Oracle DataRaker Cloud Service

User Provisioning Guide

E97587-01

Release 18.1.3 / 18.1 HF3

Last Updated: June 11, 2018

Oracle Utilities Oracle DataRaker Cloud Service User Provisioning Guide

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.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Contents

Introduction 1

Dependencies 1

Provisioning End Users in Oracle Identity Manager 1

Logging On to Oracle Identity Manager 2

Verifying Business Application Access 2

Verifying Subscriber User Organization Access 2

Managing Users in Oracle Identity Manager 3

Provisioning Oracle Identity Manager Accounts 4

End User Provisioning Tasks in Oracle DataRaker 5

Locating Users in Oracle DataRaker 5

Assigning Groups and Roles in Oracle DataRaker 6

User Access Auditing and Reporting 8

Introduction

This guide provides instructions for creating and provisioning end users for the Oracle DataRaker Cloud Service (ODR). ODR is an online, utility-facing analytics engine that turns smart gird data into actionable insights for electric, gas, and water utilities. It is designed to evolve with the utility and solve problems spanning business areas, such as including distribution planning, meter and grid operations, energy efficiency, demand response, customer service, and more.

User provisioning for ODR is completed in two parts: creating users in Oracle Identity Manager (OIM) so they appear in the ODR user list, and assigning users ODR groups and roles that determine their ODR user features within the ODR user interface. Only users with OIM Administrator *and* ODR Administrator privileges can add and configure users in OIM and ODR. Contact your Oracle Cloud Engineering Representative to request administrative privileges.

This guide does not provide in depth information about OIM or ODR functionality. See the *Oracle Fusion Middleware Oracle Identity Management Guide* (https://docs.oracle.com/en/middleware/) and the *Oracle DataRaker User Guide* (https://docs.oracle.com/cd/E72219_01/documentation.html) for more information.

Dependencies

The following prerequisites must be met before users can be created and provisioned in ODR:

- The Security Administrator is created and provisioned to all instances of the business applications within the subscription as part of the post-provisioning steps.
- The authorized users assigned user management tasks have been provided with the following:
  - The unique User Name and Password for the instance of OIM. The user will be prompted to change the password and complete security questions the first time they log in to OIM.
  - The URL of OIM self-service. The URL format is **http://<host>/identity**.

Provisioning End Users in Oracle Identity Manager

In order for a user to appear in the ODR user interface, you must first create and configure them in OIM.

Logging On to Oracle Identity Manager

To log on to Oracle Identity Manager:

1. Navigate to the URL provided by Oracle, and then log on using your credentials. The first time you log on to OIM, you must use the credentials provided by Oracle.
2. If logging on to OIM for the first time, follow the prompts to enter and confirm a new password, and set security questions.

Verifying Business Application Access

As Security Administrator, you will need access to the business applications for verification purposes. Business Application Access is determined by the cisusers role in OIM.

To verify business application access:

1. From the **Identity Self-Service** home page, click **Self Service** button, and then click **My Access**.
2. Review your assigned Roles, Accounts, and Admin Roles.
3. If the cisusers role is not assigned, request the cisusers role and provision yourself to all environments.

See "Provisioning Oracle Identity Manager Accounts" on page 4.

Verifying Subscriber User Organization Access

User organization access in OIM determines which user groups and roles options will be available when you set up user access in the product interface.

To verify access to the Subscriber User organization:

1. From the **Identity Self-Service** home page, click the **Manage** button to open the **Management** home page, and then click **Organizations**.
2. Verify that **Subscriber Users** is the only listed available organization, and then click **Subscriber Users** to load the organizations.
3. Click the**Available Roles**tab and verify that the following roles are listed for the **Subscriber User** entry:
   - cisusers
   - Integration Admin

- ExternalIntegrationUsers

4. Click the **Available Accounts** tab and verify that the **Accounts List** includes entries for all instances of the business application that are included in the subscription.
   Each account corresponds to a target environment. The Account name includes the product abbreviation (for example, ODR for Oracle DataRaker) and an indicator of the environment type such as Development, Test or Production.

Note: A typical subscription includes one production environment and one or more Development and Test environment. The number of environments depends on specific customer requirements and may include multiple Development or Test instances.

Managing Users in Oracle Identity Manager

Creating New Users in Oracle Identity Manager

Users must be created in OIM to appear in ODR.

To create and configure a new user:

1. Open the **Identity Self-Service** page, and then click the **Manage** button, then click the **Users** tab.
2. Click the **Create** button and complete the following fields:
   - **First Name**: (Recommended for personal accounts) The first name of the user you are creating.
   - **Last Name**: (Required) The last name of the user you are creating.
   - **User Login**: (Required) A unique user name not exceeding eight characters.
   - **Email**: (Required for personal accounts) The user email address. This address is used by OIM for event notifications such as password expiration and other user-related events.
   - **User Type**: (Required) Select any value. This field is required by OIM but has no impact on user attributes in the target application.
   - **Organization**: (Required) Select **Subscribe Users**.
   - **Password**: The administrator creates a one-time use password. The user will be prompted to reset the password and set the challenge questions/answers when logging in for the first time.
3. Click the **Submit** button.
4. Return to the **Users** tab, then click **Refresh**. Verify that the user appears in the list of users and that the user status settings are:

- **Identity Status**: Active
- **Active Account Status**: Unlocked

Modifying an Existing User in Oracle Identity Manager

Once a user exists in OIM, the user record can be modified from the **Users** screen.

To modify an existing user:

1. Highlight the **User Login** in from the Users table, and then click **Edit** to open the user record.
2. Edit the user record attributes as necessary.
   Note: The password is not available for editing.
3. Click **Submit** to save the changes.

Provisioning Oracle Identity Manager Accounts

Provisioning allows a user to access the connected environments. Use the following procedure to provision accounts to ODR users.

To provision OIM accounts:

1. Select the user role from the Users table, and then click **Open** to open the **User Details**.
2. Select the **Accounts** tab, and then click the **Request Accounts** button or click the **Actions** drop-down and select **Request**. A list of **Application Instances** is displayed. Application Instances represent the connection between OIM and the target application included in the subscription.
3. Click the **Add to Cart** button to add a specific Application Instance to the cart, and then click **Next**.
4. Review the request.
5. (Optional) Complete the justification field.
6. If applicable, set an effective start and end date.
7. Click **Update**, and then click **Submit**.
8. Refresh the **Users** tab and verify that the newly created and provisioned user is listed with the following status settings:
   - **Identity Status**: Active
   - **Active Account Status**: Unlocked

Note: ODR uses an OIM resource to link the user profile to the ODR database. Roles, Proxies, Direct Reports, and Requests are not applicable.

End User Provisioning Tasks in Oracle DataRaker

Once a user has been created in OIM and appears in the ODR user list, you must configure and assign the user to ODR groups and roles. Groups and roles determine the user features and functionality available to each user.

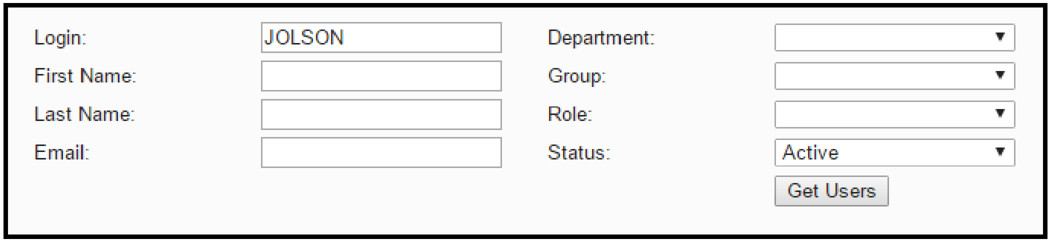
Locating Users in Oracle DataRaker

Once a user has been created in OIM, it will appear in the ODR user list. See "Provisioning End Users in Oracle Identity Manager" on page 1.

Note: You need to have customer administration rights to complete this task. If you do not have access to the **Administer** menu, contact your Oracle Cloud Engineering Representative for support.

To locate a user:

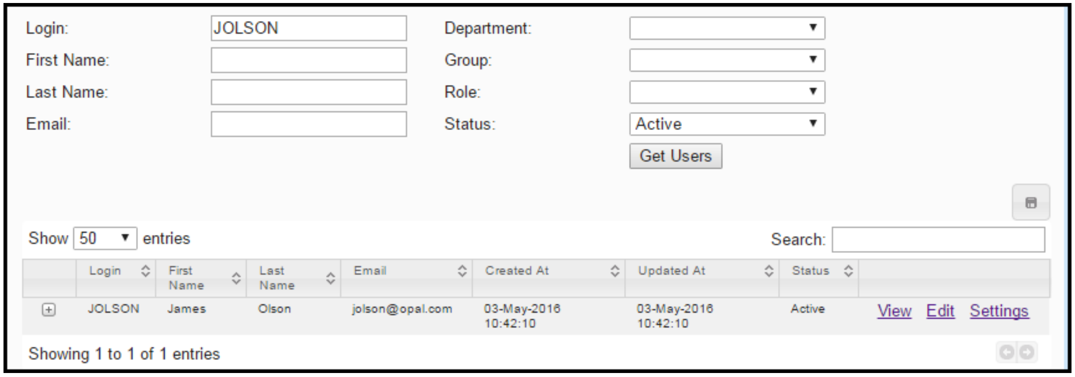
1. Log in to ODR.
2. Select **Administer > Security>Users** to navigate to the **Administer Users** page.
3. Search for the user you created in OIM by completing one of the user information fields and then clicking the **Get Users** button.



Login:	JOLSON	Department:	
First Name:		Group:	
Last Name:		Role:	
Email:		Status:	Active
			Get Users

You may search for a user by any data entered when creating the user.
The data table will return with the user information and links that allow you to assign their user environment. See the *Oracle DataRaker User Guide* (https://docs.oracle.com/cd/E72219_01/documentation.html) for additional information about the **Administer User** page.

4. Click the **Edit** link located in the user row to open the **Manage Users** dialog box. The **Manage Users** dialog box allows you to modify group and role permissions.



Login:	JOLSON	Department:	
First Name:		Group:	
Last Name:		Role:	
Email:		Status:	Active

Get Users

Show 50 entries

Search:

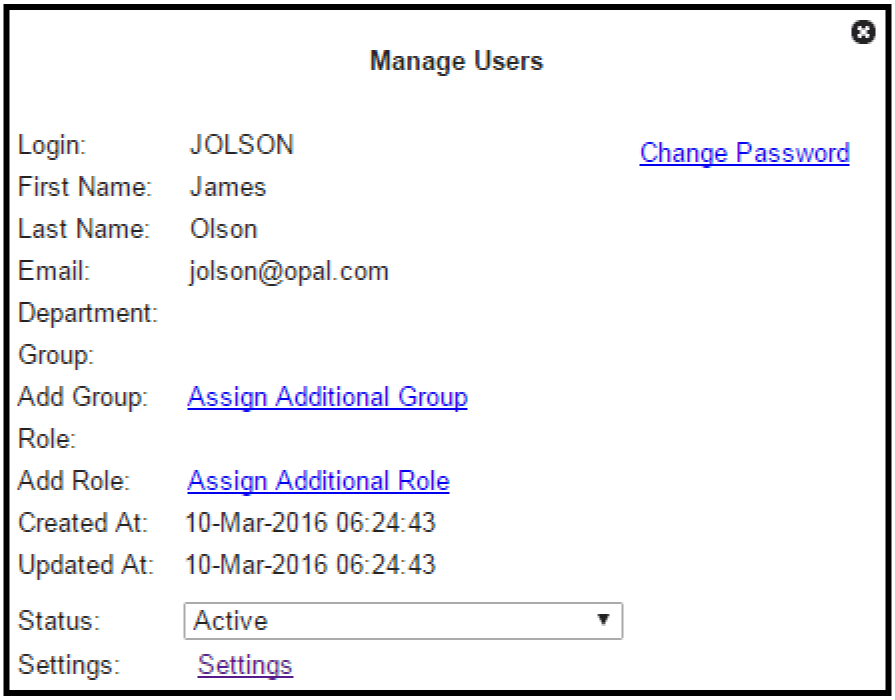
	Login	First Name	Last Name	Email	Created At	Updated At	Status	
⊞	JOLSON	James	Olson	jolson@opal.com	03-May-2016 10:42:10	03-May-2016 10:42:10	Active	View Edit Settings

Showing 1 to 1 of 1 entries

Assigning Groups and Roles in Oracle DataRaker

User environment access is managed through the **Add Group** and **Add Role** functions located in the **Mange Users** pane.

- **Add Group**: Determines general user interface characteristics (for example, the menus that are displayed) and, consequently, which pages are accessible to the user and sets of users.
- **Add Role**: Assigns user roles and determines the features that are available on the pages made available by the user's group privileges.



Manage Users

Login:	JOLSON
First Name:	James
Last Name:	Olson
Email:	jolson@opal.com
Department:	
Group:	
Add Group:	Assign Additional Group
Role:	
Add Role:	Assign Additional Role
Created At:	10-Mar-2016 06:24:43
Updated At:	10-Mar-2016 06:24:43
Status:	Active
Settings:	Settings

Change Password

Roles are associated with modules. Assigning a role automatically associates the user to a module. The following table provides an example of possible user role to module associations. See the *Oracle DataRaker User Guide* (https://docs.oracle.com/cd/E72219_01/documentation.html) for more information.

Module	Role
Meter to Bill	AMI Deployment
	Billing
	Meter Operations
	Safety
Revenue Protection	Revenue Protection
Distribution Planning and Operations	Distribution Planning
Demand Response and Energy Efficiency	Demand Response
	Energy Efficiency

Most end users have access to environments with Explore and Export functionality based on their group assignment. The features available for the user on the **Explore** and **Export** pages are determined by their role. For example, a user with a Billing role in the **Meter to Bill** module has different algorithms and panels on the **Explore** page than a user assigned to the Distribution Planning role in the **Distribution Planning and Operations** module.

Note: The user interface features defined for groups and roles are determined by licensing and implementation. They are not configurable by the customer.

Assigning and Removing User Group Permissions

The Group options in this section are examples only. Your environment may have different group types or group names.

Assigning User Group Permissions

To assign a user to a group:

1. Locate the user in ODR and open the **Manage User** dialog box for the user. See "Locating Users in Oracle DataRaker" on page 5.
2. Click **Assign Additional Group**.
3. Select the appropriate group from the **Add Group** drop-down, and then click **Save**. The **Manage Users** dialog box will update the **Group** field with the assigned group.
4. If a user needs permissions for multiple groups, repeat the previous steps for each additional group.

5. Click **Cancel** or any area outside of the dialog box to close the dialog box.

Removing User Group Permissions

To remove group assignments:

1. Open the **Manage User** dialog box for the user. See "Locating Users in Oracle DataRaker" on page 5.
2. Click the **Remove** link next to the group name you want to remove.

Assigning User Role Permissions

Users must be assigned roles in order to access the environment. Once assigned roles, a user will be able to choose from the modules that correspond to their assigned roles.

To assign user Role permissions:

1. Open the **Manage User** dialog box for the user. See "Locating Users in Oracle DataRaker" on page 5.
2. Click **Assign Additional Role**. The dialog will update with a drop-down list of the available roles based on the modules licensed to the customer.
3. Select the appropriate role from the list and then click **Save**. The **Manage Users** dialog box will update the **Role** field with the newly assigned role.
4. If the user needs permissions for multiple roles, repeat the steps for each additional role.
5. Click **Cancel** or any area outside of the dialog box to close the dialog box.

Removing User Role Permissions

To remove user role permissions:

1. Open the **Manage User** dialog box for the user. See "Locating Users in Oracle DataRaker" on page 5.
2. Click the **Remove** link next to the role.

User Access Auditing and Reporting

OIM provides a powerful audit engine to collect extensive data for audit and compliance purposes. The audit functionality is used to capture, archive, and view entity and transactional data for compliance monitoring and IT-centric processes and forensic auditing. The collected information is then available to a limited-use version of Oracle Business

Intelligence (BI) Publisher, which is Oracle's primary reporting tool for authoring, managing, and delivering highly formatted documents.

The auditing functionality must be enabled by Oracle Cloud Engineering for your environment. For information on running Oracle BI Publisher reports, see the "Running Reports" section of the *Oracle® Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* guide.

OIM implementation of Oracle BI Publisher reports provides the following features:

- Highly formatted and professional quality reports with pagination and headers/footers.
- PDF, Microsoft Word, and HTML output of reports.
- Capability to develop your own custom reports against the OIM repository (read-only repository access).

For the auditing data that is available and a list of the standard reports that are provided, see the "Configuring Auditing" and the "Using Reporting Features" sections of the *Oracle Fusion Middleware Administering Oracle Identity Manager* guide (https://docs.oracle.com/cd/E52734_01/oim/docs.htm).