

Oracle® Retail Merchandising Cloud Services

Administration Guide

Release 16.0.025

E95222-01

April 2018

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Nathan Young

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.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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 fail-safe, 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.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

- (i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.
- (ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.
- (iii) the software component known as **Access Via**™ licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.
- (iv) the software component known as **Adobe Flex**™ licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all

reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

Send Us Your Comments	vii
Preface	ix
Audience	ix
Customer Support	ix
Improved Process for Oracle Retail Documentation Corrections	ix
Oracle Retail Documentation on the Oracle Technology Network	x
Conventions	x
 1 Administrative Tasks	
Oracle Support	1-1
User Creation	1-1
Assigning Members to a Role	1-3
Retail Merchandising System (RMS) Security Implementation	1-6
Setup Role Privileges	1-6
Setup Security Group Attribute	1-10
Setup Security User and Security User Role	1-14
Map Security User with Security Group	1-19
Setup Merchandise Hierarchy LOV Filtering Access Information	1-23
Retail Merchandising Cloud Services Default Enterprise Roles	1-28
Revoking Role Membership	1-29
Deleting a User or Disabling User Privileges	1-31
Resetting a User Password	1-32
Approve Requests from User	1-34
Approve Requests from User for Multiple Roles	1-35
Importing a Batch of User Accounts	1-37
Bulk Role Membership Update (Optional)	1-38
Nightly Batch File Uploads	1-38
Adding Authorized Keys	1-38
Steps – Login to WinSCP	1-40
Steps to Upload the Batch File	1-42
Export File Downloads	1-43

Send Us Your Comments

Oracle® Retail Merchandising Cloud Services Administration Guide, Release 16.0.025

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at <http://www.oracle.com>.

Preface

This guide describes the administration tasks for Oracle Retail Merchandising Cloud Services.

Audience

This guide is intended for administrators.

This guide describes the administration tasks for Oracle Retail Merchandising Cloud Services.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

<http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html>

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the

same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Oracle Retail product documentation is available on the following web site:

<http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html>

(Data Model documents are not available through Oracle Technology Network. You can obtain these documents through My Oracle Support.)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Administrative Tasks

This chapter describes the processes for maintaining users and roles as well as batch processes. For information regarding standard end user activities like creating and viewing reports, please see the *Oracle Retail Merchandising Cloud Services User Guide*.

Oracle Support

It is considered to be a best practice to have all Oracle Retail Merchandising Cloud Services support requests submitted through a single point of contact for that customer environment; the client designated administrator is usually designated to perform this role.

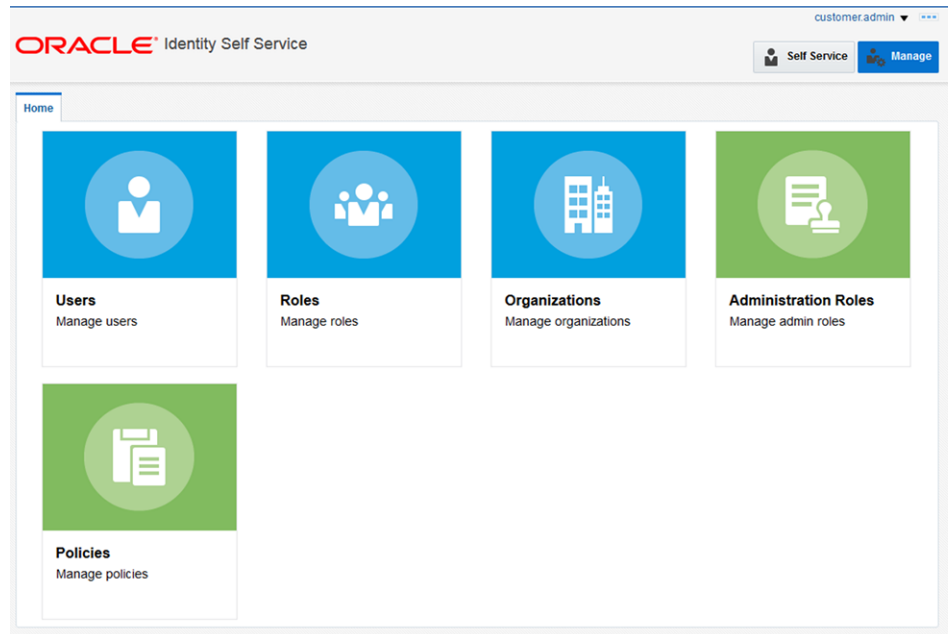
The link to use when submitting Service Requests (SR) is:

<https://support.oracle.com>

User Creation

Before users can access the Oracle Retail Merchandising Cloud Services applications it is necessary to provision each user access to the system, and assign roles to each user to control what functionality will be available to them. The access provisioning is done using Oracle Identity Management (OIM). The following steps explain how to define users, assign roles and revoke access for users when needed. The OIM Application URL and the login with the required administrator access would be needed to execute the below steps:

1. Log into the OIM application.
2. Under Administration, click **Users**.

Figure 1–1 Select Users

3. Under Actions, click **Create**.

Figure 1–2 Select Create

The Create User screen opens.

4. Under Basic Information, enter the following:
 - First Name
 - Last Name
 - For Organization, enter *Retail*
 - For User Type, enter *Full time employee*
 - For E-mail, enter the e-mail address of the employee
5. Under Account Settings, enter the following:
 - User Login: <firstname>.<lastname>
 - Password, enter a password
 - Confirm Password, reenter the password

Figure 1–3 Complete User Information

Create User

Request Information

Effective Date

Justification

Basic Information

* First Name

Middle Name

* Last Name

* E-mail

Manager

* Organization

* User Type

Display Name

Account Settings

User Login

Password

* Confirm Password

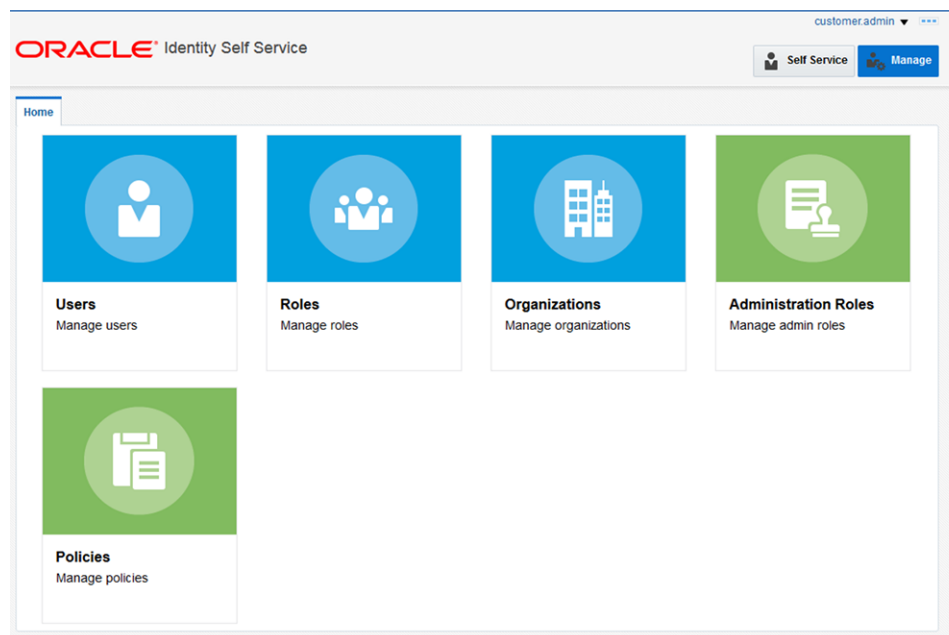
Buttons: Submit, Save As..., Cancel

6. Click **Submit**.

Assigning Members to a Role

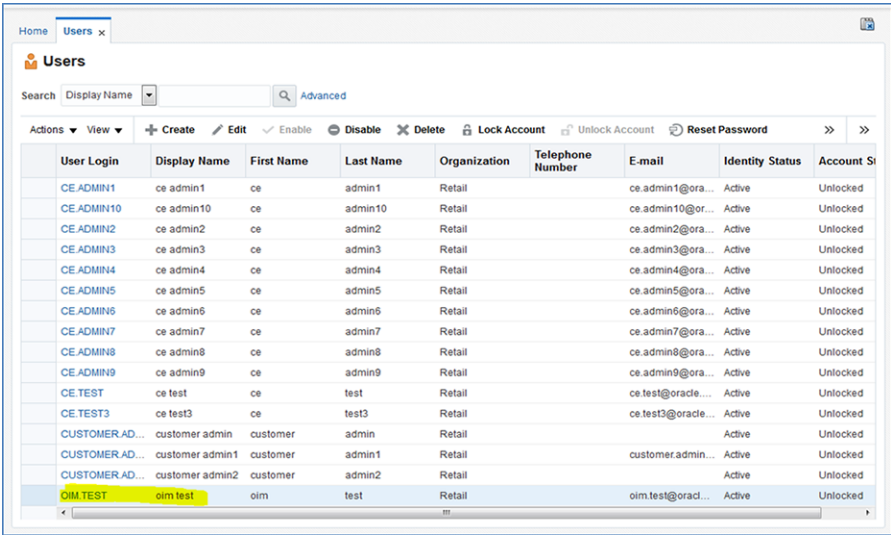
To assign members to a role, complete the following:

1. Log into the OIM application.
2. Click **Users**.

Figure 1–4 Select Users

3. Click the oim.test user.

Figure 1–5 oim.test User

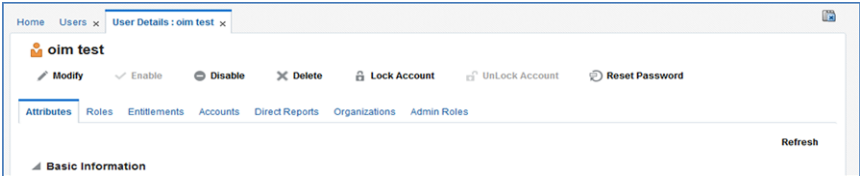


The screenshot shows the 'Users' management page in Oracle Retail Merchandising Cloud Services. A table lists various users, including several 'CE ADMIN' users, 'CE TEST' users, 'CUSTOMER AD...' users, and the 'oim.test' user. The 'oim.test' user is highlighted in blue. The table columns are: User Login, Display Name, First Name, Last Name, Organization, Telephone Number, E-mail, Identity Status, and Account Status.

User Login	Display Name	First Name	Last Name	Organization	Telephone Number	E-mail	Identity Status	Account Status
CE ADMIN1	ce admin1	ce	admin1	Retail		ce.admin1@ora...	Active	Unlocked
CE ADMIN10	ce admin10	ce	admin10	Retail		ce.admin10@or...	Active	Unlocked
CE ADMIN2	ce admin2	ce	admin2	Retail		ce.admin2@ora...	Active	Unlocked
CE ADMIN3	ce admin3	ce	admin3	Retail		ce.admin3@ora...	Active	Unlocked
CE ADMIN4	ce admin4	ce	admin4	Retail		ce.admin4@ora...	Active	Unlocked
CE ADMIN5	ce admin5	ce	admin5	Retail		ce.admin5@ora...	Active	Unlocked
CE ADMIN6	ce admin6	ce	admin6	Retail		ce.admin6@ora...	Active	Unlocked
CE ADMIN7	ce admin7	ce	admin7	Retail		ce.admin7@ora...	Active	Unlocked
CE ADMIN8	ce admin8	ce	admin8	Retail		ce.admin8@ora...	Active	Unlocked
CE ADMIN9	ce admin9	ce	admin9	Retail		ce.admin9@ora...	Active	Unlocked
CE TEST	ce test	ce	test	Retail		ce.test@oracle...	Active	Unlocked
CE TEST3	ce test3	ce	test3	Retail		ce.test3@oracle...	Active	Unlocked
CUSTOMER AD...	customer admin	customer	admin	Retail			Active	Unlocked
CUSTOMER AD...	customer admin1	customer	admin1	Retail		customer.admin...	Active	Unlocked
CUSTOMER AD...	customer admin2	customer	admin2	Retail			Active	Unlocked
oim.test	oim test	oim	test	Retail		oim.test@oracl...	Active	Unlocked

4. Click the Roles tab.

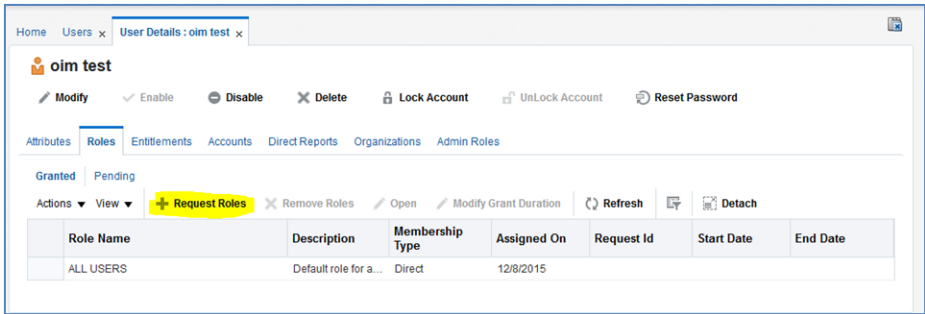
Figure 1–6 Roles Tab



The screenshot shows the 'User Details' page for the 'oim.test' user. The 'Roles' tab is selected, and the 'Basic Information' section is visible. The page includes tabs for Attributes, Roles, Entitlements, Accounts, Direct Reports, Organizations, and Admin Roles. A 'Refresh' button is located on the right side of the 'Basic Information' section.

5. Click the Request Roles button.

Figure 1–7 Request Roles Button



The screenshot shows the 'User Details' page for the 'oim.test' user, with the 'Roles' tab selected. The 'Request Roles' button is highlighted in yellow. Below the button, there is a table listing roles. The table columns are: Role Name, Description, Membership Type, Assigned On, Request Id, Start Date, and End Date.

Role Name	Description	Membership Type	Assigned On	Request Id	Start Date	End Date
ALL USERS	Default role for a...	Direct	12/8/2015			

6. Click the Add to Cart button next to the role you want to assign.

Figure 1–8 Adding Roles to the Cart

Home Users x User Details : oim test x Role Access Request x

Back Add Access Checkout Cancel Next

Cart oim test 1

Search and select individual items from the Catalog tab. Sets of pre-bundled items commonly used in your organization can be selected from the Request Profiles tab.

Catalog Request Profiles

Search Keyword Search

Categories Sort By Display Name Add Selected to Cart

Select	Role	Action
☒	OIMTest	Add to Cart
☒	Test1	<input checked="" type="button" value="Add to Cart"/>
☐	customer_admin	Add to Cart

7. Click Next.

Figure 1–9 Add Access Request

Home Users x User Details : oim test x Role Access Request x

Back Add Access Checkout Cancel Next

Cart oim test 1

Search and select individual items from the Catalog tab. Sets of pre-bundled items commonly used in your organization can be selected from the Request Profiles tab.

Catalog Request Profiles

Search Keyword Search

Categories Sort By Display Name Add Selected to Cart

Select	Role	Action
☒	OIMTest	Add to Cart
☒	Test1	<input checked="" type="button" value="Add to Cart"/>
☐	customer_admin	Add to Cart

8. Click Submit.

Figure 1–10 Submit Access Request

Home Users x User Details : oim test x Role Access Request x

Back Add Access Checkout Cancel Next

Cart oim test 1

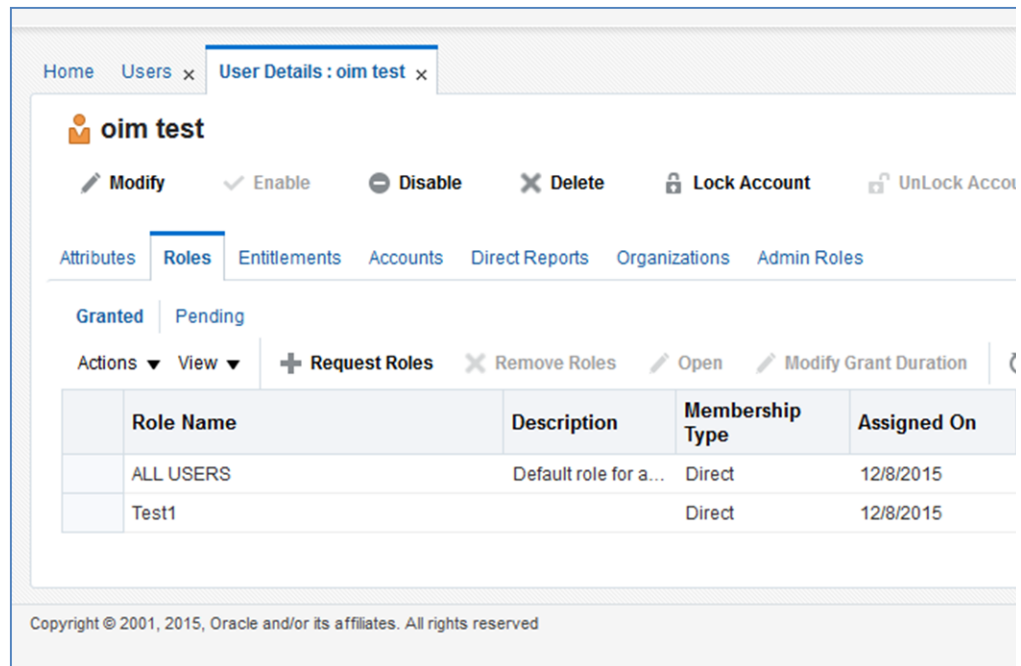
Cart Details

Request Information

Justification

Submit Save As...

The role is now assigned to the User.

Figure 1–11 User Details

Retail Merchandising System (RMS) Security Implementation

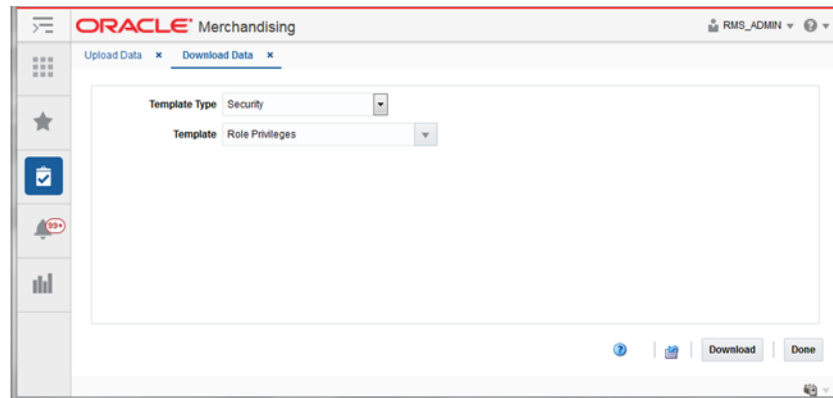
If Data Level Security is enabled in RMS then for the users to have access to the data, the below must be setup through the Data Upload Utility available in the RMS application:

- Role Privileges
- Security Group Attribute
- Security User and Security User Role
- Security User and Security Group mapping information
- Merchandise Hierarchy LOV filtering access information

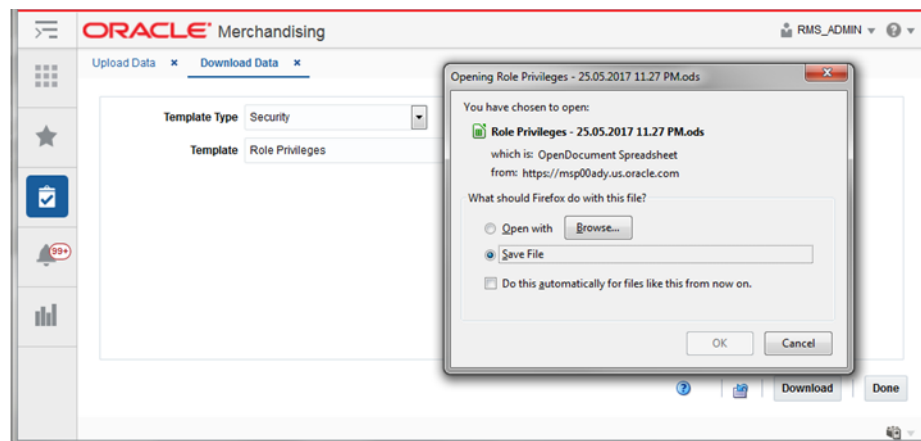
Setup Role Privileges

The setup of role privileges is required for purchase order approval.

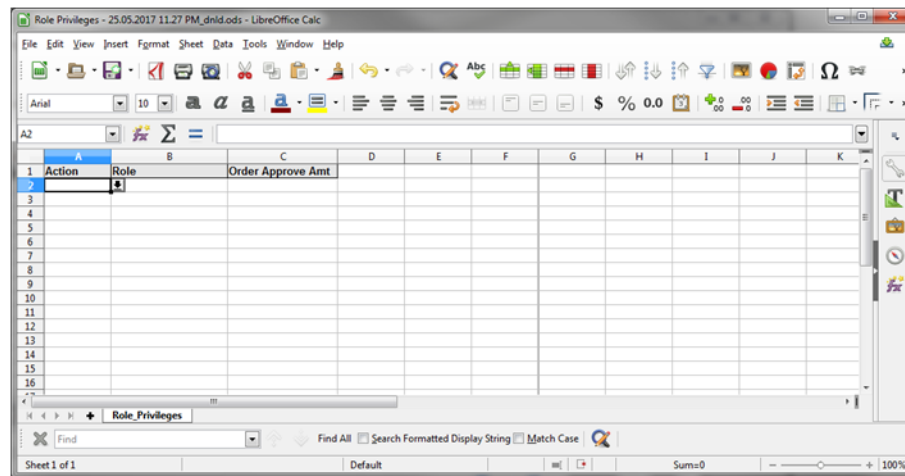
1. Log into the RMS Application.
2. Navigate to Foundation Data > Data Loading > Download.
3. In the Download Data screen, select:
 - Template Type as 'Security'
 - Template as 'Role Privileges'

Figure 1–12 Download Security Privileges Template Spreadsheet

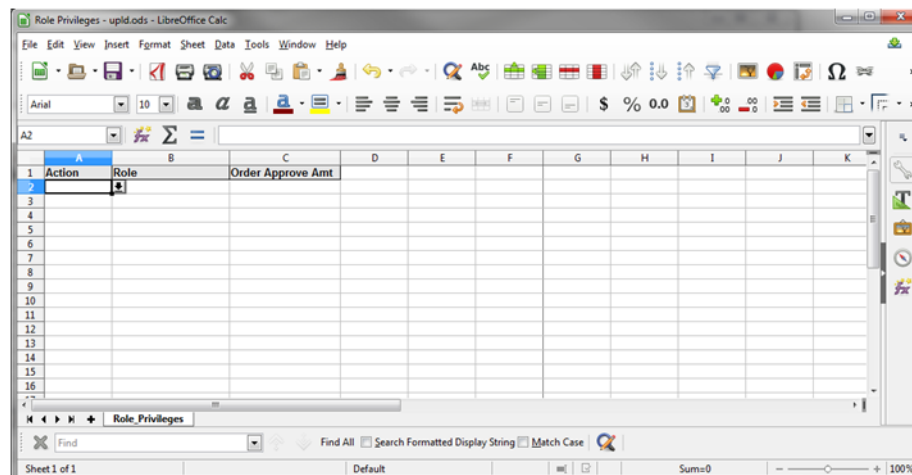
4. Click the **Download** button.
5. Save File to the local directory location when prompted.

Figure 1–13 Save File

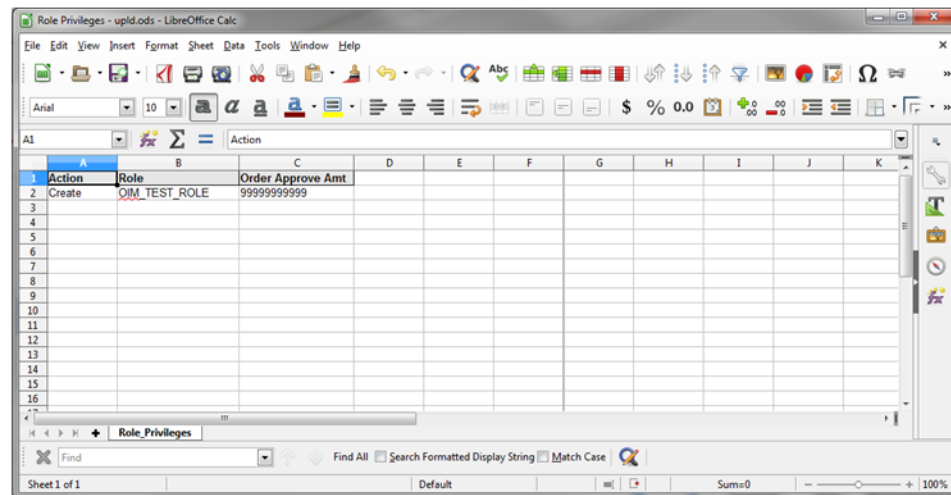
6. Click the **Done** button.
7. Open the downloaded file.

Figure 1–14 Open File

8. Save As < file name>.

Figure 1–15 Save as <File Name>

9. In the Security_Groups tab, enter/select the following:
 - Action: 'Create'
 - Role: <Role>
 - Order Approve Amt: < Upper limit that the role will be able to approve on an order

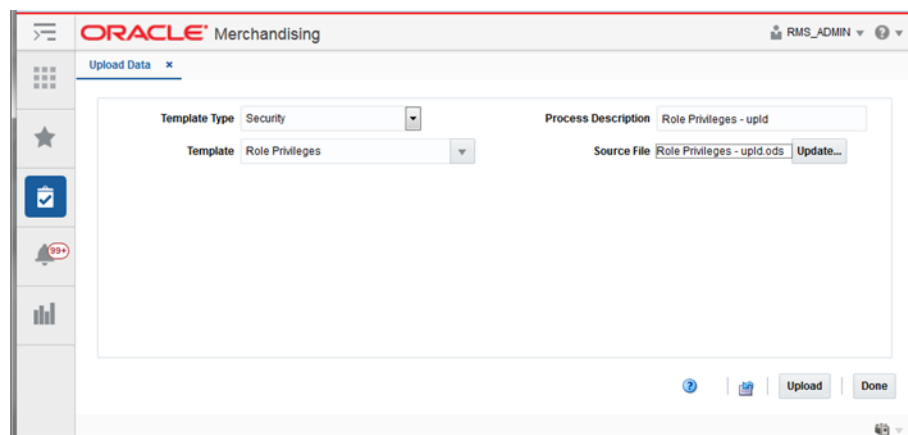
Figure 1–16 Enter Role Privileges information

10. Save and Close the file.

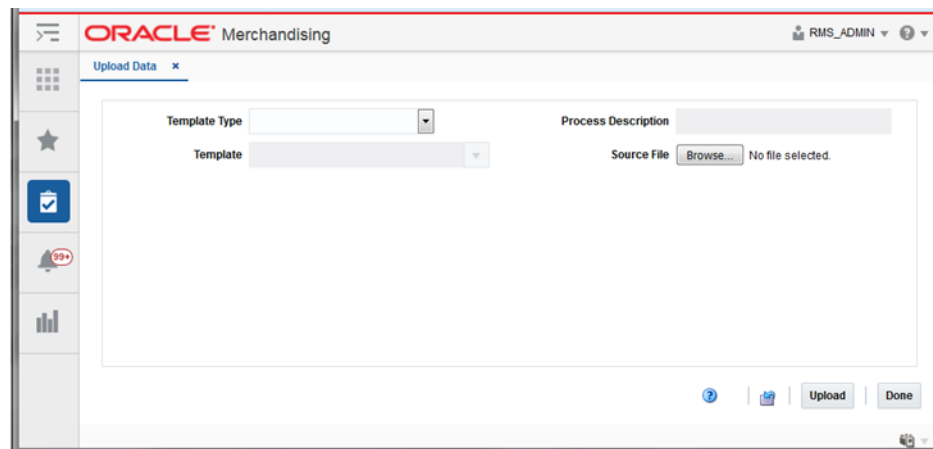
11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.

12. In the Upload Data screen, select:

- Template Type as 'Security'
- Template as 'Role Privileges'
- Enter new Process Description or retain as is
- Browse and select the Source file that was created in Step 10

Figure 1–17 Upload Role Privileges Information

13. Click the **Upload** button.

Figure 1–18 Upload Role Privileges Information Complete

14. Click the **Done** button..
15. View the newly created Role Privileges by downloading the Role privileges spreadsheet (Steps 2 - 7).

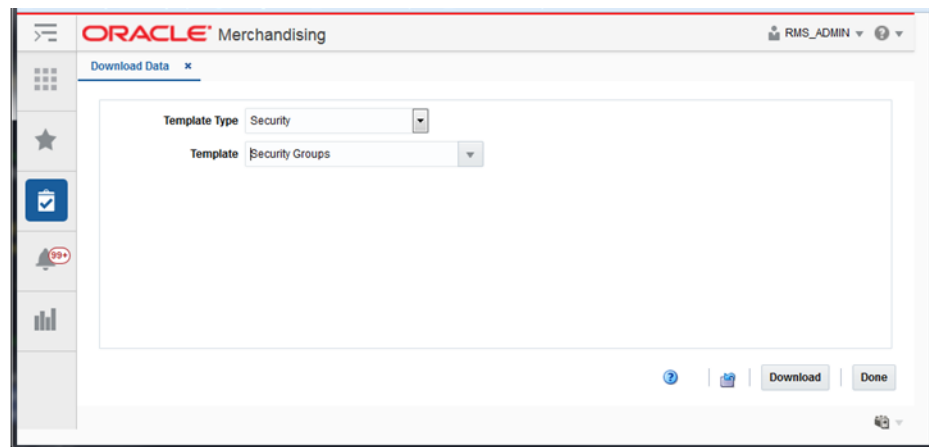
Figure 1–19 View Newly Created Role Privilege

A1	B1	C1	D1	E1	F1	G1	H1	I1	J1	K1	L1
1	Action	Role	Order Approve Amt								
2	Update	OIM_TEST	999999999999								
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											

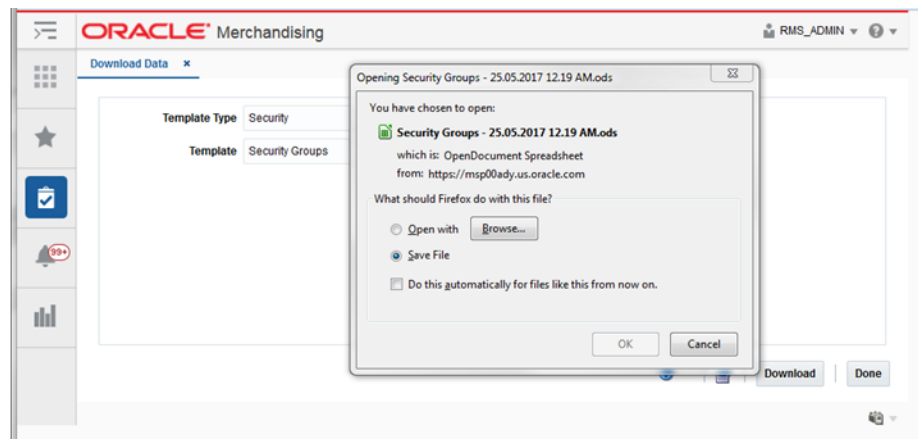
Setup Security Group Attribute

Perform the following procedure to define a Security Group in the system.

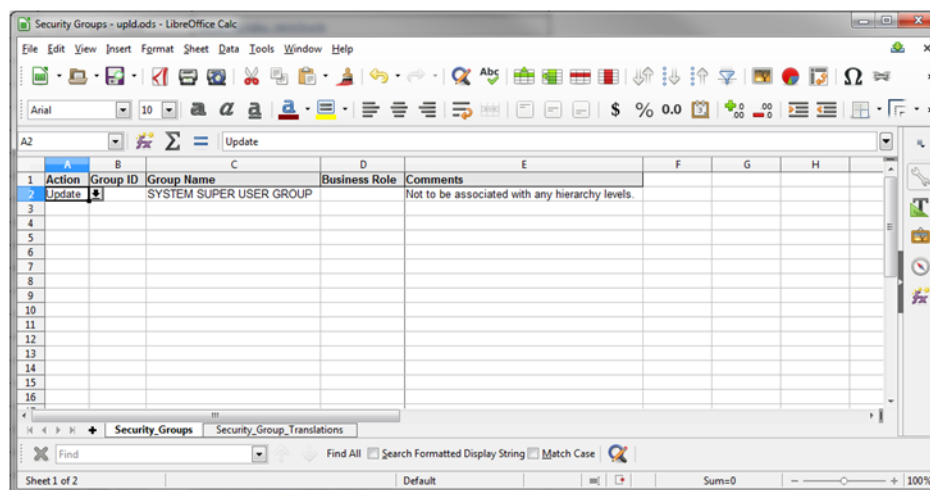
1. Navigate to Foundation Data > Data Loading > Download.
2. In the Download Data screen, select Template Type as 'Security' and Template as 'Security Groups'.

Figure 1–20 Download Security Groups Template Spreadsheet

3. Click the **Download** button.
4. Save File to a local directory location when prompted.

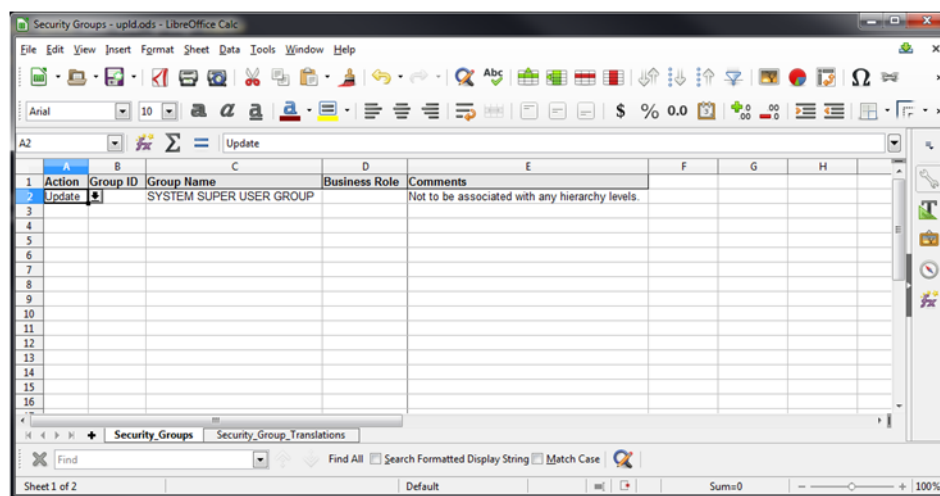
Figure 1–21 Save File

5. Click the **Done** button.
6. Open the downloaded file.

Figure 1–22 Open File

Note: The application User IDs can be mapped to the seeded Security Group (for example, SYSTEM SUPER USER GROUP) or new Security Groups can be defined. In order to define new Security Groups follow below steps.

7. Save As < file name>.

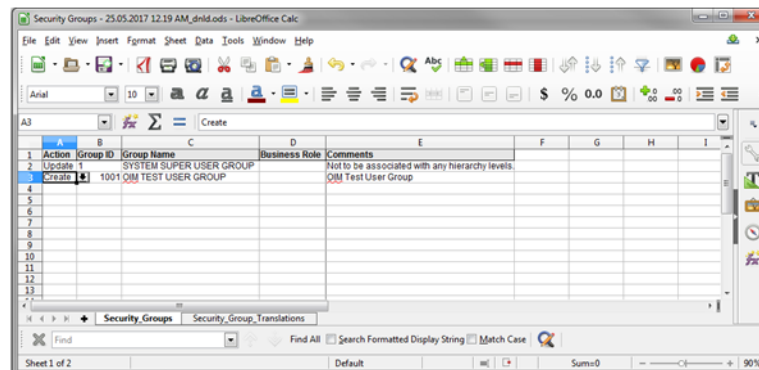
Figure 1–23 Save as <File Name>

8. In the Security_Groups tab, enter/select the following:

- Action: 'Create'
- Group ID: <Group ID>
- Group Name: <Group Name>
- Business Role: <role> (optional)
- Comments: <comments> (optional)

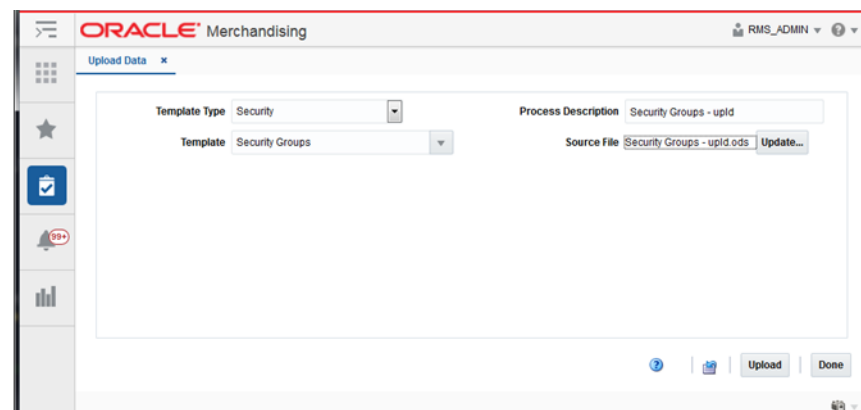
9. In the Security_Groups_Translations tab, enter the translated Security Group descriptions (optional).

Figure 1–24 Enter Security Groups information

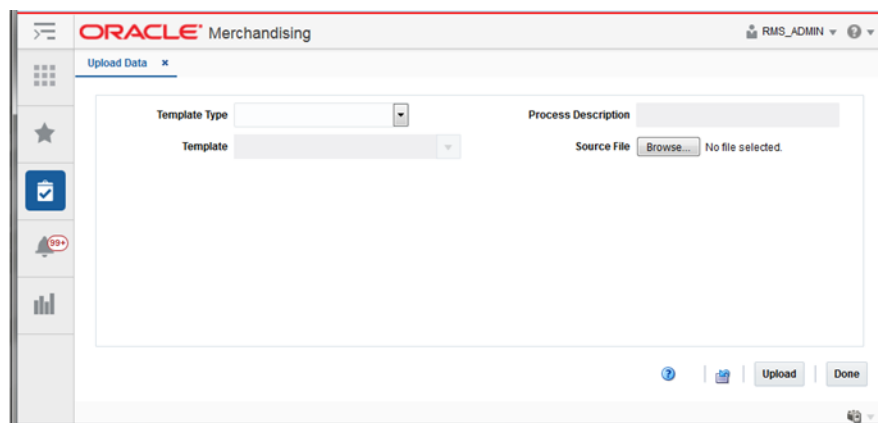


10. Save and Close the file.
11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
12. In the Upload Data screen, select:
 - Template Type as 'Security'
 - Template as 'Security Groups'
 - Enter new Process Description or retain as is
 - Browse and select the Source file that was created in Step 10

Figure 1–25 Upload Security Groups Information



13. Click the **Upload** button.

Figure 1–26 Upload Security Group Information Complete

14. Click the **Done** button.
15. View the newly created Security Group by downloading the Security Groups spreadsheet (Steps 1 - 6).

Figure 1–27 View newly created Security Group

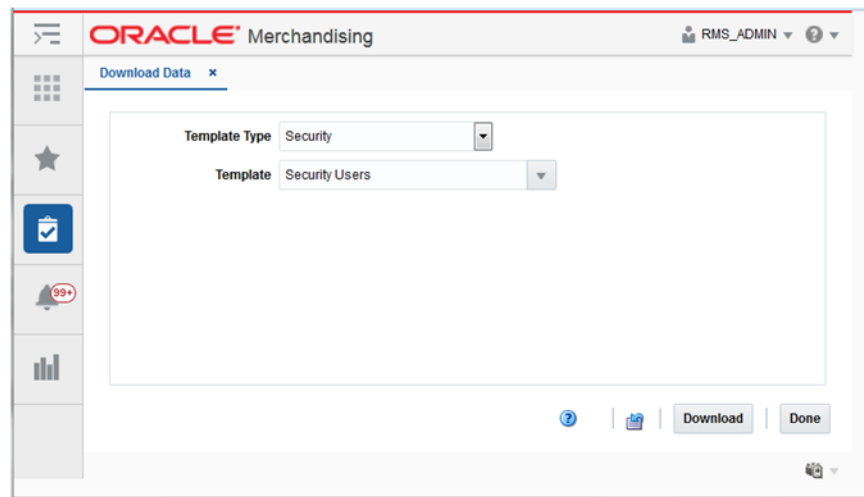
Action	Group ID	Group Name	Business Role	Comments
Update	1	SYSTEM SUPER USER GROUP		Not to be associated with any hierarchy levels.
Update	1001	OIM TEST USER GROUP		OIM Test User Group

Note: The system generated Group ID. This Group ID should be mapped to the Security Users.

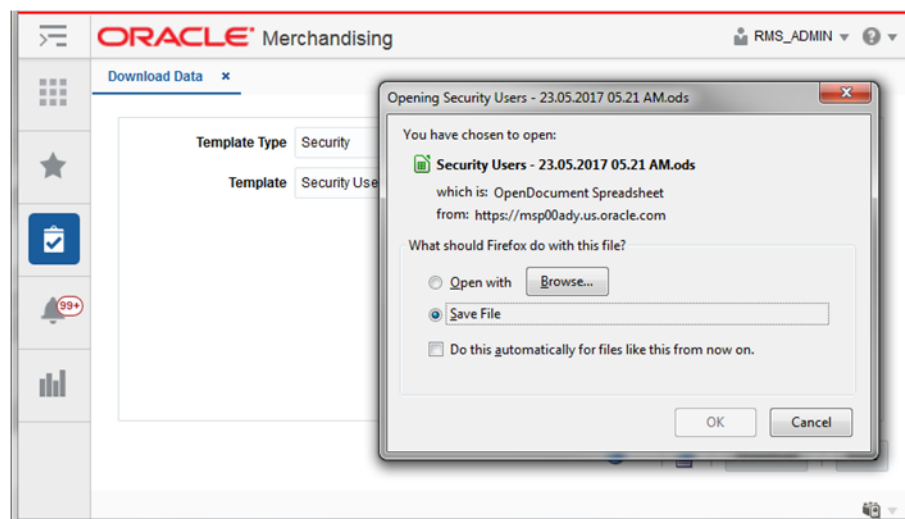
Setup Security User and Security User Role

The LDAP User ID used to login to the RMS application must be defined as a Security User.

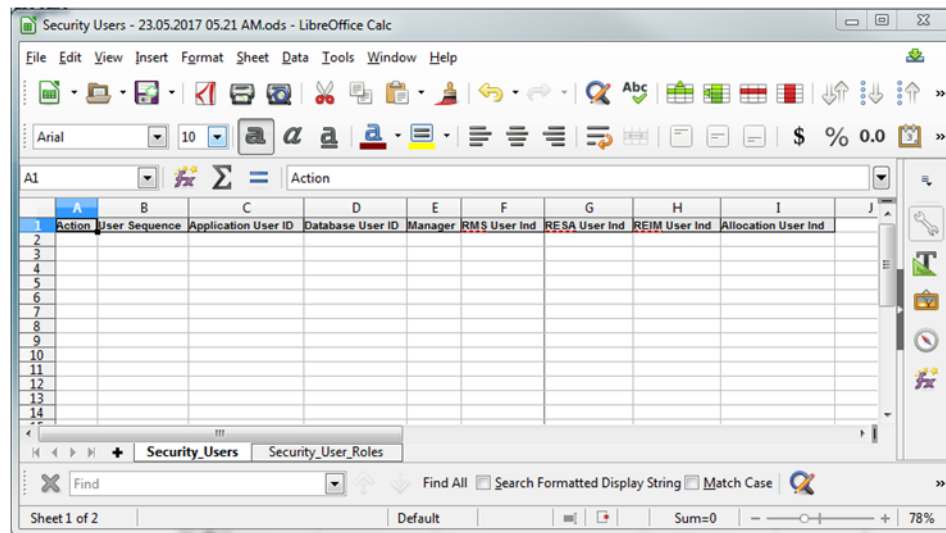
1. Navigate to Foundation Data > Data Loading > Download.
2. In the Download Data screen, select Template Type as 'Security' and Template as 'Security Users'.

Figure 1–28 Download Security Users template spreadsheet

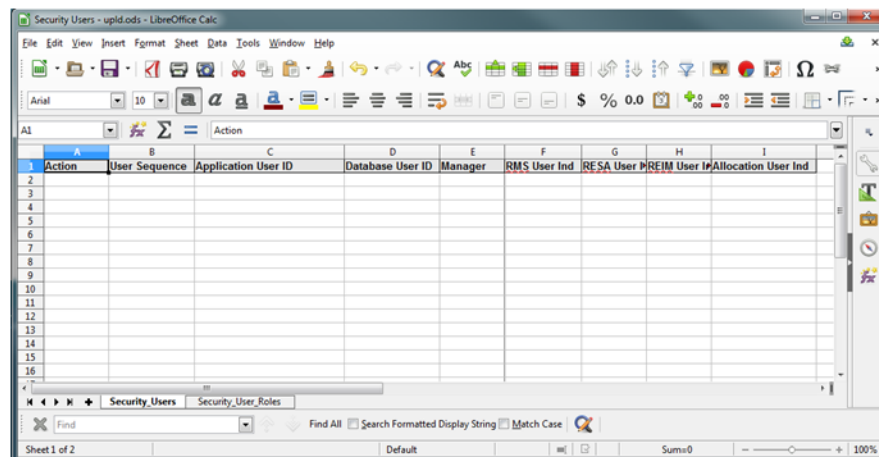
3. Click the **Download** button.
4. Save File to local directory location when prompted.

Figure 1–29 Save File

5. Click the **Done** button.
6. Open the downloaded file.

Figure 1–30 Open File

7. Save As < file name>.

Figure 1–31 Save as <File Name>

8. In the Security_Users tab, enter/select the following:

- Action: 'Create'
- User Sequence: <number>
- Application User ID: <Application User ID>
- RMS User Ind: Yes
- ReSA User Ind: Yes/No
- ReIM User Ind: Yes/No
- Allocation User Ind: Yes/No

Figure 1–32 Security Users Information

	A	B	C	D	E	F	G	H	I
	Action	User Sequence	Application User ID	Database User ID	Manager	RMS User Ind	RE SA User	PREIM User	Allocation
2	Create	15001	OIM TEST			Yes	No	No	No
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

9. In the Security_User_Roles tab, enter/select the following:

Note: Proceed to set up Security User Role, only if Role Privileges have been setup.

- Action: 'Create'
- User Sequence: <number>

Note: This must be the User Sequence provided in the Security_Users tab.

- Role: <Role>

Figure 1–33 Security User Roles Information

	A	B	C	D	E	F	G	H	I	J	K
	Action	User Sequence	Role								
2	Create	15001	OIM TEST ROLE								
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											

10. Save and Close the file.

11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.

12. In the Upload Data screen, select:

- Template Type as 'Security'

- Template as 'Security Users'
- Enter Process Description or retain as is
- Browse and select the Source file that was created in Step 10

Figure 1–34 Upload Security Users Information

The screenshot shows the 'Oracle Merchandising' application window with the 'Upload Data' tab selected. The 'Template Type' is set to 'Security' and the 'Template' is 'Security Users'. The 'Process Description' is 'Security Users - Upd' and the 'Source File' is 'Security Users - upld ods'. An 'Update...' button is next to the source file. At the bottom right, there are 'Upload' and 'Done' buttons.

13. Click the **Upload** button.

Figure 1–35 Upload Security Users Information Complete

The screenshot shows the 'Oracle Merchandising' application window with the 'Upload Data' tab selected. The 'Template Type' is set to 'Security' and the 'Template' is 'Security Users'. The 'Process Description' is 'Security Users - Upd' and the 'Source File' is 'Browse... No file selected.' At the bottom right, there are 'Upload' and 'Done' buttons.

14. Click the **Done** button.
15. View the newly created Security User and Security User Role by downloading the Security Users spreadsheet (Steps 1 - 6).

Figure 1–36 View newly created Security User and Security Role Mapping information

Action	User Sequence	Application	Database User Manager	RMS User	RESA User	REIM User	Allocation User
Update	15001	OIM TEST		Yes	No	No	No

Figure 1–37 View newly created Security User Role mapping information

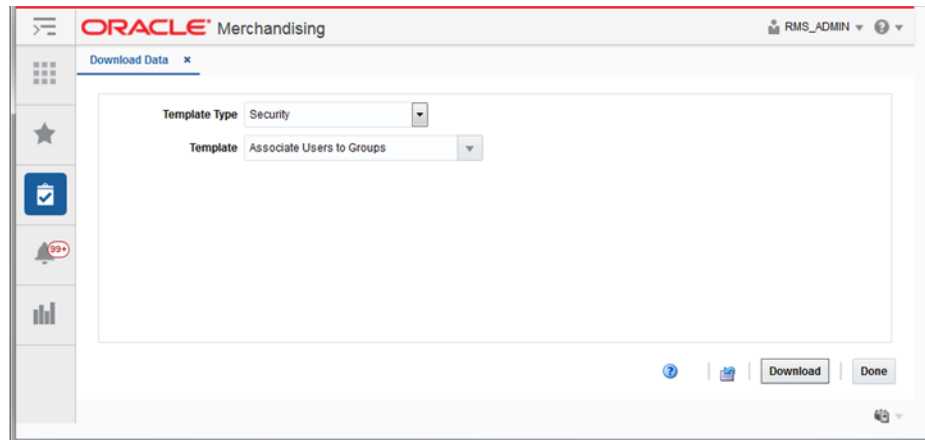
Action	User Sequence	Role
Update	15001	OIM_TEST_ROLE

Note the system generated User Sequence. This Security User (User Sequence) will be mapped to the Security Group.

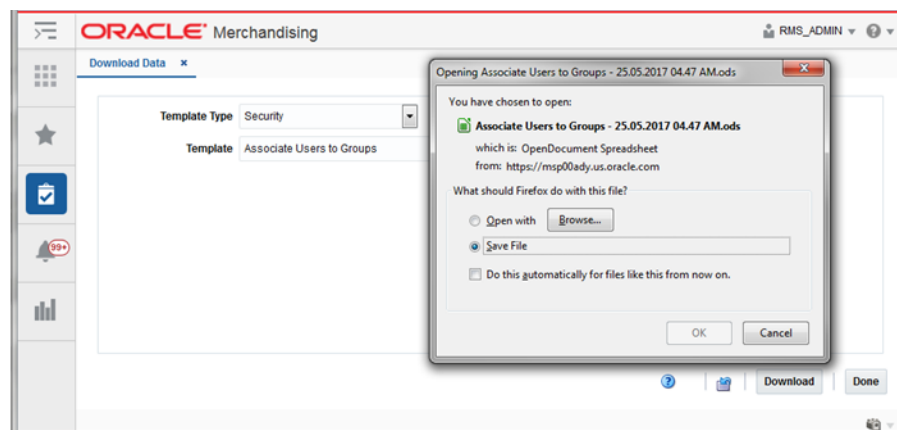
Map Security User with Security Group

The security user must be assigned to a security group. This is achieved by associating the User Sequence assigned to the Application User ID with a Security User Group.

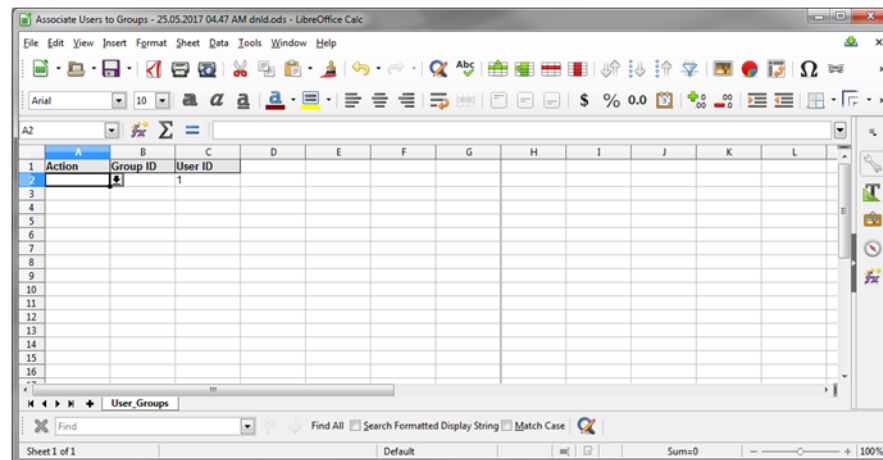
1. Navigate to Foundation Data > Data Loading > Download.
2. In the Download Data screen, select Template Type as 'Security' and Template as 'Associate Users to Groups'.

Figure 1–38 Download Associate User to Groups Template Spreadsheet

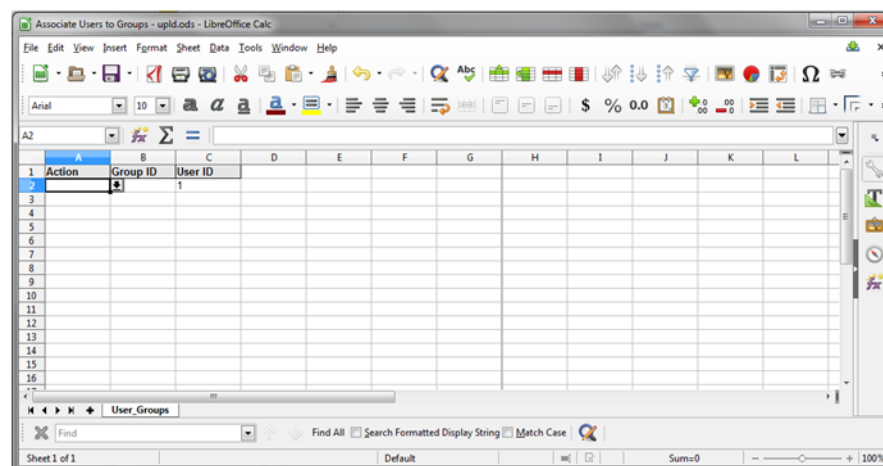
3. Click the **Download** button.
4. Save the file to a local directory location when prompted.

Figure 1–39 Save File

5. Click the **Done** button.
6. Open the downloaded file.

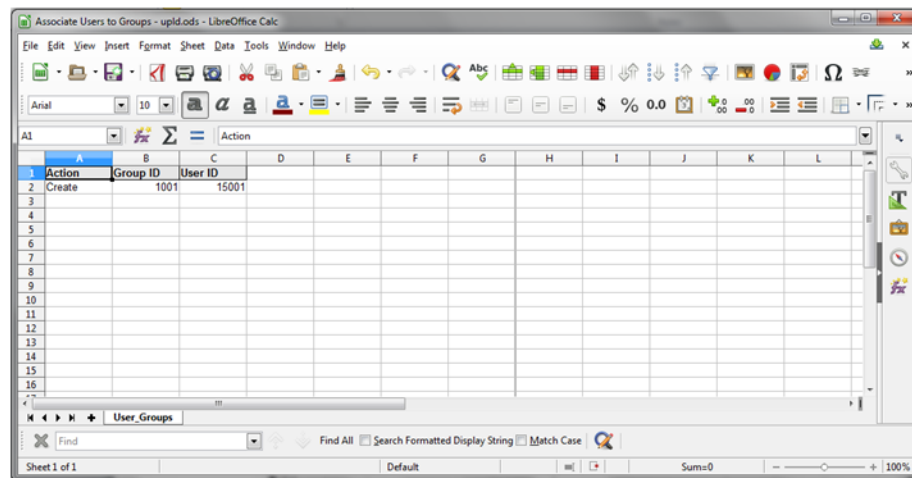
Figure 1–40 Open File

7. Save As < file name>.

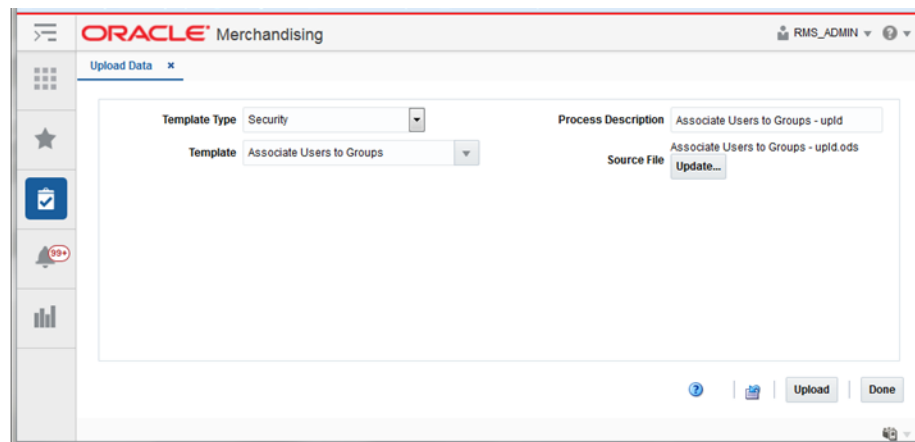
Figure 1–41 Save as <File Name>

8. In the User_Groups tab, enter/select the following:

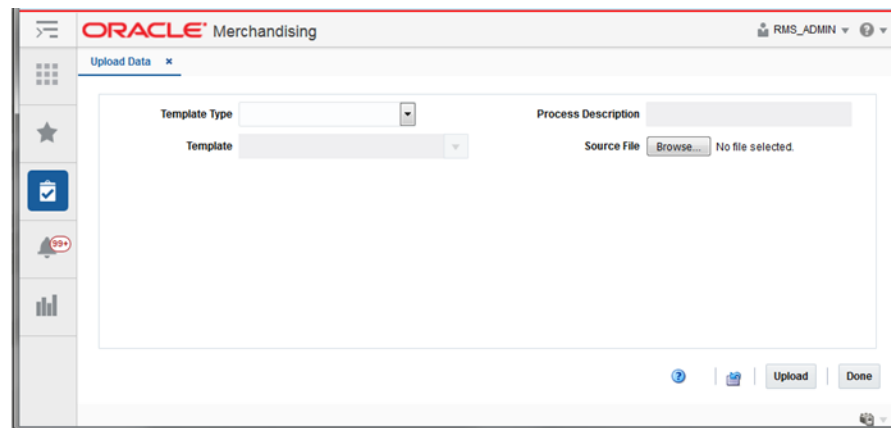
- Action: 'Create'
- Group ID: <Group ID>
- User ID: <User ID>

Figure 1–42 Enter User Groups information

9. Save and Close the file.
10. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
11. In the Upload Data screen, select:
 - Template Type as 'Security'
 - Template as 'Associate Users to Groups'
 - Enter new Process Description or retain as is
 - Browse and select the Source file that was created in Step 9

Figure 1–43 Upload User Groups Information

12. Click the **Upload** button.

Figure 1–44 Upload User Groups Information Complete

13. Click the **Done** button.
14. View the newly created User Groups mapping by downloading the User Groups spreadsheet (Steps 1 - 6).

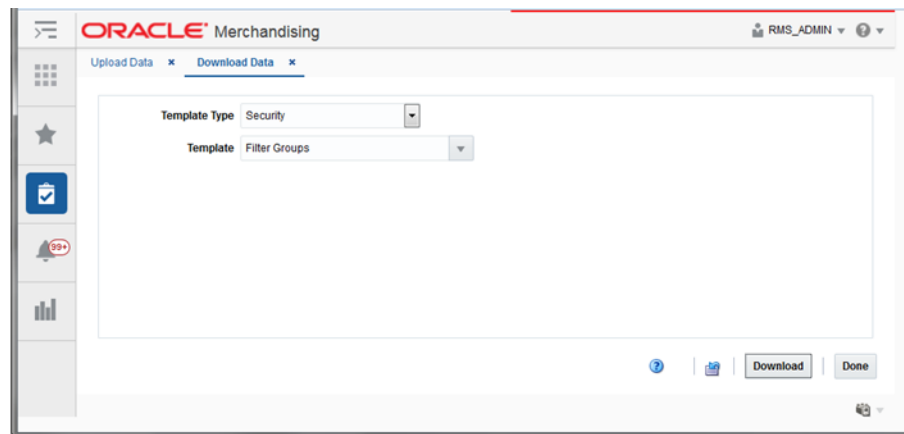
Figure 1–45 View Newly Created User Group Association

A	B	C	D	E	F	G	H	I	J	K	L
1	Action	Group ID	User ID								
2		1001	15001								
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											

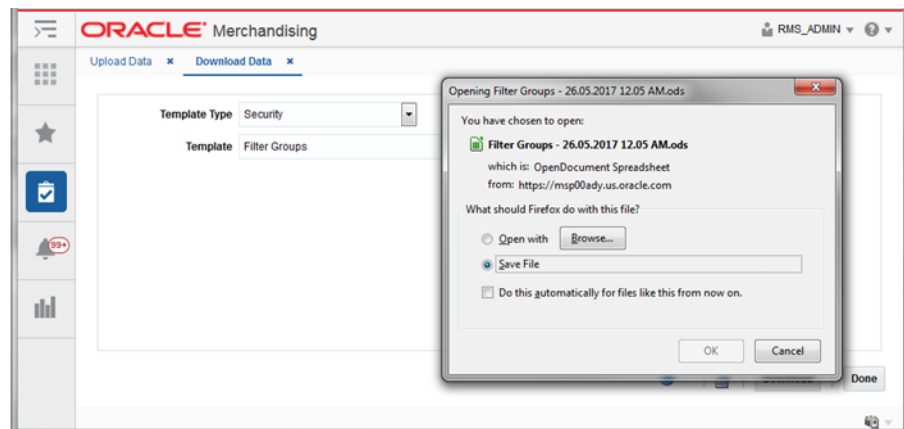
Setup Merchandise Hierarchy LOV Filtering Access Information

The security group can only access the merchandise hierarchies and organization hierarchies assigned to the user through Filter Groups. If a security group is not assigned to any Filter Group then the users in the group are considered 'super users' and will have access to all merchandise hierarchies or all organization hierarchies respectively.

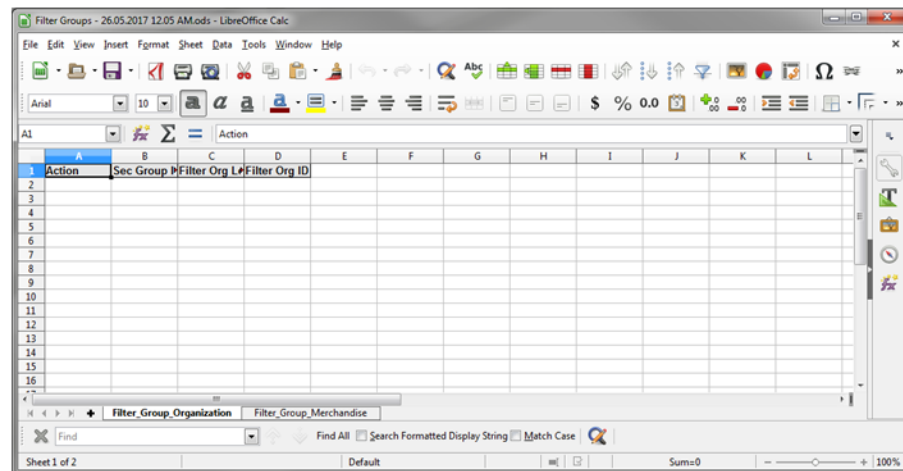
1. Navigate to Foundation Data > Data Loading > Download.
2. In the Download Data screen, select Template Type as 'Security' and Template as 'Associate Users to Groups'.

Figure 1–46 Download Filter Groups Template Spreadsheet

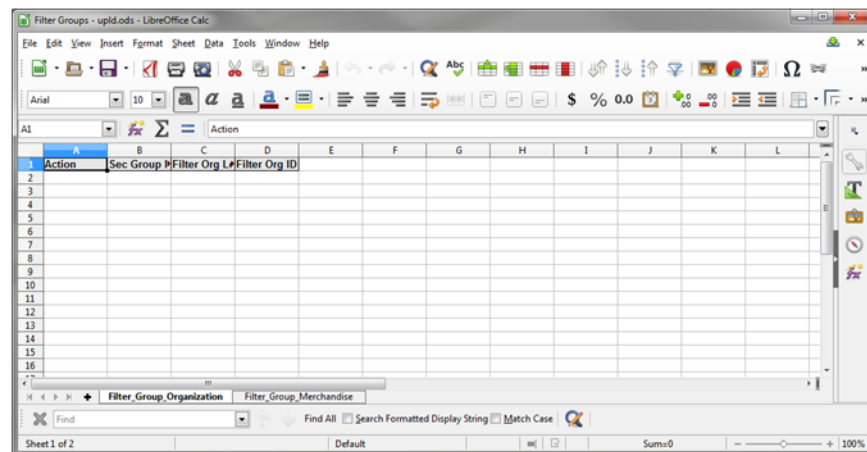
3. Click the **Download** button.
4. Save File to local directory location when prompted.

Figure 1–47 Save File

5. Click the **Done** button.
6. Open the downloaded file.

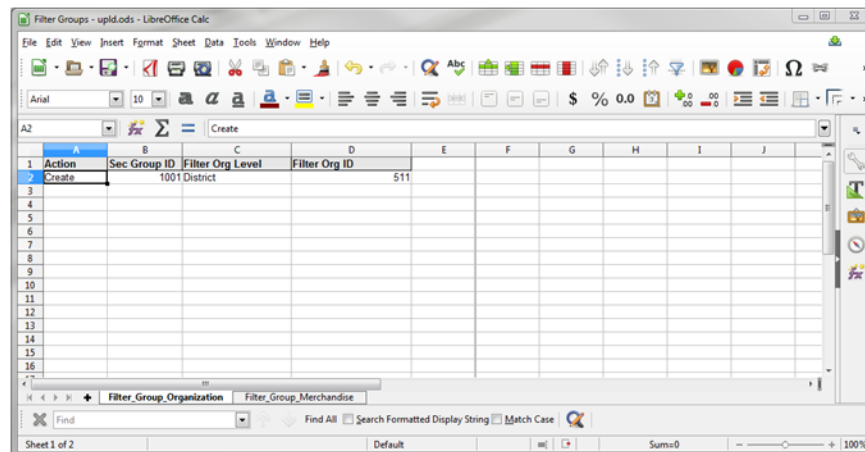
Figure 1–48 Open File

7. Save As < file name>.

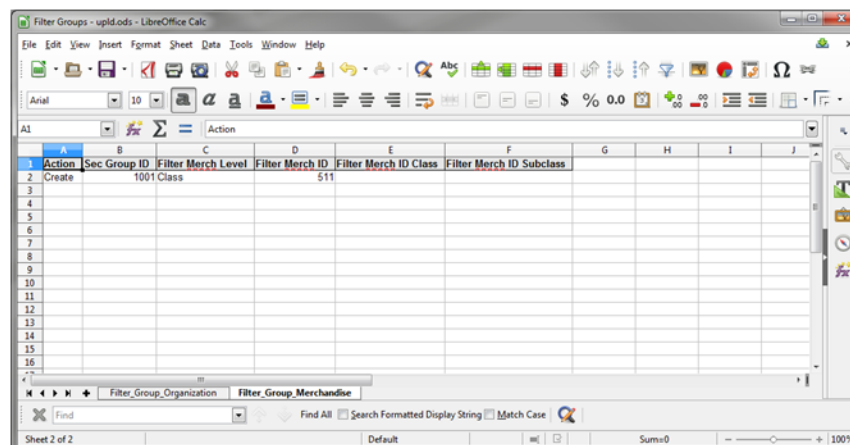
Figure 1–49 Save as <File Name>

8. In the Filter_Group_Organization tab, enter/select the following:

- Action: 'Create'
- Sec Group ID: <User Security group ID>
- Filter Org Level: <Organization hierarchy level>
- Filter Org ID: <ID of the Organization hierarchy level>

Figure 1–50 Enter Filter Group Organization information

9. In the Filter_Group_Merchandise tab, enter/select the following:
 - Action: 'Create'
 - Sec Group ID: <User Security group ID>
 - Filter Merch Level: <Organization hierarchy level>
 - Filter Merch ID: <ID of the Merchandise hierarchy level>
 - Filter Merch ID Class: <Class ID of the Merchandise hierarchy level> (optional depending on the selected Filter Merch Level)
 - Filter Merch ID Subclass: <Subclass ID of the Merchandise hierarchy level> (optional depending on the selected Filter Merch Level)

Figure 1–51 Enter Filter Group Merchandise information

10. Save and close the file.
11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
12. In the Upload Data screen, select:
 - Template Type as 'Security'
 - Template as 'Filter Groups'

- Enter new Process Description or retain as is
- Browse and select the Source file that was created in Step 10

Figure 1–52 Upload Filter Groups Information

The screenshot shows the 'Oracle Merchandising' application window with the 'Upload Data' tab selected. The interface includes a sidebar with navigation icons (home, star, checkmark, notifications, bar chart). The main content area contains the following fields:

- Template Type:** A dropdown menu set to 'Security'.
- Template:** A dropdown menu set to 'Filter Groups'.
- Process Description:** A text field containing 'Filter Groups - upld'.
- Source File:** A text field containing 'Filter Groups - upld.ods'.
- Buttons:** An 'Update...' button is located next to the Source File field. At the bottom right, there are 'Upload' and 'Done' buttons.

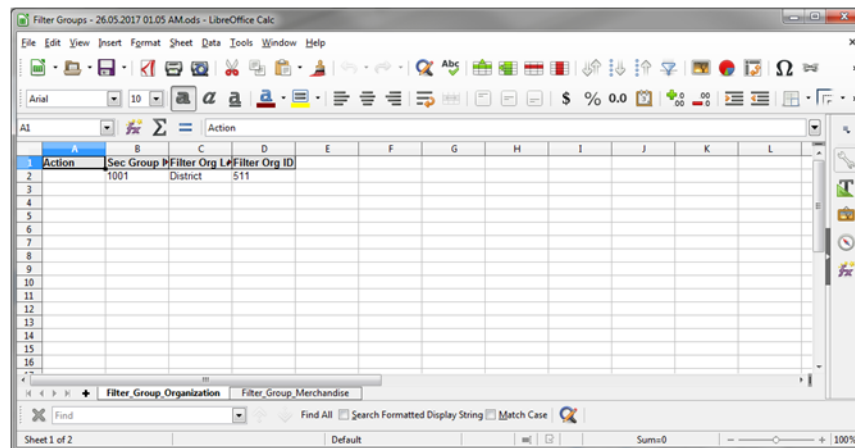
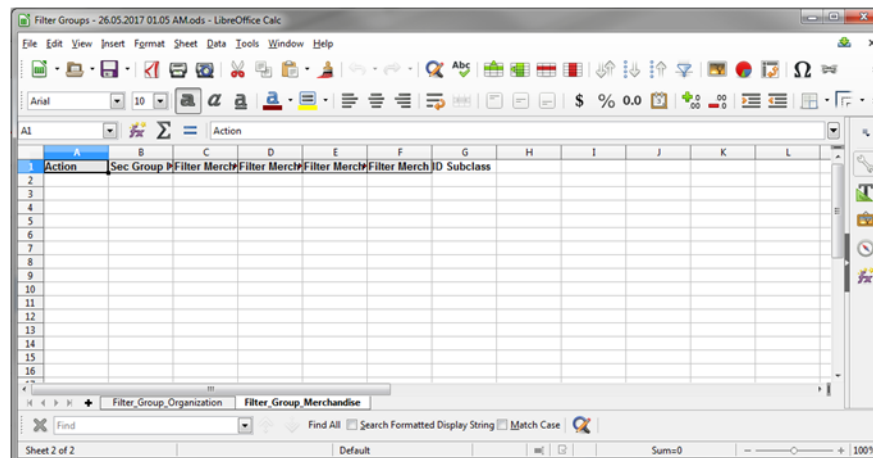
13. Click the **Upload** button.

Figure 1–53 Upload Filter Groups Information Complete

The screenshot shows the 'Oracle Merchandising' application window with the 'Upload Data' tab selected. The interface is similar to Figure 1-52, but with the following changes:

- Template Type:** The dropdown menu is now empty.
- Template:** The dropdown menu is now empty.
- Process Description:** The text field is now empty.
- Source File:** The text field is empty, and a 'Browse...' button is visible next to it. Below the field, it says 'No file selected.'.
- Buttons:** The 'Upload' and 'Done' buttons are still present at the bottom right.

14. Click the **Done** button.
15. View the newly created Filter Groups mapping by downloading the Filter Groups spreadsheet (Steps 1 - 6).

Figure 1–54 View Newly Created Filter Groups**Figure 1–55 Newly Created Filter Groups**

Retail Merchandising Cloud Services Default Enterprise Roles

Retail Merchandising Cloud Services is built with role-based access. Permissions are associated with roles. Assign these roles to the user following the steps in the section, "Assigning Members to a Role" as per your requirement.

The following roles are available for RMS and ReSA:

Table 1–1 Retail Merchandising Cloud Services Default Enterprise Roles

Module	Default Enterprise Roles	Corresponding Application Roles
Merchandising	Application Administrator	RMS Application Administrator
Merchandising	Data Steward	RMS Data Steward
Merchandising	Buyer	Buyer
Merchandising	Inventory Analyst	Inventory Analyst
Merchandising	Inventory Manager	Inventory Manager
Merchandising	Corporate Inventory Control Analyst	Corporate Inventory Control Analyst

Table 1–1 (Cont.) Retail Merchandising Cloud Services Default Enterprise Roles

Module	Default Enterprise Roles	Corresponding Application Roles
Merchandising	Inventory Control Manager	Inventory Control Manager
Merchandising	Sourcing Analyst	Sourcing Analyst
Merchandising	Finance Analyst	Finance Analyst
Merchandising	Supply Chain Analyst	Supply Chain Analyst
Merchandising	Finance Manager	Finance Manager
Sales Audit	Sales Audit Analyst	Sales Audit Analyst
Sales Audit	Sales Audit Manager	Sales Audit Manager
Sales Audit	Application Administrator	RESA Application Administrator
Sales Audit	Finance Manager	Finance Manager
Batch Schedule	Batch Business	Batch Business
Pricing	Application Administrator	Pricing Application Administrator
Pricing	Data Steward	Pricing Data Steward
Pricing	Pricing Analyst	Pricing Analyst
Pricing	Pricing Manager	Pricing Manager
Pricing	Promotion Planner	Promotion Planner
Pricing	Promotion Manager	Promotion Manager
Invoice Matching	Accounts Payable Specialist	Accounts Payable Specialist
Invoice Matching	Finance Manager	Finance Manager
Invoice Matching	Buyer	Buyer
Invoice Matching	Corporate Inventory Control Analyst	Corporate Inventory Control Analyst
Invoice Matching	Application Administrator	ReIM Application Administrator
Invoice Matching	Finance Analyst	Finance Analyst
Invoice Matching	Accounts Payable Manager	Accounts Payable Manager
Invoice Matching	Data Steward	Data Steward
Allocation	Application Administrator	Allocation Application Administrator
Allocation	Allocation Manager	Allocation Manager
Allocation	Allocator	Allocator
Allocation	Buyer	Buyer

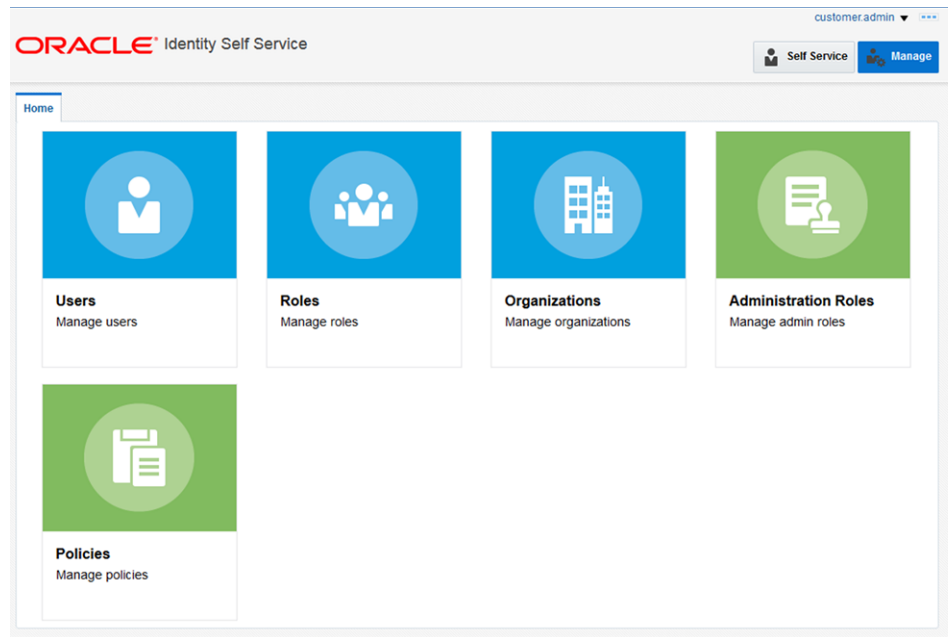
Note: A new DATAPRIV_ADMINISTRATOR_REST_API_ROLE and DATA_PRIVACY_ADMINISTRATOR_JOB was created which are not associated to application users. These should be assigned to the users that invoke ReST services.

Revoking Role Membership

To revoke the membership of a member in a role:

1. Log into the OIM application.
2. Click **Users**.

Figure 1–56 Select Users



3. Click the oim.test user.

Figure 1–57 Select Role to Revoke Users

Home **Users** x

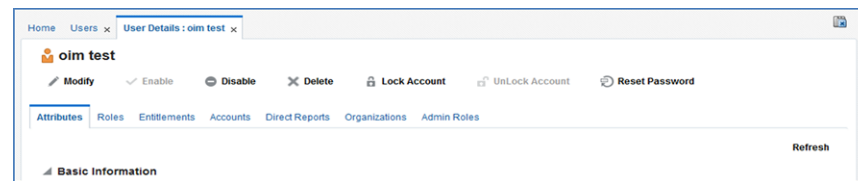
Users

Search

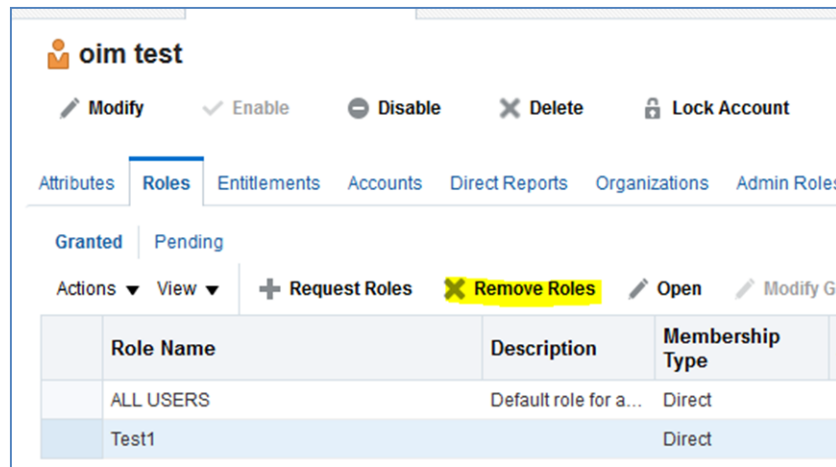
Actions View >> >>

User Login	Display Name	First Name	Last Name	Organization	Telephone Number	E-mail	Identity Status	Account St
CE ADMIN1	ce admin1	ce	admin1	Retail		ce.admin1@ora...	Active	Unlocked
CE ADMIN10	ce admin10	ce	admin10	Retail		ce.admin10@or...	Active	Unlocked
CE ADMIN2	ce admin2	ce	admin2	Retail		ce.admin2@ora...	Active	Unlocked
CE ADMIN3	ce admin3	ce	admin3	Retail		ce.admin3@ora...	Active	Unlocked
CE ADMIN4	ce admin4	ce	admin4	Retail		ce.admin4@ora...	Active	Unlocked
CE ADMIN5	ce admin5	ce	admin5	Retail		ce.admin5@ora...	Active	Unlocked
CE ADMIN6	ce admin6	ce	admin6	Retail		ce.admin6@ora...	Active	Unlocked
CE ADMIN7	ce admin7	ce	admin7	Retail		ce.admin7@ora...	Active	Unlocked
CE ADMIN8	ce admin8	ce	admin8	Retail		ce.admin8@ora...	Active	Unlocked
CE ADMIN9	ce admin9	ce	admin9	Retail		ce.admin9@ora...	Active	Unlocked
CE.TEST	ce test	ce	test	Retail		ce.test@oracle...	Active	Unlocked
CE.TEST3	ce test3	ce	test3	Retail		ce.test3@oracle...	Active	Unlocked
CUSTOMER.AD...	customer admin	customer	admin	Retail			Active	Unlocked
CUSTOMER.AD...	customer admin1	customer	admin1	Retail		customer.admin...	Active	Unlocked
CUSTOMER.AD...	customer admin2	customer	admin2	Retail			Active	Unlocked
OIM.TEST	oim test	oim	test	Retail		oim.test@orac...	Active	Unlocked

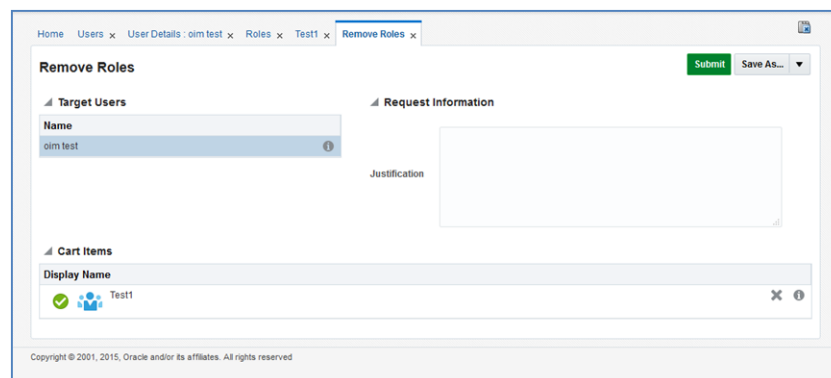
4. Click the Roles tab.

Figure 1–58 Roles Tab

5. Select the Role you want to revoke and click the **Remove Role** button.

Figure 1–59 Remove Roles Button

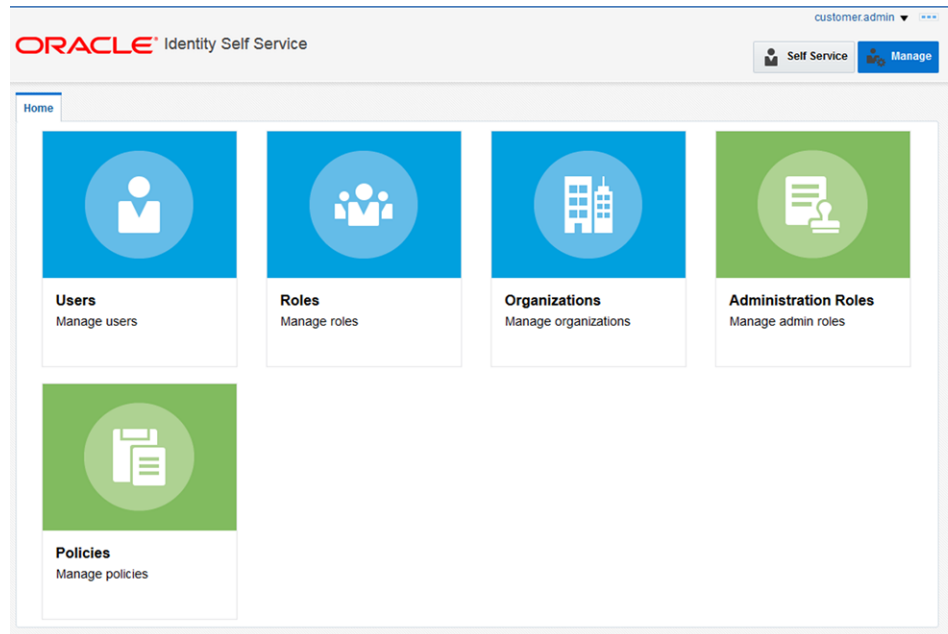
6. In the Remove Roles screen, click **Submit**.

Figure 1–60 Remove Roles Screen

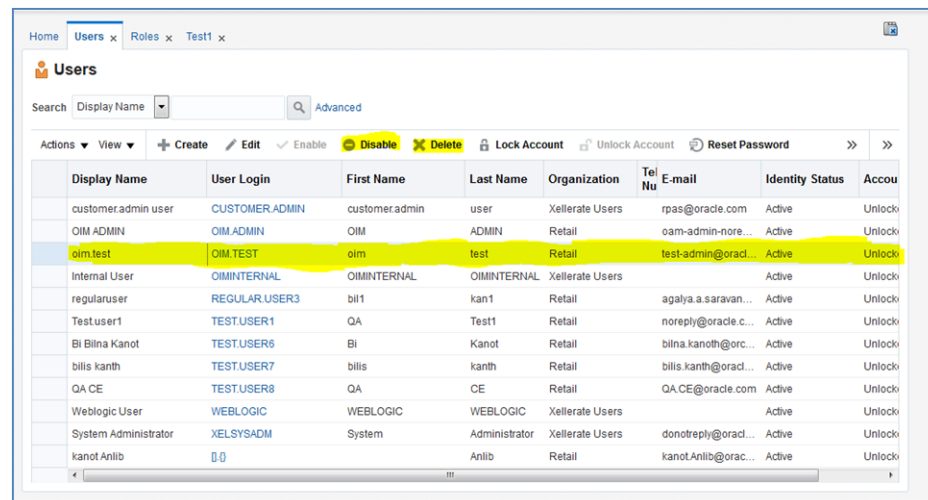
Deleting a User or Disabling User Privileges

To delete or disable a user

1. Log into the OIM application.
2. Under Administration, click **Users**.

Figure 1–61 Select Users

3. Select the user and click **Disable** or **Delete** as necessary.

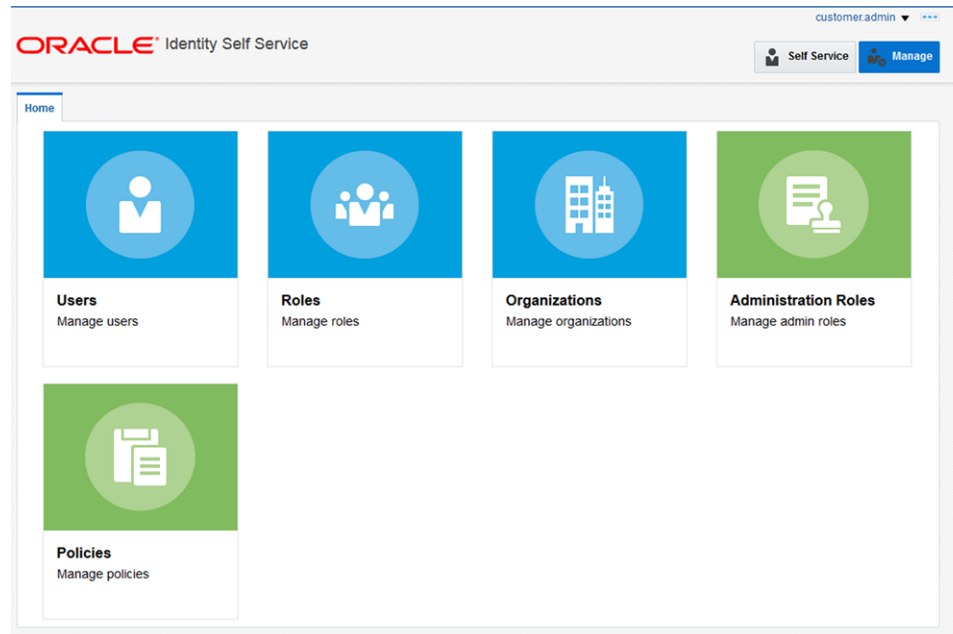
Figure 1–62 Delete and Disable

4. You can also Lock or Unlock a particular user from the same screen if needed.

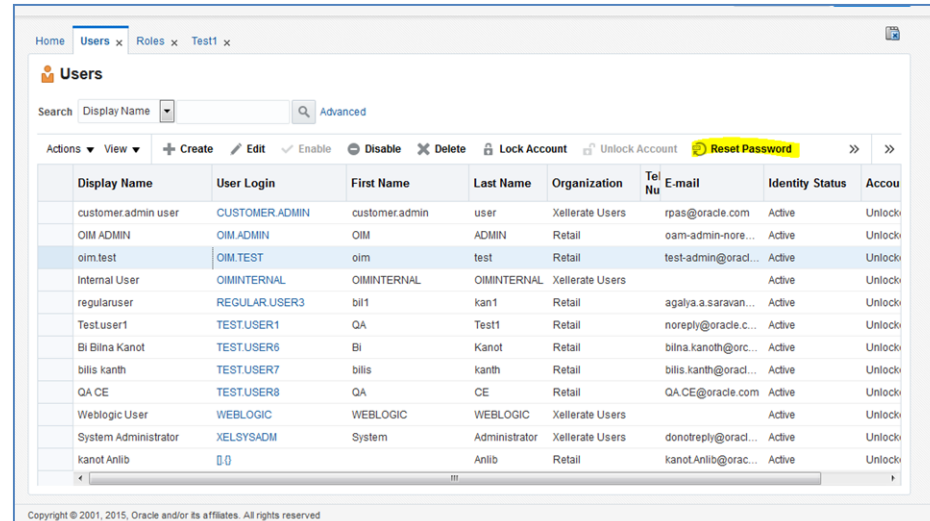
Resetting a User Password

To reset the password of a user:

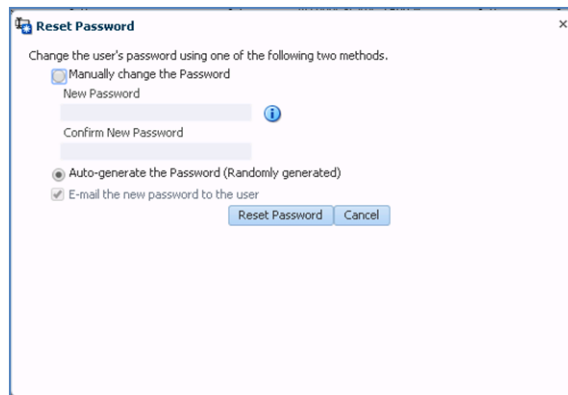
1. Log into the OIM application.
2. Under Administration, click **Users**.

Figure 1–63 Select Users

3. Click the **Search** tab and then select on the User you want to reset the password.
4. Click **Reset Password**.

Figure 1–64 Reset Password Button

5. In the Reset Password screen, make sure Auto-generate the Password is selected and then click **Reset Password**. (The system auto-generates the password and e-mails it to the user.)

Figure 1–65 Reset Password


Reset Password

Change the user's password using one of the following two methods.

☐ Manually change the Password

New Password

Confirm New Password

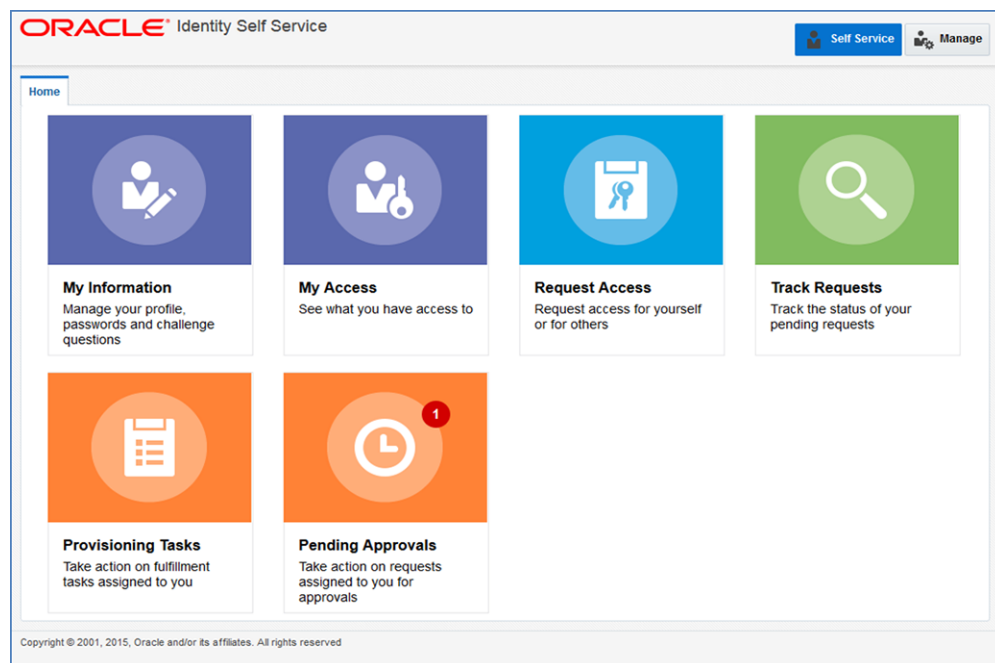
☒ Auto-generate the Password (Randomly generated)

☒ E-mail the new password to the user

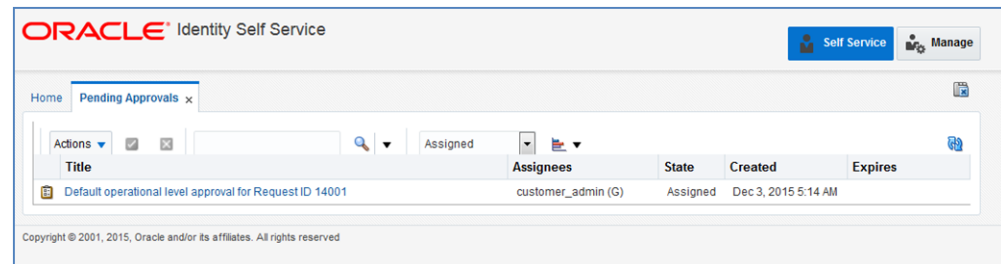
Approve Requests from User

The users can also request for the Roles or revoke those that are available for him to access the RIS Service. Follow these steps to approve the request from the User.

1. Login into OIM Application.
2. Click **Pending Approvals**.

Figure 1–66 Select Pending Approvals

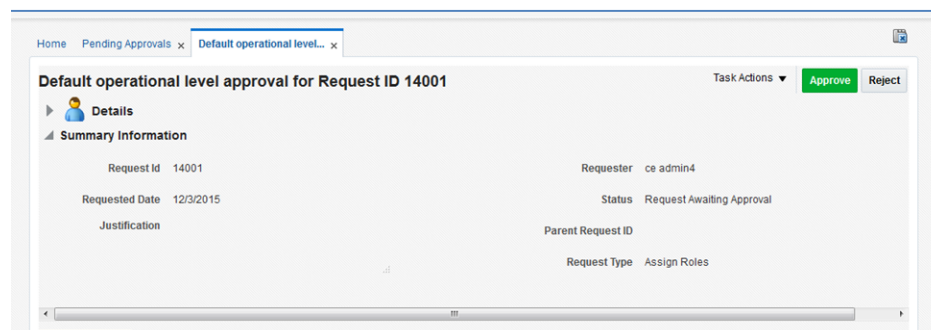
3. Click on the Action that is assigned to you.

Figure 1–67 Pending Approvals Tab

4. Click the **Claim** button.

Figure 1–68 Claim the Pending Approval

5. Click **Approve** or **Reject**.

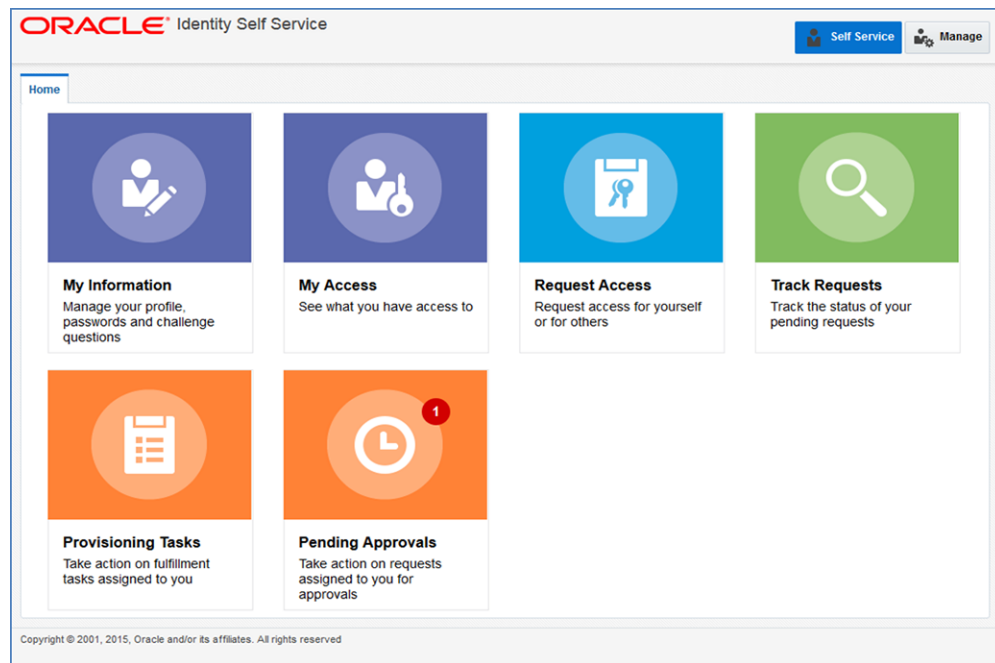
Figure 1–69 Approve Pending Approval

6. The request is complete.

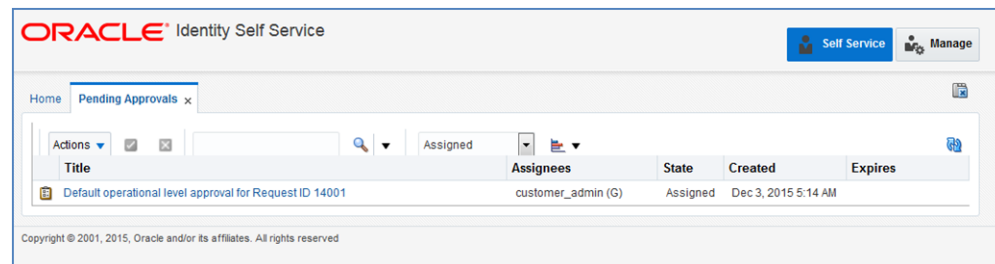
Approve Requests from User for Multiple Roles

Users can also request for the multiple Roles or revoke them if they are available for him to access the RIS Service. Follow these steps to approve the request from the User.

1. Login into OIM Application.
2. Click **Pending Approvals**.

Figure 1–70 Select Pending Approvals

3. Click on the Action that is assigned to you.

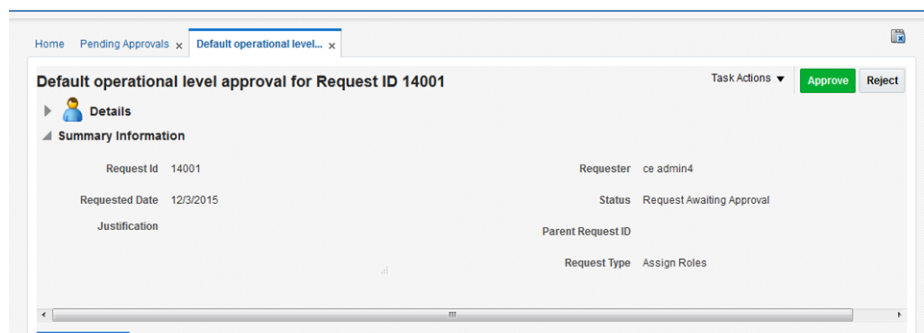
Figure 1–71 Pending Approvals Tab

4. Click the **Claim** button.

Figure 1–72 Claim the Pending Approval

5. Click **Approve** or **Reject**.

Figure 1–73 Approve Pending Approval



6. Once done, if approved, the request is split into multiple requests, one for each role for each user. Approve all of them by following steps 3-5.
7. Once all the requests are approved, all the roles are assigned to users.

Note: The customer administrator can request multiple roles for multiple users. Once this request is made, the customer administrator is required to approve the request using the Approve Requests from User for Multiple Roles process.

Importing a Batch of User Accounts

If you have batch of users that have to be created, the Oracle team can bulk load the users into the OIM Application. When users are bulk loaded their initial password will be set to the current password of a template user. The new users are required to change their password on their first login.

To request the creation of accounts by bulk loading, perform the following steps.

1. Create a CSV file listing all of the users to create (see the example in step 3).
2. Create or identify a user whose password will be used as the initial password for all created users.
3. Open an SR with Oracle support and provide the CSV file and user from steps 1 and 2.

```
#####
filename.csv
#####
#####
USR_LOGIN,USR_FIRST_NAME,USR_LAST_NAME,USR_EMAIL,ORG_NAME
ce.admin1,ce,admin1,ce.admin1@oracle.com,Retail
ce.admin2,ce,admin2,ce.admin2@oracle.com,Retail
ce.admin3,ce,admin3,ce.admin3@oracle.com,Retail
ce.admin4,ce,admin4,ce.admin4@oracle.com,Retail
ce.admin5,ce,admin5,ce.admin5@oracle.com,Retail
ce.admin6,ce,admin6,ce.admin6@oracle.com,Retail
ce.admin7,ce,admin7,ce.admin7@oracle.com,Retail
ce.admin8,ce,admin8,ce.admin8@oracle.com,Retail
ce.admin9,ce,admin9,ce.admin9@oracle.com,Retail
ce.admin10,ce,admin10,ce.admin10@oracle.com,Retail
#####
```

Bulk Role Membership Update (Optional)

If you have quite a few users that have roles to be assigned to, the Oracle team can bulk update the role membership into the OIM Application.

To update the membership of the by bulk update, perform the following steps.

1. Create CSV file with the user role mapping. Please note that the user name must be in upper case format (see the example in step 3).
2. Open an SR with Oracle support and provide the CSV file and user from step 1.

```
#####
role.csv
#####
#####
UGP_NAME,USR_LOGIN
Role1,CE.ADMIN1
Role2,CE.ADMIN1
Role1,CE.ADMIN2
Role3,CE.ADMIN3
Role4,CE.ADMIN4
Role5,CE.ADMIN5
Role6,CE.ADMIN6
Role7,CE.ADMIN7
Role8,CE.ADMIN8
Role2,CE.ADMIN8
Role2,CE.ADMIN9
#####
```

Note: If you want more than one role attached to a particular user, add one more row with the role that you want the user to have and the user name. Refer to the CE.ADMIN1 in above table for example.

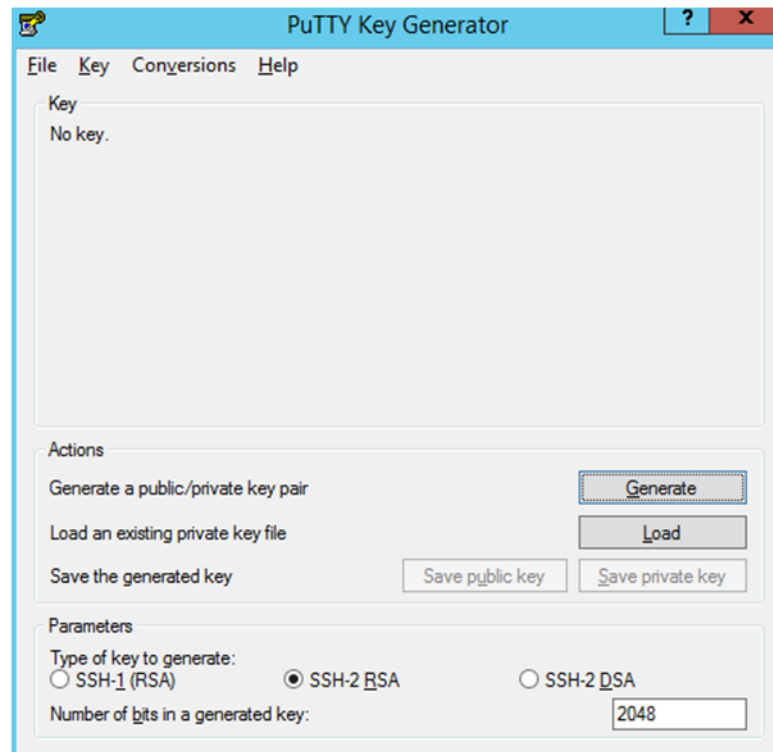
Nightly Batch File Uploads

The following is the file upload process. The Private/Public Keys must be generated and the public Key must be associated with your SFTP Account for the file uploads. The [Adding Authorized Keys](#) section describes the step-by-step method to generate the Keys (2048 bit RSA Keys).

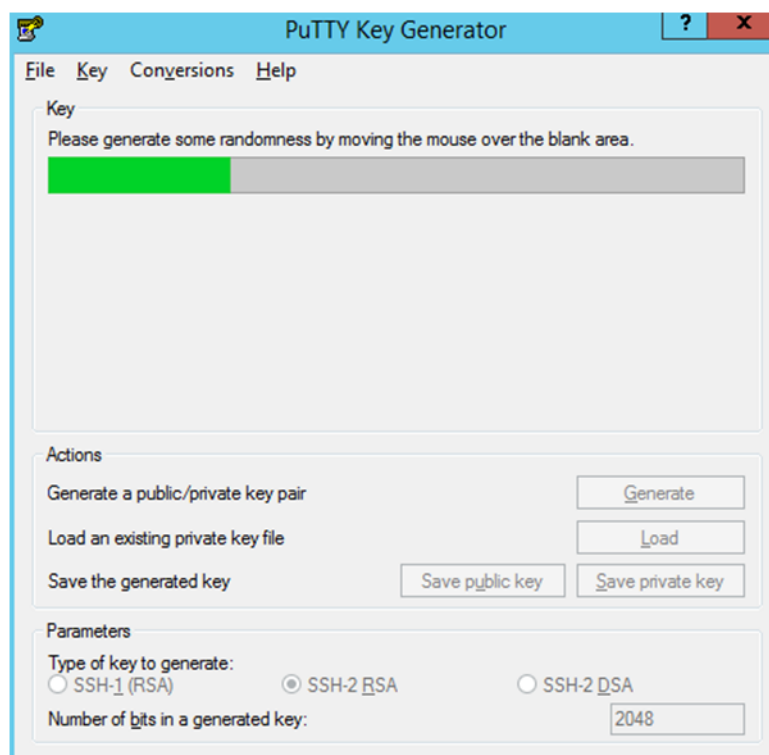
Adding Authorized Keys

Use this process to generate a 2048 bit RSA key and add the same to the SFTP server. With Windows, use the WinSCP tool or with Linux, use ssh-keygen.

1. Launch WinSCP and select Tools -> Run PuttyGen.
2. Select *SSH-2 RSA* for the type of key to generate and enter *2048* for the number of bits in a generated key field and click **Generate**.

Figure 1–74 Key Generator

3. Move the mouse over the blank space in the window until the key is generated.

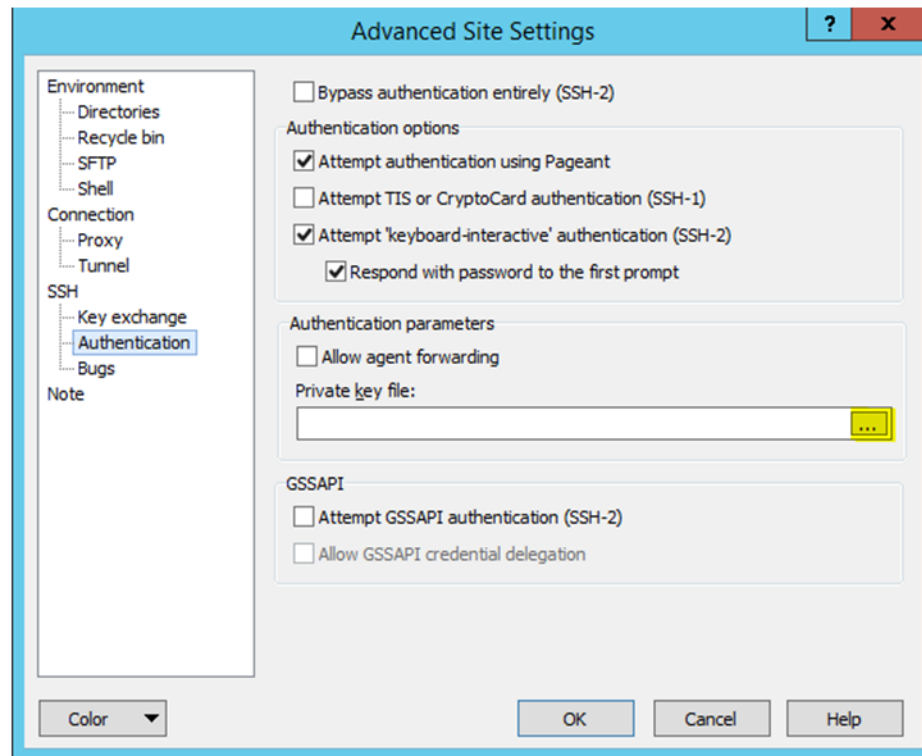
Figure 1–75 Key Generator Progress

4. Once the key is generated, click **Save public key** to save the public key to a file.
5. Click **Save private key** to save the Private key to a file. Confirm to save it with or without a passphrase.
6. Open an SR with Oracle Support, to associate the Public half of the Key with your SFTP account (attach the Key with the SR).

Steps – Login to WinSCP

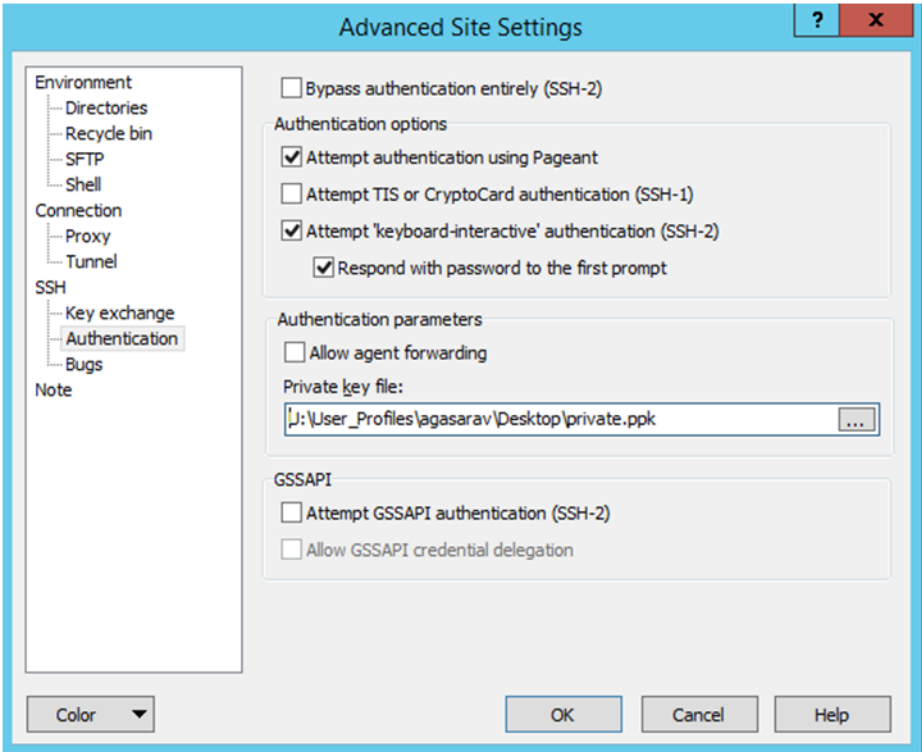
These upload steps use the private key generated in section, Adding Authorized Keys.

1. Launch WinSCP and connect to <SFTP Server> using port 22.
2. Enter the username and then click **Advanced**.
3. Click **Authentication**.
4. In the Private Key File field, click **Browse** and select the private key created in the section, Adding Authorized Keys.

Figure 1–76 Advanced Site Settings Dialog

5. After loading the private key file, click **OK**.

Figure 1–77 Private Key File Loaded



6. Click **Login**. The window does not prompt for a password and logs into the SFTP server. Provide a passphrase if one has been set up.

Note: Login can only be performed using the authorized keys. Login with username / password is not supported.

Steps to Upload the Batch File

Login to the WinSCP by Following the [Steps – Login to WinSCP](#) section.

1. Transfer the file to be copied (e.g., test) to /<SFTP User>.

Figure 1–78 <SFTP User> Directory

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017 4:36:54 PM	..	2/8/2017 2:49:59 PM
test.complete	COMPLETE File	11/28/2016 9:43:43 PM	COMMAND	2/9/2017 4:36:48 PM
test	File	11/28/2016 9:43:43 PM	COMPLETE	11/28/2016 9:43:43 PM
			test	11/28/2016 9:43:43 PM

2. Transfer an empty file <filename>.complete (eg: test.complete) to the directory /<SFTP User>.

Figure 1–79 Transferring Empty File

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017	..	2/8/2017 2:49:59 PM
test.complete	COMPLETE File	11/28/2016	COMMAND	2/9/2017 4:36:48 PM
test	File	11/28/2016	COMPLETE	11/28/2016 9:43:43 PM
			test	11/28/2016 9:43:43 PM
			test.complete	11/28/2016 9:43:43 PM

3. If multiple files have to be transferred, copy all the files to /<SFTP_user>.

Figure 1–80 Transferring Multiple Files

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017	..	2/8/2017 2:49:59 PM
test	File	11/28/2016	COMMAND	2/9/2017 4:36:48 PM
test1	File	11/28/2016	COMPLETE	11/28/2016 9:43:43 PM
test2	File	11/28/2016	test	11/28/2016 9:43:43 PM
			test1	11/28/2016 9:43:43 PM
			test2	11/28/2016 9:43:43 PM

4. Transfer all the corresponding <filename>.complete files to the /<SFTP_user> directory for the transfer to complete.

Figure 1–81 Transferring .complete Files

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017	..	2/8/2017 2:49:59 PM
test.complete	COMPLETE File	11/28/2016	COMMAND	2/9/2017 4:36:48 PM
test1.complete	COMPLETE File	11/28/2016	COMPLETE	11/28/2016 9:43:43 PM
test2.complete	COMPLETE File	11/28/2016	test	11/28/2016 9:43:43 PM
			test.complete	11/28/2016 9:43:43 PM
			test1	11/28/2016 9:43:43 PM
			test1.complete	11/28/2016 9:43:43 PM
			test2	11/28/2016 9:43:43 PM
			test2.complete	11/28/2016 9:43:43 PM

Export File Downloads

Login to the WinSCP by following the [Steps – Login to WinSCP](#) section. The following is the download file process.

1. Change the directory to /<SFTP User>/EXPORT.
2. Download all data files.

