[Display] This column displays the name of the user, based on the user ID.
<b>Branch Code</b>	[Display] This column displays the branch code to which the logged in users belong to.
<b>Terminal Id</b>	[Display] This column displays the identification code of the terminal where each user has logged in to the system.
<b>Login Time</b>	[Display] This column displays the date and time on which the user had last logged in.

3. Click the **Close** button.

## 1.17. SMM02 - User Profile Maintenance

Using this option you can add user profiles centrally for a new user to be created in the system. In User Profile Maintenance, various attributes and roles of a user are defined.

Using the **Modify User Details** tab, you can maintain the Resetting of Primary Password, Primary Password Expiry Date change, Modification in Login Status and Enable/Disable User.

### Definition Prerequisites

- SMM18 - Access Domain Maintenance
- SMM14 - Template Securities Settings

### Modes Available

Add, Modify, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

### To add the user profile details

1. Type the fast path **SMM02** and click **Go** or navigate through the menus to **Global Definitions > Security > User Profile Maintenance**.
2. The system displays the **User Profile Maintenance** screen.

### User Profile Maintenance

**Field Description**

Field Name	Description
<b>User Id</b>	[Mandatory, Alphanumeric, 12] Type the identification code for the user.
<b>User Code</b>	[Display] This field displays the system-generated user code.
<b>Modify User Details OnLine (Branch database only)</b>	[Conditional, Check Box] Select the <b>Modify User Details OnLine (Branch database only)</b> check box to modify the user details. This field is enabled in the <b>Modify</b> mode. Selecting this check box enables the <b>Modify User Details</b> tab. This option is used if there is a centralized system administrator so that the administrator can change the following details for any user of any branch. <ul style="list-style-type: none"> <li>• Reset Primary Password</li> <li>• Change Primary Password Expiry Date</li> <li>• Modify Login Status</li> <li>• Enable/Disable User</li> </ul>

3. Click the **Add** button.
4. Type the user ID and press the **<Tab>** key.

## User Profile Maintenance

The screenshot shows the 'User Profile Maintenance' window with the 'User Details' tab selected. The window has a title bar 'User Profile Maintenance' and a toolbar with icons for Save, Undo, Redo, and Close. The main area contains various input fields for user information:

- User Id: 1, User Code: 2273
- Check box: Modify User Details Online (Branch database only)
- User Name, Employee ID, Language Code, Host Template, Primary Password, Password Chg Flg, Previous Password Count, Profile Start Date (22/12/2009), and Vacation Start Date (01/01/1800) are input fields.
- Cost Center, Access Domain Code, Password Reset Flag (Primary), Email Id, Profile End Date (31/12/2049), and Vacation End Date (01/01/1800) are input fields.
- Current Status and Permanently Disabled checkboxes.
- Record Details section with columns: Input By, Authorized By, Last Mnt. Date, Last Mnt. Action, and Authorized.
- Buttons at the bottom: Add (radio button selected), Modify, Delete, Cancel, Amend, Authorize, Inquiry, Ok, Close, and Clear.

5. Modify the required information in the various tab screens.

## User Details

The screenshot shows the 'User Profile Maintenance' window with the 'User Details' tab selected. The window has a title bar 'User Profile Maintenance' and a toolbar with icons for Save, Print, and Close. The main area contains the following fields:

- User Id: TDEV
- User Code: 2263
- Modify User Details Online (Branch database only):
- User Name: TDEV
- Employee ID: 5333
- Language Code: ENG
- Cost Center: PRABHADEVI
- Access Domain Code: 11
- Host Template: 10
- Primary Password:  (REDACTED)
- Password Reset Flag: Primary
- Password Chg Flg:
- Email Id: dev@gmail.com
- Previous Password Count: 0
- Profile Start Date: 08/12/2009
- Profile End Date: 31/12/2049
- Vacation Start Date: 01/01/2010
- Vacation End Date: 01/03/2010
- Current Status:
- Permanently Disabled:

At the bottom, there is a 'Record Details' section with fields for Input By, Authorized By, Last Mnt. Date, Last Mnt. Action, and Authorized. Below this is a toolbar with buttons for Add, Modify, Delete, Cancel, Amend, Authorize, Inquiry, Ok, Close, and Clear.

## Field Description

Field Name	Description
<b>User Name</b>	[Mandatory, Alphanumeric, 40] Type the name of the user. It should be unique for all branches. This field cannot be modified or amended.
<b>Employee ID</b>	[Mandatory, Alphanumeric, 40] Type the employee ID of the bank staff.
<b>Access Domain Code</b>	[Mandatory, Pick List] Select the appropriate access domain code from the pick list. The access domain codes are maintained in the <b>Access Domain Maintenance</b> (Fast Path: SMM18) option. Based on the access domain and access codes, the user will be able to inquire and maintain accounts that are having one of the access code included in the users access domain or else the inquiry/maintenance will not be allowed for that user on that CIF/Account.

Field Name	Description
<b>Language Code</b>	[Mandatory, Drop-Down] Select the code of the language from the drop-down list.
<b>Cost Center</b>	[Mandatory, Pick List] Select the branch code of the user from the pick list.
<b>Host Template</b>	[Mandatory, Pick List] Select the code of the host template from the pick list. If the field is blank, the value of the template is taken as zero and the user is attached only to the host template.
<b>Primary Password</b>	[Mandatory, Alphanumeric, 12] Type the primary password. Password policy of the bank can be set at the template level by <b>Template Security Settings</b> (Fast Path: SMM14). For e.g., It should be a combination of an uppercase and lowercase letter, and a numeric digit. This field cannot be modified or amended. The value can be between eight and 12.
<b>Password Reset Flag</b>	[Optional, Drop-Down] Select the password reset flag from the drop-down list. The options are: <ul style="list-style-type: none"> <li>• Primary</li> <li>• Secondary</li> <li>• Both</li> <li>• None</li> </ul> When the user logs in for the first time, a password change would be required if any option other than <b>None</b> is selected. This field cannot be modified or amended.
<b>Password Chg Flg</b>	[Display] This field is selected if the change in password is required during the first login.
<b>Email Id</b>	[Mandatory, Alphanumeric, 60] Type the e-mail address of the user.
<b>Previous Password Count</b>	[Mandatory, Numeric, One] Type the number of previous passwords that cannot be used again. This field cannot be modified or amended.
<b>Profile Start Date</b>	[Mandatory, Pick List, dd/mm/yyyy] Select the date from which the user's profile will be enabled from the pick list. This field cannot be modified or amended.

Field Name	Description
<b>Profile End Date</b>	<p>[Mandatory, Pick List, dd/mm/yyyy]  Select the date after which the user's profile will no longer be valid from the pick list.</p>
<b>Vacation Start Date</b>	<p>[Mandatory, Pick List, dd/mm/yyyy]  Select the vacation start date from the pick list.  The user cannot access the system during the specified vacation period. This ensures that any illegal attempt to access the system is not allowed. The system validates between the vacation start date and vacation end date (Excluding both the dates).  This date should be later than the profile start date.</p>
<b>Vacation End Date</b>	<p>[Mandatory, Pick List, dd/mm/yyyy]  Select the vacation end date from the pick list.  The user can access the system when he or she returns from the vacation. The system validates between the vacation start date and vacation end date (Excluding both the dates).  This date should be before the profile end date.</p>
<b>Current Status</b>	<p>[Mandatory, Drop-Down]  Select the current status of the user from the drop-down list.  The options are:</p> <ul style="list-style-type: none"> <li>• Disable</li> <li>• Enable</li> <li>• Lock</li> </ul>
<b>Permanently Disabled</b>	<p>[Display]  This field displays the status of the user.  The check box is selected if the user is permanently disabled.</p>

## Branch Template Details

This tab is for future use.

## User Template Details

User Profile Maintenance

User Id : TDEV User Code : 2240

Modify User Details Online (Branch database only)

User Details | Branch Template Details | **User Template Details** | Modify User Details

User Template : 12  
Password Lifetime : 99  
Template Access Code : 90  
Template Category : SM  
Template Level : 60  
Login Time (Half an Hour slots) :  Login Allowed  Login Not Allowed

Hour	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								
Holiday																								

Record Details

Input By	Authorized By	Last Mnt. Date	Last Mnt. Action	Authorized
----------	---------------	----------------	------------------	------------

Add  Modify  Delete  Cancel  Amend  Authorize  Inquiry  Ok  Close  Clear

## Field Description

Field Name	Description
<b>User Template</b>	[Display] This field displays the template code of the template linked to the user. Each code uniquely identifies a different template.
<b>Password Lifetime</b>	[Display] This field displays the password validity period for the user.
<b>Template Category</b>	[Display] This field displays the category of the template. The category identifies the role of the user, whether the user is the security manager, system operator or other user.

Field Name	Description
<b>Template Access Code</b>	<p>[Display]</p> <p>This field displays the access code of the template.</p> <p>It indicates the type of accounts in the bank that the users of a given template can access.</p>
<b>Template Level</b>	<p>[Display]</p> <p>This field displays the level of the template.</p> <p>It indicates the authority of the user. The higher the template level, the higher is the user's profile.</p>
<b>Login Time (Half an Hour slots)</b>	<p>[Display]</p> <p>This field displays the login time of the user.</p> <p>The user can log into the system only during specified slots during the week. The duration of each slot is half an hour.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• Login Allowed (Light Blue): Indicates that the user has access to the system during that time slot.</li> <li>• Login Not Allowed (White): Indicates that the user does not have access to the system during that time slot.</li> </ul>

6. Click the **Ok** button.
7. The system displays message "Record Added...Authorisation Pending...Click Ok to Continue". Click the **OK** button.
8. The user profile details are added once the record is authorized.

#### To modify the user profile details

1. Click the **Modify** button.
2. Select the user ID from the pick list.
3. To modify the user details online, select the **Modify User Details Online** check box.
4. The system displays the **Modify User Details** tab.

## Modify User Details

User Profile Maintenance

User Id : TDEVBROP User Code : 2559

Modify User Details OnLine (Branch database only)

User Details | Branch Template Details | User Template Details | **Modify User Details**

Reset Primary Password

Password:  Verify Password:

Change Primary Password Expiry: 10/01/2050

Modify Login Status

Current Status :  Permanently Disabled :

**Record Details**

Input By: SYSADM01	Authorized By: SYSADM02	Last Mnt. Date: 04/08/2007 19:25:39	Last Mnt. Action: Authorize	Authorized: <input checked="" type="checkbox"/>
--------------------	-------------------------	-------------------------------------	-----------------------------	---

Add  Modify  Delete  Cancel  Amend  Authorize  Inquiry

### Field Description

Field Name	Description
<b>Reset Primary Password</b>	[Optional, Check Box] Select the <b>Reset Primary Password</b> check box to reset the primary password.
<b>Password</b>	[Conditional, Alphanumeric, 12] Type the new password for the user. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz, etc. The value can be between eight and 12. This field is enabled only if the <b>Reset Primary Password</b> check box is selected.

Field Name	Description
<b>Verify Password</b>	[Conditional, Alphanumeric, 12] Type the new password to verify it. This field is enabled only if the <b>Reset Primary Password</b> check box is selected.
<b>Change Primary Password Expiry Date</b>	[Optional, Check Box] Select the <b>Change Primary Password Expiry Date</b> check box to change the user's primary password expiry date.  [Conditional, Pick List, dd/mm/yyyy] Select the date on which the primary password will expire from the pick list. This field is enabled only if the <b>Change Primary Password Expiry Date</b> check box is selected.
<b>Modify Login Status</b>	[Optional, Check Box] Select the <b>Modify Login Status</b> check box to modify the user login status.
<b>Current Status</b>	[Mandatory, Drop-Down] Select the current status of the user from the drop-down list. The options are: <ul style="list-style-type: none"><li>• Disable</li><li>• Enable</li><li>• Lock</li></ul>
<b>Permanently Disabled</b>	[Optional, Check Box] Select this check box to permanently disable a user id.

5. Click the **Ok** button.
6. The system displays message "Record Modified...Authorization Pending...Click Ok to Continue". Click the **OK** button.
7. The user profile details are modified once the record is authorised.

## 1.18. SMM03 - Task Profile Maintenance

Using this option you can maintain a task profile which includes the following details like Task ID, Task Description and Category.

All options are broken into tasks that can be individually assigned to the user. You can use a task only if you have access rights to it. A group of tasks in conjunction will display a menu with options that lead to screens. Depending on the tasks assigned , the menus are generated dynamically. Each task has a task profile associated with it.

### Definition Prerequisites

- BAM15 - Transaction Mnemonic Codes

### Modes Available

Add By Copy, Add, Modify, Delete, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

### To add the task profile details

1. Type the fast path **SMM03** and click **Go** or navigate through the menus to **Global Definitions > Security > Task Profile Maintenance**.
2. The system displays the **Task Profile Maintenance** screen.

### Task Profile Maintenance

The screenshot shows the 'Task Profile Maintenance' window. The window title is 'Task Profile Maintenance\*'. The main area contains the following fields:

- Task ID: [Text Box]
- Task Category: [Text Box]
- Module Code: [Text Box]
- Form Name: [Text Box]
- Task Description: [Text Box]
- Program Name: [Text Box]
- Task Level: [Text Box]
- HelpContext Id: [Text Box]
- Task Type: [Text Box]

Below these fields is a 'Record Details' section with the following fields:

- Input By
- Authorized By
- Last Mnt. Date
- Last Mnt. Action
- Authorized: [Check Box]

At the bottom of the window are several buttons:

- Add By Copy
- Add
- Modify
- Delete
- Cancel
- Amend
- Authorize
- Inquiry
- UDF
- Ok
- Close
- Clear

**Field Description**

Field Name	Description
<b>Task ID</b>	<p>[Mandatory, Alphanumeric, Five]</p> <p>Type the appropriate task code.</p> <p>The task codes are assigned to the tasks or type of transactions that the user can access. Task code is a unique ID assigned to maintenance to provide easy access to the users.</p> <p>Once added, this field cannot be modified.</p>
<b>Task Category</b>	<p>[Mandatory, Drop-Down]</p> <p>Select the task category from the drop-down list.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• OP (Operator) - The System Operators are the other users of <b>FLEXCUBE</b> Retail application. The responsibility of system operators includes: End of Day Processing, File Transfer, Archival/Retrieval. The System Operators cannot perform any application related activities.</li> <li>• OT (Other Tellers) - The Other Tellers are the on-line users. They have the maximum interaction with <b>FLEXCUBE Retail</b> application. The responsibility of other tellers includes: Tables Maintenance, Performing Host transactions. This category of users cannot perform any System Administrator / System Operator kind of activities. These users perform all the application related activities.</li> <li>• SM (Security Manager) - The security manager has management level access rights. The responsibility of Security Manager includes: User Profile Maintenance, Template Profile Maintenance, Class Profile Maintenance, User Class Linkage, Task Access Control, System Security (involving Audit trail tracking and Exception activities tracking). The Security Manager cannot perform any application related activities.</li> </ul> <p>It indicates that the user with specific access rights can perform the assigned task.</p>
<b>Module Code</b>	<p>[Mandatory, Drop-Down]</p> <p>Select the code of the module to which the task ID belongs from the drop-down list.</p> <p>The user can maintain a sequence format that will be applicable to all the modules available in the bank.</p>
<b>Form Name</b>	<p>[Optional, Alphanumeric, 30]</p> <p>Type the DLL name of the related function.</p> <p>This field is currently not in use.</p>
<b>Task Description</b>	<p>[Mandatory, Alphanumeric, 40]</p> <p>Type the description for the task that the user wants to add.</p>

Field Name	Description
<b>Program Name</b>	[Optional, Alphanumeric, 64]  Type the name of the program, which is linked to the parent task. The name of the program cannot begin with underscore.  This field has to be blank if the process code is blank.
<b>Task Level</b>	[Mandatory, Numeric, Four]  Type the level of the task.  All templates with a level greater than the specified level can be granted access to this task.
<b>HelpContext Id</b>	[Optional, Numeric, Nine]  Type the help context identification number of the task.
<b>Task Type</b>	[Optional, Drop-Down]  Select the task type from the drop-down list.  The options are: <ul style="list-style-type: none"> <li>• Cash Task</li> <li>• Non-Cash Task</li> </ul>

3. Click the **Add** button.
4. Enter the task id and select the task category from the drop-down list.
5. Select the module code from the drop-down list.
6. Enter the form name, task description, program name, and help context id.

## Task Profiles Maintenance

The screenshot shows the 'Task Profile Maintenance' window. The 'Record Details' section at the bottom is expanded, showing fields for 'Input By', 'Authorized By', 'Last Mnt. Date', 'Last Mnt. Action', and 'Authorized'. Below these fields are buttons for 'Add By Copy', 'Add', 'Modify', 'Delete', 'Cancel', 'Amend', 'Authorize', and 'Inquiry'. At the bottom right are buttons for 'UDF', 'Ok', 'Close', and 'Clear'. The main area of the window displays a list of task profiles, with the last entry being the one currently being added.

Task ID	Module Code	Form Name	Task Description	Program Name	Task Level	HelpContext Id	Task Type
01	CH	Cash Deposit	011	CasaAcctCashDeposit	1	1401	Cash Task

7. Click the **Ok** button.
8. The system displays message "Record Added...Authorisation Pending...Click Ok to Continue". Click the **OK** button.
9. The task profile is added once the record is authorized.

## 1.19. SMM09 - User Prohibited Password Maintenance

Security Management System can maintain two lists of passwords that each user should not use. One list is common to all users in the branch, and the other is unique to each user.

Using this option you can maintain a list of prohibited passwords for each user individually. These passwords are generally names, words, and numbers that can be easily associated with the user. For example, name of the user's spouse, car number, telephone number, date of birth, etc. When a new user is added to the system, a new list of user prohibited passwords can be added.

### Definition Prerequisites

- User Ids to be available for this maintenance

### Modes Available

Add, Delete, Cancel, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

### To add user prohibited passwords

1. Type the fast path **SMM09** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Others > User Prohibited Password Maintenance**.
2. The system displays the **User Prohibited Password Maintenance** screen.

### User Prohibited Password Maintenance

The screenshot shows the 'User Prohibited Password Maintenance' window. At the top, there are three input fields: 'User ID' (with a dropdown arrow and a '...' button), 'User Name' (with a dropdown arrow), and 'Prohibited Passwords' (a text input field). At the bottom, there is a 'Record Details' section with five input fields: 'Input By', 'Authorized By', 'Last Mnt. Date', 'Last Mnt. Action', and 'Authorized' (with a checkbox). Below these fields are buttons for 'Add', 'Modify', 'Delete', 'Cancel', 'Amend', 'Authorize', 'Inquiry', 'Ok', 'Close', and 'Clear'.

**Field Description**

Field Name	Description
<b>User ID</b>	[Mandatory, Drop-Down] Select the ID of the user, to add a list of prohibited passwords, from the drop-down list.
<b>User Name</b>	[Display] This field displays the user name of the Id selected in the corresponding field.
<b>Prohibited Passwords</b>	[Mandatory, Alphanumeric, 12] Type the password that is prohibited for this user ID.

3. Click the **Add** button.
4. Select the user Id from the drop-down list.
5. Enter the password that is prohibited for this user.

**User Prohibited Password Maintenance**

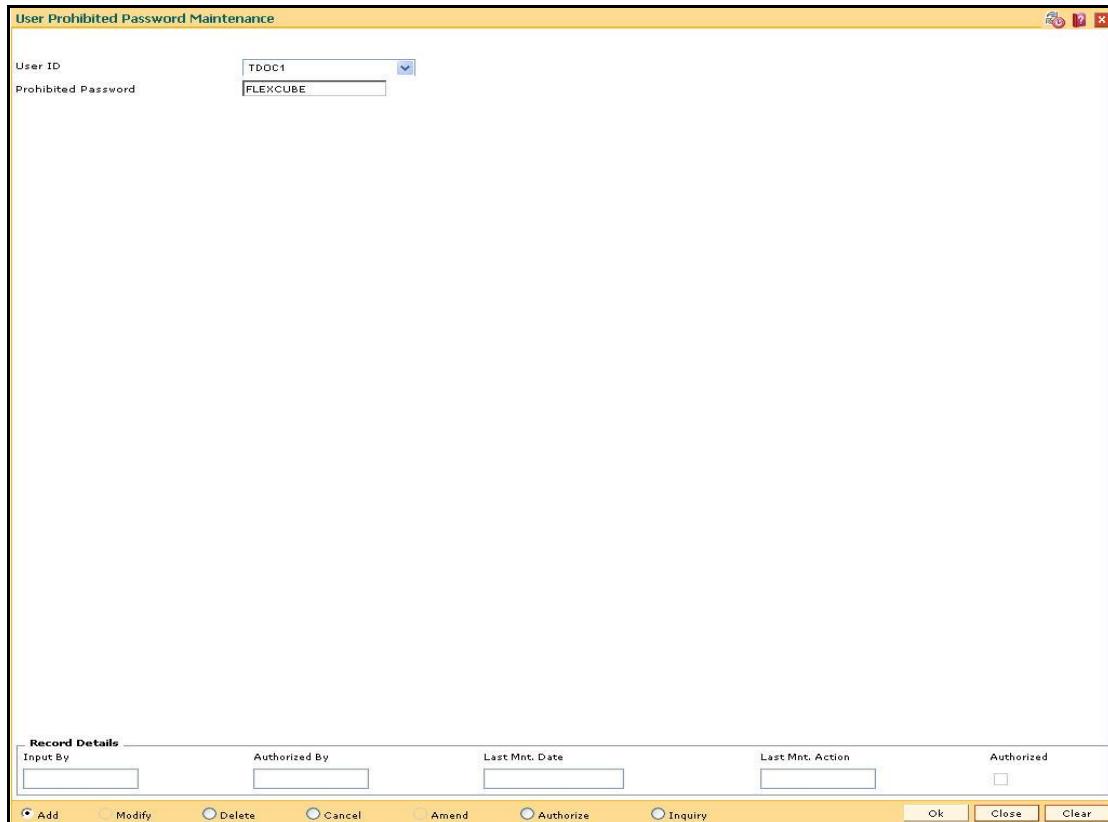
The screenshot shows a Windows application window titled "User Prohibited Password Maintenance". Inside the window, there are two text input fields: "User ID" containing "TDOC1" and "Prohibited Password" containing "FLEXCUBE". Below these fields is a section titled "Record Details" with five empty input fields for "Input By", "Authorized By", "Last Mnt. Date", "Last Mnt. Action", and "Authorized". At the bottom of the window is a toolbar with several buttons: "Add" (radio button selected), "Modify", "Delete", "Cancel", "Amend", "Authorize", "Inquiry", "Ok", "Close", and "Clear".

6. Click the **Ok** button.
7. The system displays the message "Record Added ...Authorisation Pending. Click Ok to Continue". Click the **OK** button.
8. The prohibited password gets added once the record is authorised.

### To view the user prohibited passwords

1. Click the **Inquiry** button.
2. Select the user id from the drop-down list.
3. The system displays the list of prohibited passwords for the selected user.

### User Prohibited Password Maintenance



User ID	TDOC1
Prohibited Password	FLEXCUBE

**Record Details**

Input By	Authorized By	Last Mnt. Date	Last Mnt. Action	Authorized
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Buttons at the bottom:

- Add
- Modify
- Delete
- Cancel
- Amend
- Authorize
- Inquiry
- Ok
- Close
- Clear

4. Click the **Close** button.

## 1.20. SMM12 - User Class Cross Reference Maintenance

Classes are created for grouping users for authorisation purposes. Any action performed by the maker of a particular class, will have to be authorised by the authoriser of the same class. A user can be linked to more than one class.

Users in the branch are given access to various classes maintained in the **Class Profile Maintenance** (Fast Path: SMM04) option. Using this option allows the system administrator to enable users to belong to various pre-defined classes.

### Definition Prerequisite

- SMM02 - User Profile Maintenance
- SMM04 - Class Profile Maintenance

### Modes Available

Add, Delete, Inquire. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

#### To add a user class cross reference

1. Type the fast path **SMM12** and click **Go** or navigate through the menus to **Global Definitions > Security > User Class Cross Reference Maintenance**.
2. The system displays the **User Class Cross Reference Maintenance** screen.

### User Class Cross Reference Maintenance

**Field Description**

Field Name	Description
<b>User Id</b>	[Mandatory, Drop-Down]  Select the user ID from the drop-down list.  These user ID's are maintained in the <b>User Profile Maintenance</b> (Fast Path: SMM02) option.
<b>User Name</b>	[Display]  This field displays the user name based on the selected user ID.
<b>Branch Name</b>	[Display]  This field displays the branch name to which the selected user ID belongs.
<b>Class Code</b>	[Mandatory, Pick List]  Select the class code, for linking the class to a user ID, from the pick list.  A valid user should have a class code associated to the user ID. The user can link a user to more than one class.
<b>Delete All Records</b>	[Conditional, Check Box]  Select the <b>Delete All Records</b> check box to delete the records associated with the user ID.  This field is enabled if the user selects the <b>Delete</b> mode.  This field is non-editable in the <b>Add</b> mode.

Column Name	Description
<b>Code Class</b>	[Display]  This column displays the class code.
<b>Description</b>	[Display]  This column displays the description of the class code.

3. Click the **Add** button.
4. Select the user ID from the drop-down list and select the class code from the pick list.

**User Class Cross Reference Maintenance**

Code	Class	Description
SYS	SYS	SYS

5. Click the **+** button.
6. The system displays the message "Class code appended to the List". Click the **OK** button.
7. The system refreshes the **User Class Cross Reference Maintenance** screen with the updated fields. Click the **Ok** button.
8. The system displays the "Authorization Required. Do You Want to continue?". Click the **OK** button.
9. The system displays the **Authorization Reason** screen.
10. Enter the relevant information and click the **Grant** button.
11. The system displays the message "Record Added". Click the **OK** button.
12. The user cross reference is added successfully.

## 1.21. SMM13 - Template Transaction Limits

Using this option limits on financial transactions can be maintained in the system for all users of the system. The limits can be maintained for a group of users under a particular template and currency combination. The online and offline limits for same branch and for inter branch are maintained in this option. You can also populate the limits that are assigned to the transaction group to the individual transaction mnemonics.

### Definition Prerequisites

- BAM25 - Currency Definition
- BAM15 - Transaction Mnemonic Codes

### Modes Available

Add, Modify, Delete, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to Standard Maintenance Procedures.

### To add template limits

1. Type the fast path **SMM13** and click **Go** or navigate through the menus to **Global Definitions > Security > Template Transaction Limits**.
2. The system displays the **Template Transaction Limits** screen.

### Template Transaction Limits

**Field Description**

Field Name	Description
<b>All Branches</b>	[Optional, Check Box] Select the <b>All Branches</b> check box to link the template to all the branches of the bank.
<b>Branch Code</b>	[Mandatory, Pick List] Select the branch code, for which the template is to be defined, from the pick list. By default, it displays the branch code as zero if the <b>All Branches</b> check box is selected.
<b>Branch Name</b>	[Display] This field displays the name of branch.
<b>Template Code</b>	[Mandatory, Pick List] Select the template code, for which the limit is to be defined, from the pick list.
<b>Currency Code</b>	[Mandatory, Drop-Down] Select the currency for the template. from the drop-down list The system fetches the data from bank currency maintenance. The drop-down lists all the currencies that are defined in the <b>Currency Definition</b> (Fast Path: BAM25) option.
<b>Lower Retention Limit</b>	[Mandatory, Numeric, 10, Two] Type the appropriate lower retention limit for a teller. This is the minimum amount that a teller can retain with himself at the end of the day.
<b>Upper Retention Limit</b>	[Mandatory, Numeric, 10, Two] Type the upper retention limit for a teller. This is the maximum amount that a teller can retain with himself at the end of the day.
<b>Exchange Rate Variance Limit</b>	[Mandatory, Numeric, 10, Two] Type the variance in percentage over base exchange rates that the users linked to this template are allowed to permit.
<b>SC Waiver Limit for Loans in LCY</b>	[Mandatory, Numeric, 10] Type the SC waiver limit for the loan account.

3. Click the **Add** button.
4. Select the **All Branches** check box to link the template to all the branches of the bank.
5. Enter the required information in the various fields.

## Template Transaction Limits

6. Enter the required information in the various tab screens.

## Transaction Groups

The screenshot shows the 'Template Transaction Limits' application window. At the top, there are fields for 'Branch Code' (0), 'Template Code' (12), 'Branch Name' (All Branches), and 'Currency Code' (USD). Below these are fields for 'Lower Retention Limit' (0.0), 'Upper Retention Limit' (0.0), 'Exchange Rate Variance Limit' (0.0), and 'SC Waiver Limit for Loans in LOY' (0.0). The main area displays a table of transaction groups:

Group Name	Same Branch Online Limit	Same Branch Offline Limit	Interbranch Online Limit	Interbranch Offline Limit
CASH_CR	0.00	0.00	0.00	0.00
CASH_DR	0.00	0.00	0.00	0.00
CLG	0.00	0.00	0.00	0.00
INT_CASH_CR	0.00	0.00	0.00	0.00
INT_CASH_DR	0.00	0.00	0.00	0.00
XFER	0.00	0.00	0.00	0.00

At the bottom, there are buttons for 'Show Transactions' and 'Populate Transaction Limits'. The 'Record Details' section shows 'Input By' (SYSADM22), 'Authorized By' (SMSSUPER), 'Last Mnt. Date' (30/04/2008 11:19:46), and 'Last Mnt. Action' (empty). The 'Authorized' checkbox is unchecked. Below this are buttons for 'Add', 'Modify', 'Delete', 'Cancel', 'Amend', 'Authorize', 'Inquiry', and 'Clear'.

## Field Description

Column Name	Description
<b>Group Name</b>	<p>[Display]</p> <p>This column displays the transactions group name.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• CASH_CR: This group lists all the cash debit transaction mnemonics</li> <li>• CASH_DR: This group lists all the cash credit transaction mnemonics</li> <li>• CLG: This group lists all the clearing related transaction mnemonics</li> <li>• INT_CASH_CR: This group lists all the interest cash credit transaction mnemonics</li> <li>• INT_CASH_DR: This group lists all the interest cash debit transaction mnemonics</li> <li>• XFER: This group lists all the transfer related transaction mnemonics</li> </ul>

Column Name	Description
<b>Same Branch Online Limit</b>	[Mandatory, Numeric, 10, Two] Type the online transaction limit for the same branch for the corresponding group.
<b>Same Branch Offline Limit</b>	[Mandatory, Numeric, 10, Two] Type the offline transaction limit for the same branch for the corresponding group.
<b>Interbranch Online Limit</b>	[Mandatory, Numeric, 10, Two] Type the online interbranch transaction limit for the corresponding group.
<b>Interbranch Offline Limit</b>	[Mandatory, Numeric, 10, Two] Type the offline interbranch transaction limit for the corresponding group.
<b>Show Transactions</b>	[Command Button] Click the button to view the transactions listed in the selected transaction group. This is only for information purposes.
<b>Populate Transaction Limits</b>	[Command Button] Click the button to populate the limits that are assigned to the transaction group to the individual transaction mnemonics. The system displays the <b>Template Transaction Limits</b> screen. The user cannot change the limit assigned to a group once he clicks the <b>Populate Transaction Limits</b> button.

## Template Transaction Limits

Template Transaction Limits

All Branches	<input checked="" type="checkbox"/>	Branch Code:	<input type="text" value="0"/>	Branch Name:	<input type="text" value="All Branches"/>
Template Code:	<input type="text" value="12"/>	Currency Code :	<input type="text" value="USD"/>		
Lower Retention Limit:	<input type="text" value="0.0"/>	Upper Retention Limit:	<input type="text" value="0.0"/>		
Exchange Rate Variance Limit:	<input type="text" value="0.0"/>	SC Waiver Limit for Loans in LCY:	<input type="text" value="0.0"/>		
<a href="#">Transaction Groups</a> <a href="#">Template Transaction Limits</a>					
Transaction Mnemonic	Mnemonic Description	Same Branch Online Limit	Same Branch Offline Limit	Interbranch Online Limit	Interbranch Offline Limit
1001	Cash Withdrawal	0.00	0.00	0.00	0.00
1002	Excess Refund By Cash	0.00	0.00	0.00	0.00
1003	Disbursement By Cash	0.00	0.00	0.00	0.00
1004	Cash Withdrawal From Ext.A/C	0.00	0.00	0.00	0.00
1005	Miscellaneous GL Xfer.	0.00	0.00	0.00	0.00
1006	Funds Transfer Debit	0.00	0.00	0.00	0.00
1007	TD. Payin Casa Xfer.	0.00	0.00	0.00	0.00
1008	Miscellaneous Customer Debit	0.00	0.00	0.00	0.00
1011	Disbursement By Cheque	0.00	0.00	0.00	0.00
1012	LN. Rev. Credit Withdrawal	0.00	0.00	0.00	0.00
1013	CASA. Cheque Withdrawal	0.00	0.00	0.00	0.00
1014	DD. Sale Against Account	0.00	0.00	0.00	0.00
1017	Revolving Loan Debit By Cash	0.00	0.00	0.00	0.00
1019	Revolving Loan Debit By Cheque	0.00	0.00	0.00	0.00
1021	TD. Payin By GL	0.00	0.00	0.00	0.00
1022	Cheque Withdrawal	0.00	0.00	0.00	0.00
1023	FC Account to KBI Account Transfer	0.00	0.00	0.00	0.00
1024	KBI Account to FC Account Transfer	0.00	0.00	0.00	0.00
1025	Bill Payment By Cash	0.00	0.00	0.00	0.00
1026	Advance Payment against Credit Card	0.00	0.00	0.00	0.00
1060	GL. Miscellaneous Debit	0.00	0.00	0.00	0.00
1064	Loan Interest Subsidy Pay-In through CASA	0.00	0.00	0.00	0.00
1065	Installment Payment By Xfer.	0.00	0.00	0.00	0.00
1066	Partial Payoff By Xfer. From CASA	0.00	0.00	0.00	0.00
1067	EPS. By Xfer. From CASA	0.00	0.00	0.00	0.00
1068	LN. Advance Payment	0.00	0.00	0.00	0.00
1069	LN. Rescission By Xfer. From CASA	0.00	0.00	0.00	0.00
1072	Rev LN Installment Payment By Xfer.	0.00	0.00	0.00	0.00
1075	Bill Payment (Against Account)	0.00	0.00	0.00	0.00

Record Details

Input By	Authorized By	Last Mnt. Date	Last Mnt. Action	Authorized
SYSADM22	GMSSUPER	30/04/2008 11:19:46		<input type="checkbox"/>

Add  Modify  Delete  Cancel  Amend  Authorize  Inquiry

### Field Description

Column Name	Description
<b>Transaction Mnemonic</b>	[Display] This column displays the mnemonics of the transactions listed in the transaction group.
<b>Mnemonic Description</b>	[Display] This column displays the description of the transaction mnemonic.
<b>Same Branch Online Limit</b>	[Mandatory, Numeric, 10, Two] Type the online transaction limit for the same branch for the corresponding mnemonic.  By default, the system displays the limit specified for the transaction group.

Column Name	Description
<b>Same Branch Offline Limit</b>	[Mandatory, Numeric, 10, Two] Type the offline transaction limit for the same branch for the corresponding mnemonic. By default, the system displays the limit specified for the transaction group.
<b>Interbranch Online Limit</b>	[Mandatory, Numeric, 10, Two] Type the online interbranch transaction limit for the corresponding mnemonic. By default, the system displays the limit specified for the transaction group.
<b>Interbranch Offline Limit</b>	[Mandatory, Numeric, 10, Two] Type the offline interbranch transaction limit for the corresponding mnemonic. By default, the system displays the limit specified for the transaction group.

7. Click the **Ok** button.
8. The system displays the message "Record Added...Authorization Pending". Click the **Ok** button.
9. The template transaction limits are added once the record is authorised.



**Security Management System User Manual**

**May 2011**

**Version : 4.3.1.0.0**

**Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.**

**Worldwide Inquiries:**

**Phone: +1.650.506.7000  
Fax: +1.650.506.7200**

**[www.oracle.com/financial\\_services/](http://www.oracle.com/financial_services/)**

**Copyright © 2011 Oracle and/or its affiliates. All rights reserved.**

**No part of this work may be reproduced, stored in a retrieval system, adopted or transmitted in any form or by any means, electronic, mechanical, photographic, graphic, optic recording or otherwise, translated in any language or computer language, without the prior written permission of Oracle Financial Services Software Limited.**

**Due care has been taken to make this document and accompanying software package as accurate as possible. However, Oracle Financial Services Software Limited makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this document and the accompanying Software System. Furthermore, Oracle Financial Services Software Limited reserves the right to alter, modify or otherwise change in any manner the content hereof, without obligation of Oracle Financial Services Software Limited to notify any person of such revision or changes.**

**All company and product names are trademarks of the respective companies with which they are associated.**