Oracle FLEXCUBE Direct Banking

Core Help Desk User Manual Release 12.0.3.0.0

Part No. E52543-01

April 2014



Core Help Desk User Manual

April 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/

Copyright © 2008, 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

1.	Pretace	4
2.	Transaction Host Integration Matrix	5
	Introduction	
4.	Advance Search	7
5.	Manage Policies	12

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 User Manual.

Transaction Host Integration Matrix provides information on host integration requirements for the transactions covered in the User Manual.

Introduction provides brief information on the overall functionality covered in the User Manual.

Chapters post Introduction are dedicated to individual transactions and its details, covered in the User Manual.

1.5 Related Information Sources

For more information on Oracle FLEXCUBE Direct Banking Release 12.0.3.0.0, refer to the following documents:

Oracle FLEXCUBE Direct Banking Licensing Guide

2. Transaction Host Integration Matrix

Legends

NH	No Host Interface Required
*	Host Interface to be developed separately
✓	Pre integrated Host interface available
×	Pre integrated Host interface not available

Transaction Name	FLEXCUBE UBS	Third Party Host System
Advance Search	NH	NH

3. Introduction

The Help Desk User module allows the Bank Administrator to carry out various transactions required on behalf of the customer. The transactions available for the Help Desk User are mainly for advance search and view purpose.

4. Advance Search

Using the **Advance Search** option the Help Desk User can carry out an advanced search to view the user details and login in the application on behalf of the selected use.

Advance Search



Field Description

Field Name	Description
User Type	[Mandatory, Drop-Down]
	Select the Type of Channel available under the User Type from the drop-down list.
	By default, the system displays the Internet channel.
First Name	[Optional, Drop Down, Alphanumeric, 40]
	Select the appropriate option from the drop-down list to indicate the position of the full/partial characters being entered in the text box forming first name of the user.
	The options are:
	Starts with
	Ends with
	• Equals
	• Contains
	The Search clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field.
	Type the search string in the adjacent field.
	For Example:
	If you select the search criteria as Starts With and enter A in the adjacent field, then the system displays all the customers' first names starting with A .

Field Name

Description

Last Name

[Optional, Drop Down, Alphanumeric, 40]

Select the appropriate option from the drop-down list to indicate the position of the full/partial characters being entered in the text box forming last name of the user.

The options are:

- Starts with
- Ends with
- Equals
- Contains

The *Search* clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field.

Type the search string in the adjacent field.

For Example:

If you select the search criteria as **Starts With** and enter **E** in the adjacent field, then the system displays all the customers' last names starting with **E**.

User ID

[Optional, Drop Down, Alphanumeric,18]

Select the appropriate option from the drop-down list to indicate the position of the full/partial characters being entered in the text box forming user ID of the user.

The options are:

- Starts with
- Ends with
- Equals
- Contains

The Search clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field.

Type the Search string in the adjacent field.

For Example:

If you select the search criteria as **Starts With** and enter **1** in the adjacent field, then the system displays the entire user IDs starting with **1**.

Field Name

Description

Email

[Optional, Drop Down, Alphanumeric, 18]

Select the appropriate option from the drop-down list to indicate the position of the full/partial characters being entered in the text box forming E-mail ID of the user.

The options are:

- Starts with
- Ends with
- Equals
- Contains

The *Search* clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field.

Type the search string in the adjacent field.

For Example:

If you select the *Search* criteria as **Starts With** and enter **L** in the adjacent field, then the system displays all the email IDs starting with **L**.

Customer Id

[Optional, Drop Down, Alphanumeric,20]

Select the appropriate option from the drop-down list to indicate the position of the full/partial characters being entered in the text box forming customer ID of the user.

The options are:

- Starts with
- Ends with
- Equals
- Contains

The Search clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field.

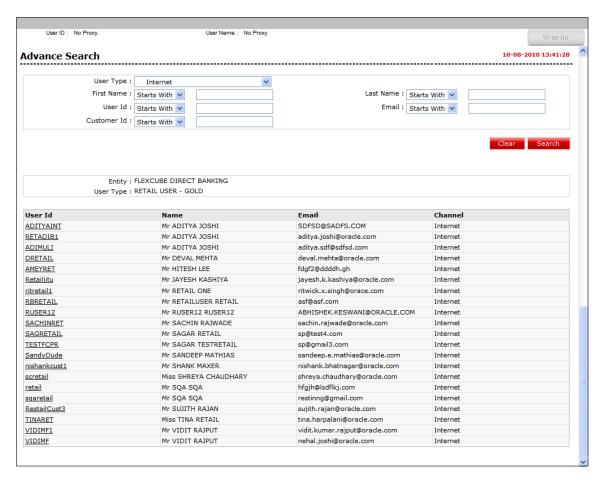
Type the search string in the adjacent field.

For Example:

If you select the *Search* criteria as **Starts With** and enter **1** in the adjacent field, then the system displays all the users whose customer ID starts with **1**.

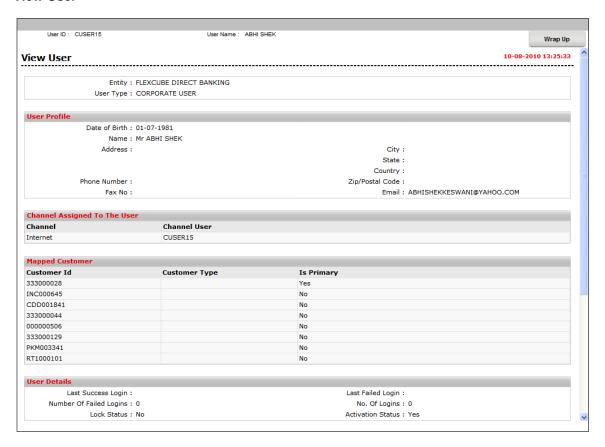
- 1. Enter the appropriate information in the relevant fields.
- 2. Click the **Search** button. The system displays the **Advance Search** screen with the search result.

Advance Search



3. Click the appropriate user id in the **User Id** column corresponding to the user. The system displays the View User screen.

View User



This will start the session on behalf of the user selected in the advanced search.

- 4. The Help Desk User will able to access inquiry transactions on behalf of the selected user. The Help Desk User needs to click on Wrap-Up to close the session.
- 5. Click the **Wrap Up** button shown at the upper right corner of the above screen. The system displays the initial **Advance Search** screen.

Advance Search



5. Manage Policies

The Bank Administrator can set User ID and Password Policy for different user types for available channels. The parameters can be set-up at each entity. The Manage Policy option allows the Bank Administrator to select the User Type and Type of Policy which is to be set up.

To set a Password Policy:

- 1. Logon to the Internet Banking application.
- Navigate through the menus to Maintenances > Manage Policy. The system displays the Manage Policy screen.

Manage Policy

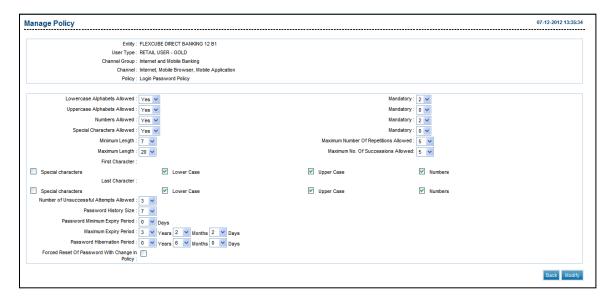


Field Description

Field Name	Description	
User Type	[Mandatory, Drop-Down] Select the User Type from the drop-down list.	
Select Policy Type	[Mandatory, Drop-Down] Select the Password Policy from the drop-down list. The options are:	
	Login Password Policy	
	 Transaction Password Policy 	
	User ID Policy	

- 3. Select the User Type and Login Password Policy from the drop-down list.
- 4. Click the **Get Details** button. The system displays the **Manage Policy** screen.
- 5. Select the appropriate Password Policy details. Here details are shown for the Login Password Policy.

Manage Policy - Login Password Policy



Manage Policy - User ID Policy



Field Description

Field Name	Description
Entity	[Display] This column displays the <i>Entity Name</i> .
User Type	[Display] This column displays the <i>Type of the User</i> .
Channel Group	[Display] This column displays the <i>Channel Group</i> for which the policy is being set.
Channel	[Display] This column displays the <i>Channel</i> for which the policy is being set.
Policy	[Display] This column displays the <i>Password Policy</i> set to the <i>User Type</i> .

Field Name Description Lowercase [Mandatory, Drop-Down] **Alphabets Allowed** Select whether the lowercase alphabets are allowed in a password. The options are: No Yes Mandatory [Conditional, Drop-Down] Select the number of lowercase characters allowed in a password from the drop-down list. The options are: 0 1 2 3 4 5 **Uppercase** [Mandatory, Drop-Down] **Alphabets Allowed** Select whether the uppercase alphabets are allowed in a password from the dropdown list. The options are: No Yes **Mandatory** [Conditional, Drop-Down] Select the number of uppercase characters allowed in a password from the drop-down list. This drop-down list is disabled if No is selected in Uppercase Alphabets Allowed. The options are: 0 1 2 3 4

5

Field Name Description Numbers Allowed [Mandatory, Drop-Down] Select numbers allowed from the drop-down list to allow numeric values in the password. The options are: No Yes Mandatory [Conditional, Drop-Down] Select the number of numeric characters allowed in a password from the drop-down list. This drop-down list is disabled if **No** is selected in **Numbers** Allowed. The options are: 0 1 2 3 4 5 Special [Mandatory, Drop-Down] Characters Select Special Characters Allowed from the drop-down list to **Allowed** allow special characters in the password. The options are: No Yes Mandatory [Conditional, Drop-Down] Select the number of special characters allowed in a password from the drop-down list.

This drop-down list is disabled if No is selected in Numbers

Allowed.

Field Name Description Minimum Length [Mandatory, Drop-Down] Select the Minimum Password Length from the drop-down list. The options are: 5 6 7 8 9 10 Maximum No. of [Mandatory, Drop-Down] Repetitions Select the Maximum Number of Repetitions allowed from the Allowed drop-down list. The options are: [0-20]**Maximum Length** [Mandatory, Drop-Down] Select the Maximum Password Length from the drop-down list. Maximum No. Of [Mandatory, Drop-Down] **Successions** Select the number of successful attempts allowed to enter a Allowed password from the drop-down list. First Character In [Mandatory, Check Box] **Password** Select the check box to select the first character of the password. The options are: Special Character: If this check box is selected then user can enter special characters as first character of the password. Lower Case: If this check box is selected then user can enter first character in lower case. Upper Case: If this check box is selected then user can enter first character in upper case.

can enter first character as numeric.

Numbers: If this check box is selected then user

Field Name Description Last Character In [Mandatory, Check Box] Password Select the check box to select the last character of the password. The options are: Special Character: If this check box is selected then user can enter special characters as last character of the password. Lower Case: If this check box is selected then user can enter last character in lower case. Upper Case: If this check box is selected then user can enter last character in upper case. Numbers: If this check box is selected then user can enter last character as numeric. Number of [Mandatory, Drop-Down] Unsuccessful Select the Number of Unsuccessful Attempts allowed from the **Attempts Allowed** drop-down list. The account will be locked after the specified number of attempts. Note: This field will be enabled only for password policy. **Password History** [Mandatory, Drop-Down] Size Select the Password History from the drop-down list. The system retains a log of old passwords which cannot be repeated. Note: This field will be enabled only for password policy. Password [Mandatory, Drop-Down] **Minimum Expiry** Select the password minimum expiry period from the drop-down Period list. **Note**: This field will be enabled only for password policy. **Maximum Expiry** [Mandatory, Drop-Down] Period Select the Password Maximum Expiry Period in Years, Month and Days from the drop-down list. The values are: Years - [0-10] Months - [0-11]

Note: The period set cannot be less than the minimum password expiry period.

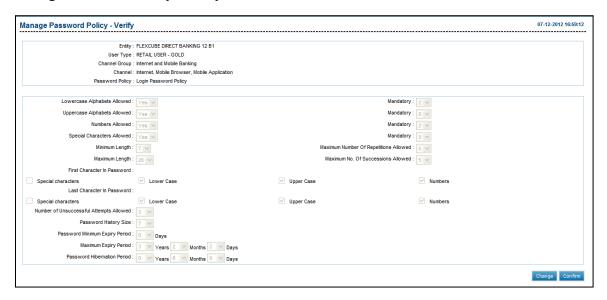
Days - [0-30]

Field Name	Description		
Password	[Mandatory, Drop-Down]		
Hibernation Period	Select the password Hibernation Period from the drop-down list.		
	Note : This field will be enabled only for <i>Password Policy</i> .		
Forced Reset Of	[Mandatory, Check Box]		
Password With Change In Policy	Select the Forced Reset Of Password With Change In Policy check box this forces the users to change password with each change in the password policy.		
	Note : This field will be enabled only for password policy.		

Click the Modify button. The system displays the Manage Password Policy - Verify screen.
 OR

Click the **Back** button to return to the previous screen.

Manage Password Policy - Verify

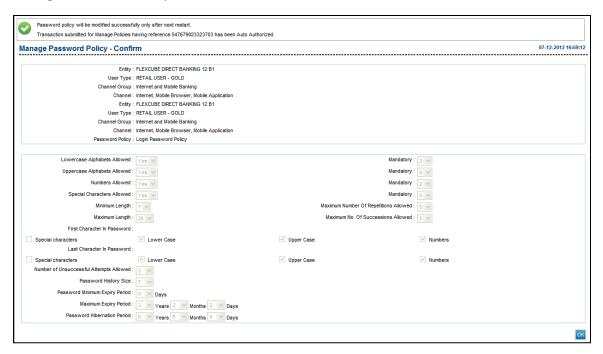


7. Click the **Confirm** button. The system displays the **Manage Password Policy - Confirm** screen with the status message.

OR

Click the **Change** button to go to the previous screen.

Manage Password Policy - Confirm



8. Click the **OK** button. The system displays the *Manage Policy* screen.

5.2 Automatic Unlock of Transaction Password

If a user enters the incorrect password consecutively for more than particular number of times, the *Transaction Password* is then locked. The system then unlocks the same after the specific time set during the configuration.

Note: Please refer to the following example for easier understanding of the feature.

For Example:

The *Transaction Password* is/can be locked in the following situation:

Scenario	Result
If a user enters the incorrect <i>Transaction</i> Password 5 times (Default OR value set by the user) consecutively within the same day.	The <i>Transaction Password</i> remains unlocked.
If a user enters the incorrect <i>Transaction</i> Password 6 times (Default OR value set by the user) consecutively within the same day.	The <i>Transaction Password</i> gets locked and is <i>automatically unlocked after</i> 24 <i>hours</i> .
If a user enters the incorrect transaction password 10 times (Default OR value set by the user) consecutively within the same day.	The <i>Transaction Password</i> gets locked and is <i>automatically unlocked after</i> 24 <i>hours</i> .
If a user enters the incorrect transaction password 11 times (Default OR value set by the user) consecutively within the same day.	The <i>Transaction Password</i> gets locked and will have to be <i>manually unlocked</i> by the <i>bank</i> or corporate administrator.

Note: The user is notified while locking the *Transaction Password*.