

# **Oracle FLEXCUBE Core Banking**

Security Management Reports Manual  
Release 11.5.0.0.0

**Part No. E52876-01**

July 2014

**ORACLE®**

Security Management Reports Reports Manual  
July 2014

Oracle Financial Services Software Limited  
Oracle Park  
Off Western Express Highway  
Goregaon (East)  
Mumbai, Maharashtra 400 063  
India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

[www.oracle.com/financialservices/](http://www.oracle.com/financialservices/)

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

## Table of Contents

<b>1. Preface</b> .....	<b>4</b>
<b>2. Security Management Reports</b> .....	<b>6</b>
2.1. Adhoc Reports.....	7
2.1.1. SMS Daily Reports.....	8
SM103 - User Access Rights Report.....	9
SM120 - SMS Event Logs .....	12
SM125 - Users Created / Deleted .....	16
SM104 - User Inactivity Report.....	20
SM112 - List Of Disabled Users .....	24
2.2. Batch Reports.....	26
2.2.1. SMS DAILY REPORTS .....	31
SM117 - User Profile Maintained Today .....	32
SM120 – SMS Event Logs .....	36
SM105 - Password Expiry Report .....	40
SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT.....	44

## 1. Preface

### 1.1. Intended Audience

This document is intended for the following audience:

- Customers
- Partners

### 1.2. Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### 1.3. Access to OFSS Support

<https://support.us.oracle.com>

### 1.4. Structure

This manual is organized into the following categories:

**Preface** gives information on the intended audience. It also describes the overall structure of the Reports Manual

**Introduction** provides brief information on the overall functionality covered in the Reports Manual

**Chapters** are dedicated to individual reports and its details, covered in the Reports Manual

## 1.5. Related Information Sources

For more information on Oracle FLEXCUBE Core Banking Release 11.5.0.0.0, refer to the following documents:

- Oracle FLEXCUBE Core Banking Licensing Guide

## 2. Security Management Reports

A report is a document that is illustrated with the help of information, and tailored to a given situation and audience. The primary purpose of a report is to provide information. However, reports may also include additional information, such as suggestions or conclusions that indicate possible future actions which the report reader might take. Reports can be public or private.

Advice is generally a written proof of a service performed, funds transferred, or a payment that is received or made. It can also be a recommendation that advises a customer about specific investment asset allocations based on age and circumstances.

**Oracle Flexcube** supports report generation in PDF, HTML and Excel formats. Based on the system configuration the reports can be generated in any of the above mentioned format.

**Note 1:** Reports can be generated by using the **Report Request** (Fast Path: 7775) option. Reports can be viewed/printed using the **Advice/Report Status Inquiry** (Fast Path: 7778) option. The above screens can be accessed by navigating through the following path: **Transaction Processing > Internal Transactions > Reports**.

**Note 2:** Report Codes precede the Report Names. Unlike the User Manual where the Fast Path preceding the Topic Title indicates the access for the screen, the Report Code is simply a unique code for the report.

### Reports are categorized under:

- Adhoc Reports
- Batch Report

## 2.1. Adhoc Reports

Adhoc reports are generated on demand or on request. Reports and advices can be requested from the Report Request screen. Adhoc reports can be viewed and generated using the teller login or the system operator login.

### List of Adhoc Reports:

- SMS DAILY REPORTS

### 2.1.1. SMS Daily Reports

The SMS Daily Reports includes reports specific to the user profiles that are maintained daily.

#### List of Customer Information Reports:

- SM103 - User Access Rights Report
- SM106 - User List
- SM120 - SMS Event Logs
- SM125 - Users Created / Deleted
- SM104-User Inactivity Report
- SM112 - List Of Disabled Users



**SM103 - User Access Rights Report**

Access rights are provided to various **FLEXCUBE** users depending on the business requirement and control mechanism. Branch users carry out various activities which depend on the user level, rights and category assigned to them.

This report is a list of user access rights for the given range of User IDs. Each column in this report provides information about the Task ID, Task Description, Parent Code, Parent Description, Category, User ID, User Level, Name, and Branch Details are grouped User ID wise.

**To generate the User Access Rights Report**

1. Access the **Report Request** (Fast Path: 7775) screen.
2. Ensure that the **Adhoc Reports** button is selected.
3. Navigate through **Security Management > SMS Daily Reports > SM103 - User Access Rights Report**.
4. The system displays the **SM103 - User Access Rights Report** screen.

**Field Description**

Field Name	Description
<b>From User ID</b>	[Mandatory, Alphanumeric, Nine] Type the valid From User Id which the report needs to be generated. This Id should not be greater than the To User Id.

Field Name	Description
<b>To User ID</b>	[Mandatory, Alphanumeric, Nine] Type the valid To User Id till which the report needs to be generated.
<b>Waived Service Charge</b>	[Optional, Check Box] Select the check box to waive the service charge.

5. Enter the appropriate parameters in the **SM103 - User Access Rights Report** screen.
6. Click the **Generate** button.
7. The system displays the message "Report Request Submitted". Click the **OK** button.
8. The system generates the **User Access Rights Listing Report**. For reference, a specimen of the report generated is given below:

# SM103 - User Access Rights Report

Bank :	335	DEMO BANK	FLEXCUBE	Run Date :	21/12/2009
Branch :	9999	DEMO	USER ACCESS RIGHTS LISTING	Run Time :	6:17 PM
Op. Id :	SYSADM01		For: 31-Dec-2007	Report No :	SM103/ 1
<hr/>					
Task Id	Task Description			Parent Code	Parent Description
<hr/>					
Branch :	9999	User Id.:	SYSADM01	Category:	SM
		Name :	First System Administrator	Level :	50
<hr/>					
7011	Event Log Inquiry			IT005	Inquiries
752	Reset primary password			IT016	Security
767	Reset secondary password			IT016	Security
768	Change primary password			IT016	Security
769	Change secondary password			IT016	Security
7775	Report Request			IT014	Reports
7778	Advice/Report Status Enquiry			IT014	Reports
7781	Advice/Report Cancel Request All Tellers			IT014	Reports
GD011	Security			GD000	Global Definitions
IT014	Reports			TPM08	Internal Transactions
IT016	Security			TPM08	Internal Transactions
SM11A	Currently logged in User list			GD011	Security
SMM16	Reports Access Maintenance			GD011	Security
SMM17	Access Codes Maintenance			GD011	Security
SMM18	Access Domain Maintenance			GD011	Security
SMM19	Transaction Group Code Maintenance			GD011	Security
SMM21	Template Transaction Field Xref			GD011	Security
TPM08	Internal Transactions			TP000	Transaction Processing
<hr/>					
*** End of Report ***					

**SM120 - SMS Event Logs**

Bank required to have very strict control and vigilance in terms of access to the system. It is imperative for a bank to ensure that access to various modules/ transactions in is well controlled. To facilitate this control an Audit trail can be maintained for any task / transaction accessed by the user along with the terminal/machine where it has been performed. A log is then recorded and can be accessed by the bank at any future date.

Each column of the report provides information on User Id, Event Date and Time, Machine Name, Task Code, Task Description, and Action. Details are grouped branch wise.

**To generate the SMS Event Logs Report**

- 1. Access the **Report Request** (Fast Path: 7775) screen.
- 2. Ensure that the **Adhoc Reports** button is selected.
- 3. Navigate through **Security Management > SMS DAILY REPORTS > SM120 - SMS Event Logs**.
- 4. The system displays the **SM120 - SMS Event Logs** screen.

SM120 - SMS Event Logs

**Input Parameters**

From User Id

To User Id

Waived Service Charge:

Generate

**Field Description**

<b>Field Name</b>	<b>Description</b>
<b>From User ID</b>	[Mandatory, Alphanumeric, Nine] Type the valid From User Id which the report needs to be generated. This Id should not be greater than the To User Id.
<b>To User ID</b>	[Mandatory, Alphanumeric, Nine] Type the valid To User Id till which the report needs to be generated.
<b>Waived Service Charge</b>	[Optional, Check Box] Select the check box to waive the service charge.

5. Enter the appropriate parameters in the **SM120 - SMS Event Logs** screen.
6. Click the **Generate** button.
7. The system displays the message "Report Request Submitted".
8. Click the **OK** button.
9. The system generates the **SMS Event Logs Report**.

**To view and print the SMS Event Logs Report**

1. Access the **Advice/Report Status Enquiry** (Fast Path: 7778) screen.
2. Select the check box corresponding to **SM120 - SMS Event Logs**.
3. Click the **View** button to view the report.
4. The system displays the **SMS Event Logs Report** screen.

Bank :	9199 DEMO	FLEXCUBE	Run Time :	08:44PM2009	
Op. Id :	SYSOPER	AUDIT TRAIL REPORT	Report No:	SM120/1	
		For: 31-Dec-2007			
User Id	Event Date and Time	Machine Name	Task Code	Task Description	Action
Branch :					
*** No data for this Report ***					

5. On the **File** menu, click **Print**.
6. The system displays the **Print** dialog box.
7. Select the appropriate parameters and click the **OK** button.

**SM125 - Users Created / Deleted**

Users are created in the system to perform various financial and non financial activities. According to the business requirement and control mechanism, user profiles are assigned to the tellers. Branches also delete users from the system in case of retirement, etc. This report is a list of users created/deleted by maker, and authorised by checker.

This is a list of users created or deleted for the given period. Each column of the report provides information about User Number, User ID, User Name, Action, Action Date, Maker ID and Checker ID.

**To generate the Users Created / Deleted Report**

1. Access the **Report Request** (Fast Path: 7775) screen.
2. Ensure that the **Adhoc Reports** button is selected.
3. Navigate through **Security Management > SMS DAILY REPORTS > SM125 - Users Created / Deleted**.
4. The system displays the **SM125 - Users Created / Deleted** screen.

**Field Description**

Field Name	Description
<b>From Date[DD/MM/YYYY]</b>	[Mandatory, dd/mm/yyyy] Type the valid start date for the report. This date should not be greater than To Date.



Field Name	Description
<b>To Date[DD/MM/YYYY]</b>	[Mandatory, dd/mm/yyyy] Type the valid end date for the report.
<b>Waived Service Charge</b>	[Optional, Check Box] Select the check box to waive the service charge.

5. Enter the appropriate parameters in the **SM125 - Users Created / Deleted** screen.
6. Click the **Generate** button.
7. The system displays the message "Report Request Submitted".
8. Click the **OK** button.
9. The system generates the **Users Created / Deleted Report**.

#### To view and print the Users Created / Deleted Report

1. Access the **Advice/Report Status Enquiry** (Fast Path: 7778) screen.
2. Select the check box corresponding to **SM125 - Users Created / Deleted**.
3. Click the **View** button to view the report.
4. The system displays the **Users Created / Deleted Report** screen.

SM125 - Users Created / Deleted

User No	User ID	User Name	Action	Action Date	Maker ID	Checker ID
2121	SUDAY	First Supervisor	Added	10-03-200	SYSADM01	SYSADM02
6005	SYSNEHA	sys adm neha	Added	12-03-200	SYSADM01	SYSADM02
6007	TPROFILE	Profile Date	Added	16-03-200	SYSADM01	SYSADM02
2120	TUDAY	First Teller	Added	10-03-200	SYSADM01	SYSADM02

\*\*\* End of Report \*\*\*

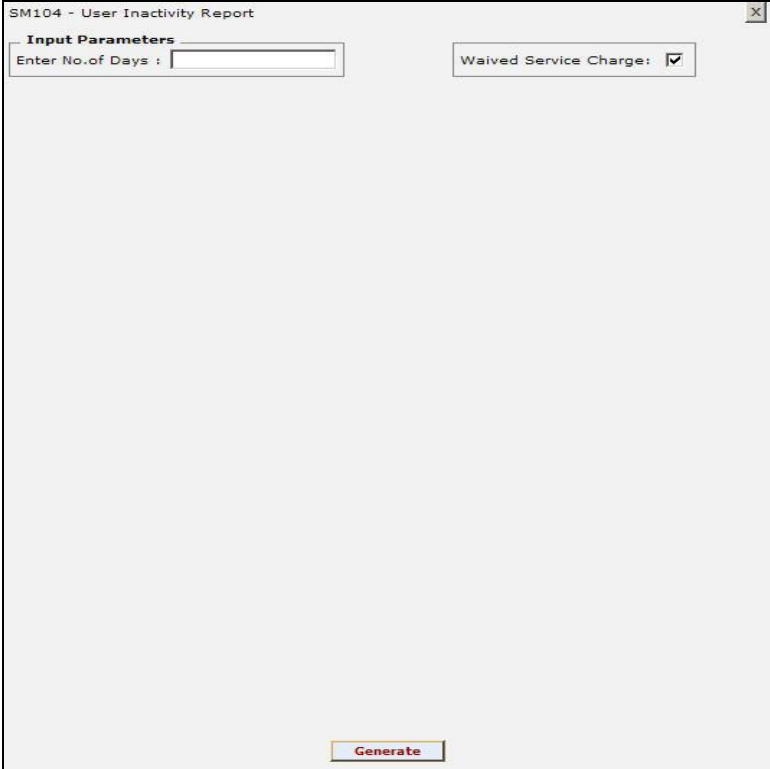
5. On the **File** menu, click **Print**.
6. The system displays the **Print** dialog box.
7. Select the appropriate parameters and click the **OK** button.

**SM104 - User Inactivity Report**

This report is a list of users who are inactive for a period of time. Each column in this report provides information about the Branch, User ID, User Name, Last Sign On and Remarks.

**To generate the User Inactivity Report**

- 1. Access the **Report Request** (Fast Path: 7775) screen.
- 2. Ensure that the **Adhoc Reports** button is selected.
- 3. Navigate through **Security Management > SMS Daily Reports > SM104 - User Inactivity Report**.
- 4. The system displays the **SM104 - User Inactivity Report** screen.



**Field Description**

Field Name	Description
Enter No. of Days	[Optional, Numeric, Nine] Type the number of days to generate the user inactivity report.
Waived Service Charge	[Optional, Check Box] Select the check box to waive the service charge.

5. Enter the appropriate parameters in the **SM104 - User Inactivity Report** screen.
6. Click the **Generate** button.
7. The system displays the message "Report Request Submitted". Click the **OK** button.
8. Click the **OK** button.
9. The system generates the **SMS Event Logs Report**.

### To view and print the User Inactivity Report

1. Access the **Advice/Report Status Enquiry** (Fast Path: 7778) screen.
2. Select the check box corresponding to **SM104 - User Inactivity Report**.
3. Click the **View** button to view the report.

The system displays the **User Inactivity Report** screen.

# SM104 - User Inactivity Report

Branch	User Id	User Name	Last sign-on	Remarks
560	SYSSMS02	Second System Administrator	04-09-2008	
560	SYSSTL	First System Administrator	12-09-2008	
560	SYSSUPER	First Supervisor	06-06-2008	
240	SYSTD	First System Administrator	05-09-2008	
560	SYSTELLER	First teller	25-07-2008	
560	SYSTEM	SYSTEM	25-07-2008	Profile Expired
560	SYSVTELLER	Vault teller	13-12-2007	
240	SYSVTELLER1	SUPER	13-12-2007	
240	TABHIJIT	TABHIJIT	31-12-1799	Primary Password Expired
240	TBHUPEN	TBHUPEN	31-12-1799	Primary Password Expired
560	TBS_USER	TBS USER	07-06-2008	
240	TDEVCSA2	First Teller	16-05-2008	
240	TELANGO	TELANGO	31-12-1799	
240	TGANESH	TGANESH	16-05-2008	
240	THARI	THARI	31-12-1799	
240	THARIKA	THARIKA	16-05-2008	
240	TIGNORE	TIGNORE	31-12-1799	
240	TJAGAN	TJAGAN	31-12-1799	
240	TJYOTI	TJYOTI	16-05-2008	
240	TKIRAN	Kiran	31-12-1799	
240	TKUMUD	TKUMUD	31-12-1799	
240	TMADHU	Madhusudhanan M	16-05-2008	
240	TMALA	TMALA	16-05-2008	
240	TMANISHA	TMANISHA	31-12-1799	
240	TMUDIT	TMUDIT	16-05-2008	
240	TNEW	TNEW	31-12-1799	Primary Password Expired
240	TRAJ	Raj	31-12-1799	
240	TRIAZ	TRIAZ	16-05-2008	
240	TSAGAR	TSAGAR	16-05-2008	
240	TSAISH	TSAISH	16-05-2008	
560	TSAISH560	SAISH 560	31-12-1799	
240	TSAMEER	TSAMEER	16-05-2008	
240	TSHAILEN	TSHAILEN	31-12-1799	Primary Password Expired
240	TSHANKAR	TSHANKAR	31-12-1799	Primary Password Expired
240	TSHIVANI	TSHIVANI	31-12-1799	
240	TSHYAM	TSHYAM	16-05-2008	
240	TTANMAY	TTANMAY	31-12-1799	
560	TTESTKUMUD	ttestkumud	31-12-1799	
240	TVIJAY	First teller	13-09-2008	

\*\*\* End of Report \*\*\*

4. On the File menu, click Print.
5. The system displays the **Print** dialog box.
6. Select the appropriate parameters and click the **OK** button.

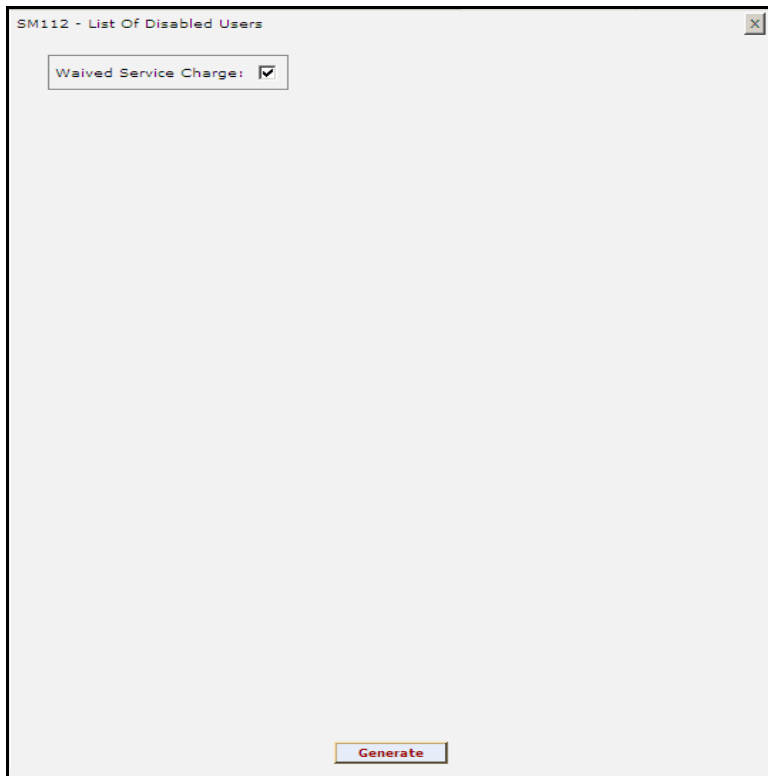
### SM112 - List Of Disabled Users

The system may disable certain user ID's due to wrong entry of password. This report is used by the systems administrator to keep track of such occurrences.

Each column in this report provides information about the User Number, User ID, User Name, and Cost Center.

#### To generate the List Of Disabled Users

1. Access the **Report Request** (Fast Path: 7775) screen.
2. Ensure that the **Adhoc Reports** button is selected.
3. Navigate through **Security Management > SMS Daily Reports > SM112 - List Of Disabled Users**.
4. The system displays the **SM112 - List Of Disabled Users** screen.



The screenshot shows a window titled "SM112 - List Of Disabled Users". Inside the window, there is a checkbox labeled "Waived Service Charge:" which is checked. At the bottom center of the window, there is a button labeled "Generate".

5. By default, the **Waived Service Charge** check box is selected. Clear the check box if you want to apply the service charge for the report.
6. Click the **Generate** button.
7. The system displays the message "Report Request Submitted". Click the **OK** button.
8. The system generates the **List Of Disabled Users**. For reference, a specimen of the report generated is given below:



Bank	:240 DEMO BANK	FLEXCUBE	Run Date	: 02 -FEB-2011
Branch	:534 DEMO	CLEARI LIST OF DISABLED USERS	Run Time	: 10:58 AM
Op. Id	:TSYSADMS34	As on 01 -Jan-2010	Report No:	SM112/1
-----				
User No.	User Id	User Name	Cost Center	
-----				
130	SHDFC9	First Supervisor	534	
-----				
*** End of Report ***				

## 2.2. Batch Reports

Batch reports are automatically generated at the end of day (EOD) or beginning of day (BOD). Reports and advices can be requested from the **Report Request** (Fast Path - 7775) screen. Batch reports can only be generated using the system operator login.

The operator must run the cut-off process at the end of every day, before starting the end of the day for that day. This is to ensure that all transactions done through the on-line delivery channels are handed over to a log for batch processing. A fresh log is created for the next day's transactions. Here it is important to note that while the processing date from the point of view of EOD processing is still today, the on-line processing date has moved to the next processing date and the online transactions done after cut-off will be processed in the next day's EOD.

EOD refers to the processing required to be done for each functional module of **FLEXCUBE Retail** as well as some files that are generated for updating data in other local offices. The EOD Client option is used to take care of the system related batch processes of cutoff, BOD, EOD, monthly report generation and printing, file hand off, eligibility of the Relationship Pricing (RP), etc.

Beginning of the Day (BOD) process opens a new transaction day for the Bank. BOD as a process depends on EOD process for the previous working day. This means, if the EOD is not completed for a day, system will not allow the BOD for the next day to start.

### List of Batch Reports:

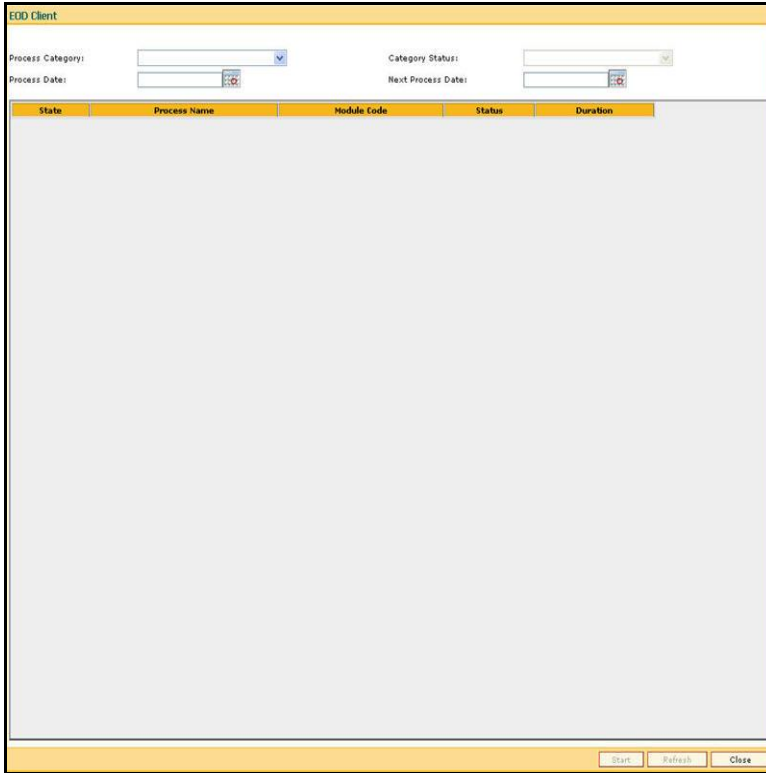
- SMS DAILY REPORTS

### Access

- Fast Path: EOD10
- Operator Process > EOD/BOD Operations > EOD Processing

### To generate batch reports

1. Take Pre Cutoff Backup before processing the EOD.
2. Log in to the **FLEXCUBE Retail** application with a valid System Operator Login ID.
3. The **FLEXCUBE Retail** window appears.
4. Access the **EOD Client** (Fast Path: EOD10) screen.



**Field Description**

Field Name	Description
<b>Process Category</b>	<p>[Mandatory, Drop-Down]</p> <p>Select the category of the process to be performed.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>End of Day:</b> It is a process where a fixed set of shell or functionality are processed. A proper handoff of GL's to <b>FLEXCUBE</b> Corporate, Consolidation etc. is done in the EOD process. Interest related processing, GL Updations, Draw-Down, Sweep-Outs, TD part redemption due to Sweep-In instructions, report related processing are done during the EOD processing.</li> <li>• <b>Beginning Of Day:</b> It is process where in some predefined functions are processed. The user can login in the system after the BOD is completed. The validation for BOD is that the previous day EOD should be completed. For e.g. TD Maturity, Standing Instruction (SI) Execution, etc.</li> <li>• <b>Cutoff:</b> It is a process where the process date of the system is changed to the next working day as maintained in the bank calendar. All the transactions entered in the system, till the point of cutoff, are picked up for EOD processing. The validation for cutoff is that the previous day BOD should be completed.</li> </ul>

Field Name	Description
	<ul style="list-style-type: none"> <li>• Transfer DB Scripts: This process was used earlier.</li> <li>• Apply DB Scripts: This process was used earlier.</li> <li>• Process CIF Handoff: This process is used to download the customers and related tables which are opened in other branch to the base branch of the customer. The validation for CIF handoff is that the previous day BOD should be completed.</li> <li>• Schedule Extracts: It is a processed to extract specific schedule and to have a proper handoff to the interface.</li> <li>• MONTHLY STATEMENTS: This process is used to generate the customer monthly statement in order to stream line the time during the actual EOM process. This process is run separately. This process can be run even after the BOD process next day.</li> <li>• Handoff After EOD: It is a processed to extract specific schedule and to have a proper handoff to the interface.</li> <li>• Elig Evaluation: It is a processed to evaluate the eligibility of the RVT schemes.</li> <li>• File Handoff: It is a processed to extract specific schedule and to have a proper handoff to the interface.</li> <li>• Automatic EFS for Converted Loan: This process is used to close the loan accounts with <b>Automatic EFS Date</b> falling on running day. If running of this process is skipped on a particular day, such accounts falling due for automatic closure on that day will be picked on next working day process. Future dated closure or back dated closure is not be supported. If the automatic closure date falls on a holiday, then such accounts will be picked up on the next working days process. All accounts attempted for such system initiated closure will be marked as <b>Tried</b> for both successful and failure cases. The accounts which are marked as <b>Tried</b> will not be picked up for further retries when the process is attempted at the later dates.</li> <li>• Mark for Write Off: In this process system displays the "Accounts marked for write off are pending processing. Cannot proceed" message for the account which are marked for write off for which the write off process has not been executed. If there are no accounts marked for write off, <b>FLEXCUBE</b> will start the process of marking accounts for write off based on the parameters defined. The system displays the message "SUCCESS MESSAGE" after the process is completed.</li> <li>• Automatic Write Off: In this process system displays the "No accounts marked for write off, Cannot Proceed" message if no account is write off for which the write off process. Accounts manually marked for write off will be fully written off irrespective of the present Credit Risk</li> </ul>

Field Name	Description
	Rating (CRR) status or the days past due. If the accounts are marked for write off, <b>FLEXCUBE</b> will write off the accounts if the accounts meet the eligibility criteria as on the date of write off. Accounting entries including off balance sheet entries will be passed by the system pertaining to written off accounts. The system displays the message "SUCCESS MESSAGE" after the process is completed.
<b>Category Status</b>	<p>[Mandatory, Drop-Down]</p> <p>This field displays the status of the selected category. The status can be as follows:</p> <ul style="list-style-type: none"> <li>• Yet to Start</li> <li>• Started</li> <li>• Aborted</li> <li>• Completed</li> </ul>
<b>Process Date</b>	<p>[Mandatory, Pick List, dd/mm/yyyy]</p> <p>Select the process date from the calendar.</p> <p>By default, this field displays the current process date for the selected process.</p>
<b>Next Process Date</b>	<p>[Mandatory, Pick List, dd/mm/yyyy]</p> <p>Select the next process date from the calendar.</p> <p>By default, this field displays the next logical working day on which the process has to be run.</p>
Column Name	Description
<b>State</b>	<p>[Display]</p> <p>This column displays a different colour for different process state.</p> <p>The different colour displayed are:</p> <ul style="list-style-type: none"> <li>• Green - Run</li> <li>• Red - Aborted</li> <li>• Default - Other Status (Complete, Yet to Start)</li> </ul>
<b>Process Name</b>	<p>[Display]</p> <p>This column displays the name of different processes which are performed.</p>
<b>Module Code</b>	<p>[Display]</p> <p>This column displays the code of the module on which the process is performed.</p>

Column Name	Description
<b>Status</b>	[Display] This column displays the status of the process performed. The status can be as follows: <ul style="list-style-type: none"> <li>• Yet to Start</li> <li>• Started</li> <li>• Aborted</li> <li>• Completed</li> </ul>
<b>Duration</b>	[Display] This column displays the duration for which the process was running, or when was the process completed.

5. Select **Cutoff** from the **Process Category** drop-down list.
6. Select the appropriate parameters in the **EOD Client** screen.
7. Click the **Start** button to start the cutoff process.
8. On successful completion of cutoff process, the system displays the message “Category Successfully Completed”.
9. Click the **OK** button.
10. Select **End of Day** from the **Process Category** drop-down list.
11. Click the **Start** button to start the EOD process.
12. On successful completion of EOD process, the system displays the message “Category Successfully Completed” and saves the reports in a folder in an appropriate location. For e.g. /home/wasadmin/USGapsSTR1/flexcube/host/runarea/rjsout.

**Note:** Once this is done, the operator should logout completely out of the system and login again. After the EOD Console is brought up again, the operator must check the process date displayed at the bottom right hand corner of the status bar below. The date should have moved to the next process date.

13. Take POSTEOD Backup for that process date before processing the BOD.
14. Select **Beginning of Day** from the **Process Category** drop-down list.
15. Click the **Start** button to start the EOD process.
16. On successful completion of BOD process, the system displays the message “Category Successfully Completed” and saves the reports in a folder in an appropriate location. For e.g. /home/wasadmin/USGapsSTR1/flexcube/host/runarea/rjsout.
17. Click the **OK** button.
18. Take POSTBOD Backup after executing the BOD.

### 2.2.1. SMS DAILY REPORTS

The SMS Daily Reports includes reports specific to the user profiles that are maintained daily.

#### List of SMS Daily Reports

- SM117 - User Profile Maintained Today
- SM120 – SMS Event Logs

### SM117 - User Profile Maintained Today

To carry out various activities in the system, users are added by the bank. Similarly, user profile modification/deletion is also performed according to the defined roles and business requirement. Any changes performed to the user profiles are logged and are reported end of the day.

This report is a list of user profiles maintained for the day. The lists of users along with the actions performed are listed in this report. Each column in this report provides information about User Number, User ID, User Name, Action, Action Date, Maker ID, and Checker ID.

#### Frequency

- Daily (EOD)

#### To view and print User Profile Maintained Today Report

1. Access the **Report Request** (Fast Path: 7775) screen.
2. Select the **Batch Reports** button.
3. Navigate through **Security Management > SMS DAILY REPORTS > SM117 - User Profile Maintained Today**.
4. The system displays the **SM117 - User Profile Maintained Today** screen.

SM117 - User Profile Maintained Today

Process Date[DD/MM/YYYY] : 15/02/2008

Branch Code Malang

View



## Field Description

Field Name	Description
<b>Process Date</b> [DD/MM/YYYY]	[Mandatory, dd/mm/yyyy] Type the date for which the report is processed. By default, the system displays the current process date.
<b>Branch Code</b>	[Mandatory, Drop-Down] Select the code of the branch for which the report needs to be viewed from the drop-down list.

5. Enter the appropriate parameters in the **SM117 - User Profile Maintained Today** screen.
6. Click the **View** button to view the report.
7. The system displays the **User Profile Maintained Today Report** screen.

FLEXCUBE						
Bank : Demo bank	USER PROFILE MAINTAINED TODAY				Run Date : 16/04/09	
Branch : 9999 Demo	For : 31-Jan-2009				Run Time : 8:02:35	
Op. Id : SYSOPER					Report No : SM117/1	
User No	User ID	User Name	Action	Action Date	Maker ID	Checker ID
70097	TR1	REPORTS TESTING	Added	16/04/09	SYSCASA	SYSADM01
70098	TR2	Reports Testing	Added	16/04/09	SYSCASA	SYSADM01
%%SM117.out,	9999					
*** End of Report ***						

8. Select the **Print** option from the **File** menu.
9. The system displays the **Print** dialog box.
10. Select the appropriate parameters and click the **OK** button.

## SM120 – SMS Event Logs

Bank required to have very strict control and vigilance in terms of access to the system. It is imperative for a bank to ensure that access to various modules/ transactions in is well controlled. To facilitate this control an Audit trail can be maintained for any task / transaction accessed by the user along with the terminal/machine where it has been performed. A log is then recorded and can be accessed by the bank at any future date.

Each column of the report provides information on User Id, Event Date and Time, Machine Name, Task Code, Task Description, and Action. Details are grouped branch wise.

### Frequency

- Daily (EOD)

### To view and print SMS Event Logs Report

1. Access the **Report Request** (Fast Path: 7775) screen.
2. Select the **Batch Reports** button.
3. Navigate through **Security Management > SMS DAILY REPORTS > SM120 – SMS Event Logs**.
4. The system displays the **SM120 – SMS Event Logs** screen.

SM120 - SMS Event Logs

Process Date[DD/MM/YYYY] : 31/12/2007

Branch Code Malang

View

**Field Description**

<b>Field Name</b>	<b>Description</b>
<b>Process Date</b> [DD/MM/YYYY]	[Mandatory, dd/mm/yyyy] Type the date for which the report is processed. By default, the system displays the current process date.
<b>Branch Code</b>	[Mandatory, Drop-Down] Select the code of the branch for which the report needs to be viewed from the drop-down list.

5. Enter the appropriate parameters in the **SM120 – SMS Event Logs** screen.
6. Click the **View** button to view the report.
7. The system displays the **SMS Event Logs Report** screen.

Bank :	9199 DEMO	FLEXCUBE	Run Time :	08:44PM2009	
Op. Id :	SYSOPER	AUDIT TRAIL REPORT	Report No:	SM120/1	
		For: 31-Dec-2007			
User Id	Event Date and Time	Machine Name	Task Code	Task Description	Action
Branch :					
*** No data for this Report ***					

8. On the **File** menu, click **Print**.
9. The system displays the **Print** dialog box.
10. Select the appropriate parameters and click the **OK** button.

### SM105 - Password Expiry Report

This report displays the list of users whose primary or secondary password has expired. This will be used by the system administrator to alert the respective users and to keep a log of updates.

Each column in this report provides information about User Number, User ID, User Name, Template, Employee Code, Last Password Change Date Primary/ Secondary, Inputter, Next Password Change Date Primary/ Secondary, Department Code, and Authoriser.

#### Frequency

- Daily (EOD)

#### To view and print Password Expiry Report

1. Access the **Report Request** (Fast Path: 7775) screen.
2. Select the **Batch Reports** button.
3. Navigate through **Security Management > SMS DAILY REPORTS > SM105 - Password Expiry Report**.
4. The system displays the **SM105 - Password Expiry Report** screen.

SM105 - Password Expiry Report

Process Date[DD/MM/YYYY] : 31/10/2010

Branch : TULSIANI - MUL

View



## Field Description

Field Name	Description
<b>Process Date</b> [DD/MM/YYYY]	[Mandatory, dd/mm/yyyy] Type the date for which the report is processed. By default, the system displays the current process date.
<b>Branch Code</b>	[Mandatory, Drop-Down] Select the branch for which the report needs to be viewed from the drop-down list.

5. Enter the appropriate parameters in the **SM105 - Password Expiry Report** screen.
6. Click the **View** button to view the report.
7. The system displays the **Password Expiry Report** screen.

SM105 - Password Expiry Report

Bank : 240 DEMO BANK LTD		FLEXCUBE		Run Date : 16-FEB-2011					
Branch :		Password Expiry Report		Run Time : 13:45 AM					
Op. Id : SYSOPER		As on 30-May-2010		Report No: SM105/1					
User No	User ID	User Name	Template	Emp Code	Last Pwd Chg Date	Inputter	Next Pwd Chg Date		
				Dept code	Primary	Authoriser	Primary		
					Secondary		Secondary		
9	C08621001	CHARU BHATIA INP RET INDERPURI	21	C0862	03-Aug-2009	5:25	SYSADMI1001	02-Sep-2009	5:25
				12	-	-	: SYSADMII1001	-	-
4	OPER1001	OPERATOR RET INDERPUR	0	10010	-	-	: 26261240	15-Oct-2008	12:00
				12	-	-	: V2180240	-	-
15	P39801001	PAWAN KUMAR BAJPAI INQ RET SAL INDERPURI	27	P3980	12-Aug-2009	1:27	SYSADMI1001	11-Sep-2009	1:27
				30	-	-	: SYSADMII1001	-	-
5	VTELLER1001	VAULT TELLER RET INDERPUR	0	1001V	-	-	: 26261240	15-Oct-2008	12:00
				12	-	-	: V2180240	-	-
* * * End of Report * * *									

8. Select the **Print** option from the **File** menu.
9. The system displays the **Print** dialog box.
10. Select the appropriate parameters and click the **OK** button.

## SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT

### SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT

The systems administrator needs to access certain system logs to track transactions performed across branches for compliance and related activities. This report is a log of the following activities.

1. Template Profile Add/ Amend/Cancel/Delete/Authorise
2. User Profile Add/Modify/Delete/Amend/Cancel/Authorize
3. Template Access Rights Selected Delete SM063
4. Template Access Rights Add
5. User Class Access Rights Add

This report provides details on - User ID, User No., User Name, Emp Code, Department Code, Date, Key Field, Task Code, Task Description

#### Frequency

- Daily EOD

#### To view and print SECURITY MANAGER DAILY ACTIVITY REPORT

1. Access the **Report Request** (Fast Path: 7775) screen.
2. Select the **Batch Reports** button.
3. Navigate through **Security Management > SMS DAILY REPORTS > SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT**.
4. The system displays the **SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT** screen.

## SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT

SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT

Process Date[DD/MM/YYYY] : 30/06/2010

Branch : TULSIANI - MUN

View

### Field Description

Field Name	Description
<b>Process Date[DD/MM/YYYY]</b>	[Mandatory, dd/mm/yyyy] Type the date for which the report is processed. By default, the system displays the current process date.
<b>Branch Code</b>	[Mandatory, Drop-Down] Select the code of the branch for which the report needs to be viewed from the drop-down list.

5. Enter the appropriate parameters in the **SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT** screen.
6. Click the **View** button to view the report.
7. The system displays the **SECURITY MANAGER DAILY ACTIVITY REPORT** screen.

SM108a - SECURITY MANAGER DAILY ACTIVITY REPORT

Bank :240 DEMO BANK		FLEXCUBE		Run Date : 09 -FEB-2011	
Branch :560 DEMO		Security Manager Daily Activity Report		Run Time : 7:02 PM	
Op. Id :SYSOPER		For 31 -Mar-2010		Report No: 1	
User Id Key Field	User No Task Code	User Name Task Description	Emp Code	Dept Code	Date
TSYSADM534 114	141 SMM01	First Teller Template Profile Add	11111	0	09 -FEB-2011 00:00
TSYSADM534 115	141 SMM01	First Teller Template Profile Add	11111	0	09 -FEB-2011 00:00
TSYSADM534 THDFC11 SMS	141 SMM12	First Teller User Class Access Rights Add	11111	0	09 -FEB-2011 00:00
TSYSADM534 THDFC10 SMS	141 SMM12	First Teller User Class Access Rights Add	11111	0	09 -FEB-2011 00:00
TSYSADM534 113	141 SMM01	First Teller Template Profile Add	11111	0	09 -FEB-2011 00:00
*** End of Report ***					

8. Select the **Print** option from the **File** menu.
9. The system displays the **Print** dialog box.
8. Select the appropriate parameters and click the **OK** button.