Oracle Utilities Cloud Services

End User Provisioning Guide

Release 18.1

E96480-01

May 2018

ORACLE

Oracle Utilities Cloud Services Release 18.1 End User Provisioning Guide

Copyright © 2016, 2018 Oracle and/or its affiliates. All rights reserved.

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.

Contents

Chapter 1

Overview 1-1

About This Book 1-2

End User Provisioning Tasks and Account Types By Product 1-3

Chapter 2

Oracle Utilities Cloud Service End User Provisioning 2-1

Introduction 2-2

Prerequisites 2-2

Logging into Oracle Identity Management for the First Time 2-2

Verifying Subscriber User Organization Access 2-4

User Management Procedures 2-6

Creating New Users 2-6

Provisioning Users 2-9

Verifying User Access 2-16

Resetting a Password 2-16

Disabling a User 2-17

Deleting a User 2-18

Accounts to Create 2-19

Pre-Defined Roles 2-19

Available Accounts 2-19

Cloud Service Foundation Accounts 2-20

Integration Accounts 2-20

Personal Accounts 2-21

Chapter 3

Using Federated Single Sign-On 3-1

Adding Oracle Utilities and Oracle DataRaker Application Authorization 3-2

User Record is Created in Oracle Identity Management 3-2

User Record is Not Created in Oracle Identity Management 3-2

Supporting Role-based Authorization 3-2

Chapter 4

Oracle DataRaker End User Provisioning Tasks 4-1

Locating Provisioned Users in Oracle DataRaker 4-2

Assigning Groups and Roles in Oracle DataRaker 4-3

Assigning and Removing User Group Permissions 4-3

Chapter 5

Meter Solution Cloud Service Itron Integration Tasks 5-1

Enabling Itron Integration 5-2

Creating an Integration Account 5-2

Creating an X.509 Certificate 5-2

Creating a Service Request to Enable Itron Integration 5-3

Verifying Integration Access 5-3

Updating Certificate Used in Itron Integration 5-4
Deleting Certificate Used in Itron Integration 5-5

Chapter 1

Overview

End user provisioning involves creating user records and granting appropriate access for users of Oracle Utilities cloud services.

This chapter provides an overview of end user provisioning for Oracle Utilities Cloud Services, including:

- About This Book
- End User Provisioning Tasks and Account Types By Product

About This Book

This guide contains the following chapters:

- Chapter 1: Overview (this chapter) provides an overview of the types of tasks that apply to specific types of cloud services.
- Chapter 2: Oracle Utilities Cloud Service End User Provisioning describes tasks involved in creating and provisioning users of Oracle Utilities cloud services. Tasks described in this chapter apply to all Oracle Utilities cloud services.
- Chapter 3: Using Federated Single Sign-On describes tasks required when using an external identity management system to provide authentication for the application instances within your cloud subscription. Tasks described in this chapter apply to all Oracle Utilities cloud services.
- Chapter 4: Oracle DataRaker End User Provisioning Tasks describe end user provisioning tasks specific to Oracle DataRaker.
- Chapter 5: Meter Solution Cloud Service Itron Integration Tasks describes end user provision tasks required to support integration with the Itron OpenWay head-end system when using Oracle Utilities Meter Solution Cloud Service.

End User Provisioning Tasks and Account Types By Product

The table below outlines the tasks and types of accounts described in this guide that apply to each type of cloud service.

Task or Account Type	Enterprise Application Cloud Services*	DataRaker Cloud Service
Verifying Subscriber User Organization Access on page 2-4	Yes	Yes
Creating New Users on page 2-6	Yes	Yes
Modifying an Existing User on page 2-8	Yes	Yes
Assigning Roles on page 2-9	Yes	No
Provisioning Accounts on page 2-12	Yes	No
Resetting a Password on page 2-16	Yes	Yes
Disabling a User on page 2-17	Yes	Yes
Deleting a User on page 2-18	Yes	Yes
Cloud Service Foundation Accounts on page 2-20	Yes	No
Integration Accounts on page 2-20	Yes	No
Personal Accounts on page 2-21	Yes	Yes

*Enterprise Application Cloud Services (also referred to as "Oracle Utilities applications") include the following:

- Oracle Utilities Customer Cloud Service
- Oracle Utilities Meter Solution Cloud Service
- Oracle Utilities Operational Device Cloud Service
- Oracle Utilities Work and Asset Cloud Service

Chapter 2

Oracle Utilities Cloud Service End User Provisioning

This chapter provides instructions for Security Administrators to set up user accounts for Oracle Utilities cloud services, managing end-to-end lifecycle of user identity, and governing user authentication in multiple business applications. User management tasks include creation of the user record, a setup of the application roles, establishing user's membership in the role and, granting user an access to the target business applications. The section contains the following topics:

- Introduction
- User Management Procedures
- Accounts to Create

Note: Screen shots are provided to show examples only.

Introduction

This section provides an introduction to working with Oracle Identity Management with Oracle Utilities cloud services, including:

- Prerequisites
- Logging into Oracle Identity Management for the First Time
- Verifying Subscriber User Organization Access

Prerequisites

The following prerequisites must be met to work with Oracle Identity Management for Oracle Utilities cloud services:

- The account for the Security Administrator has been created and has been provisioned to all instances of business applications within the subscription.
- Security Administrator users have the following information
  - User Name and Password for Oracle Identity Management.
  - The URL of the Oracle Identity Management.

    The URL format is http://<host>/identity.

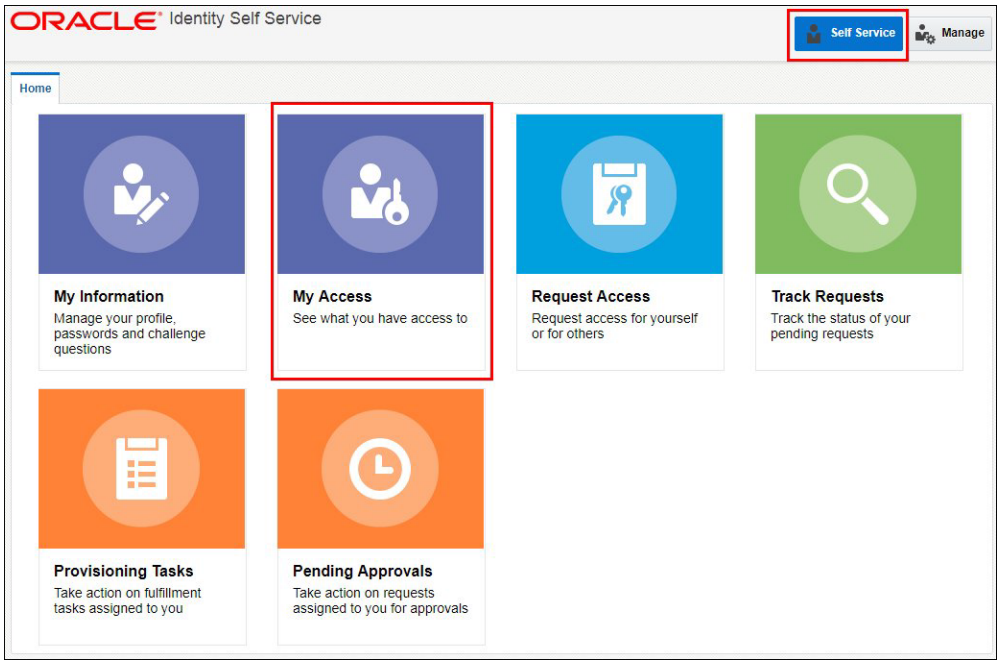
Logging into Oracle Identity Management for the First Time

System administrator users should use the following procedure the first time logging into Oracle Identity Management

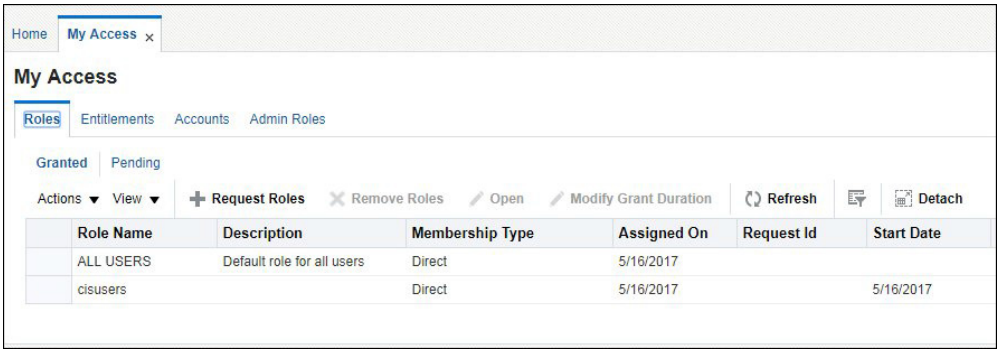
1. Log into the Oracle Identity Manager application with the URL and credentials provided by Oracle.

   You will be prompted to change your password and create security questions and answers the first time you log into OIM.
2. Enter and confirm the new password.
3. Select three security questions and provide the answers to those questions.
4. Security Administrator users will need access to the business applications for verification purposes.

Verify your Security Administrator access by switching to the **Identity Self-Service** home page and clicking **My Access**.



5. Explore your access information: **Roles**, **Accounts**, **Admin Roles**.



6. If not yet assigned, request the "cisusers" role and provision yourself to all environments (See **Provisioning Users** on page 2-9).

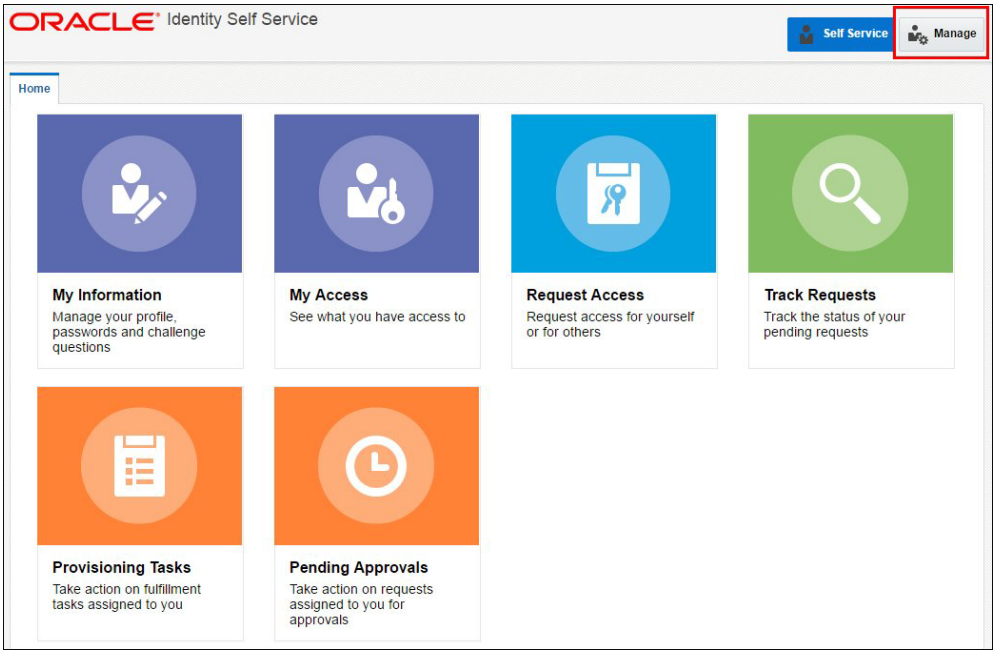
Verifying Subscriber User Organization Access

You must also verify the access to the "Subscriber Users" organization.

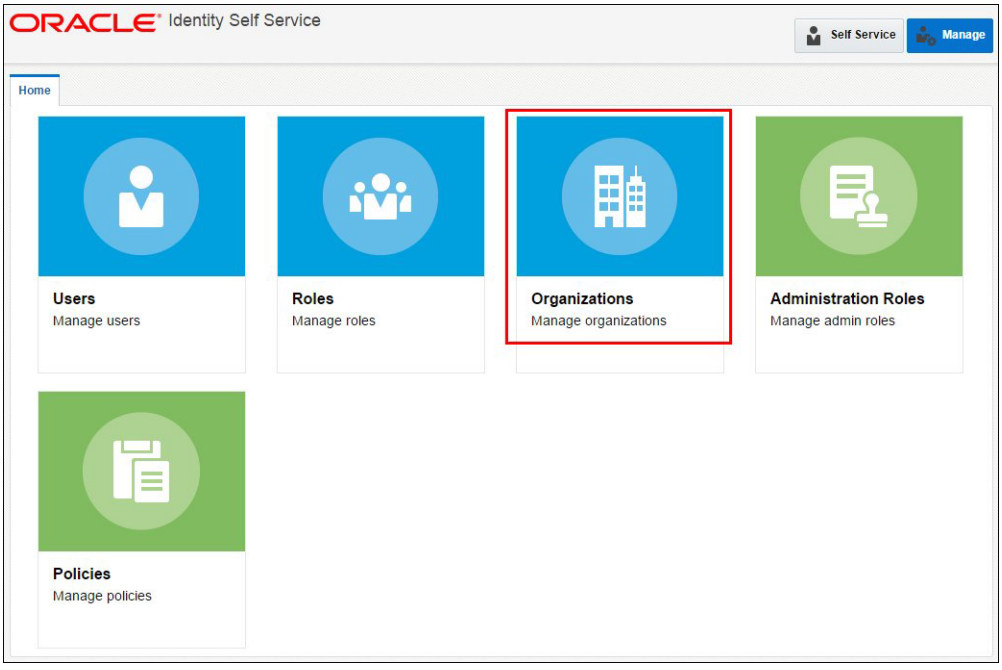
1. Login to Oracle Identity Management.

   Upon successful login, the **Identity Self-Service** home page opens.

2. Click the **Manage** button in the top right corner to open the **Management** home page.

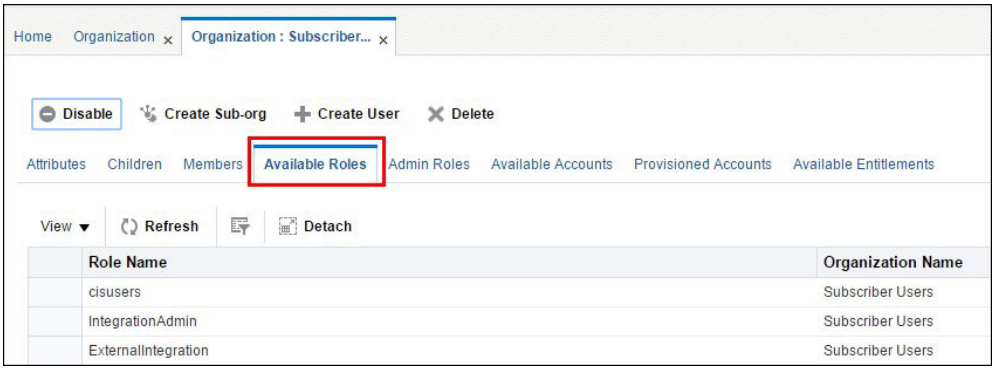


3. On the **Management** home page, click **Organizations**.



4. Verify that the list of available Organizations contains one entry: Subscriber Users.
5. Click on the entry to load the organization.

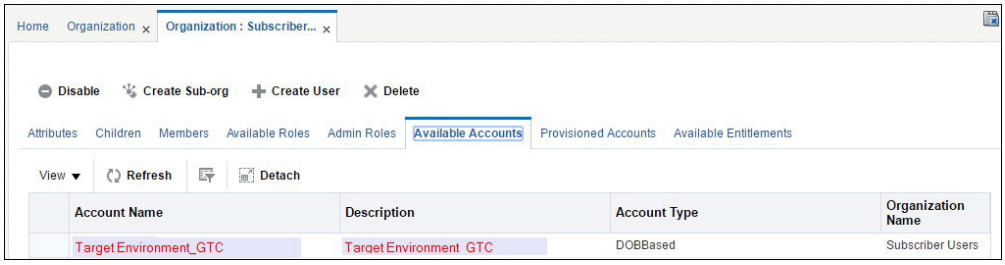
6. Click the **Available Roles** tab and verify that the **Roles** list includes:
    - cisusers
    - IntegrationAdmin
    - ExternalIntegrationUsers



7. Click the **Available Accounts** tab. Verify that the **Accounts** list includes entries for all instances of business applications that are included in the subscription.

    Each account corresponds to a target environment. Account name includes the product abbreviation (e.g. MDM) and an indicator of the environment 'type' - Development, Test or Production.

    Note: Oracle DataRaker account names include "ODR".



Note: A typical subscription includes one Production environment, and at least one Development and one Test environment. The number of environments depends on specific customer requirements and may include multiple Development and/or Test instances.

User Management Procedures

This section describes procedures related to user management, including:

- Creating New Users
- Provisioning Users
- Verifying User Access
- Resetting a Password
- Disabling a User
- Deleting a User

Creating New Users

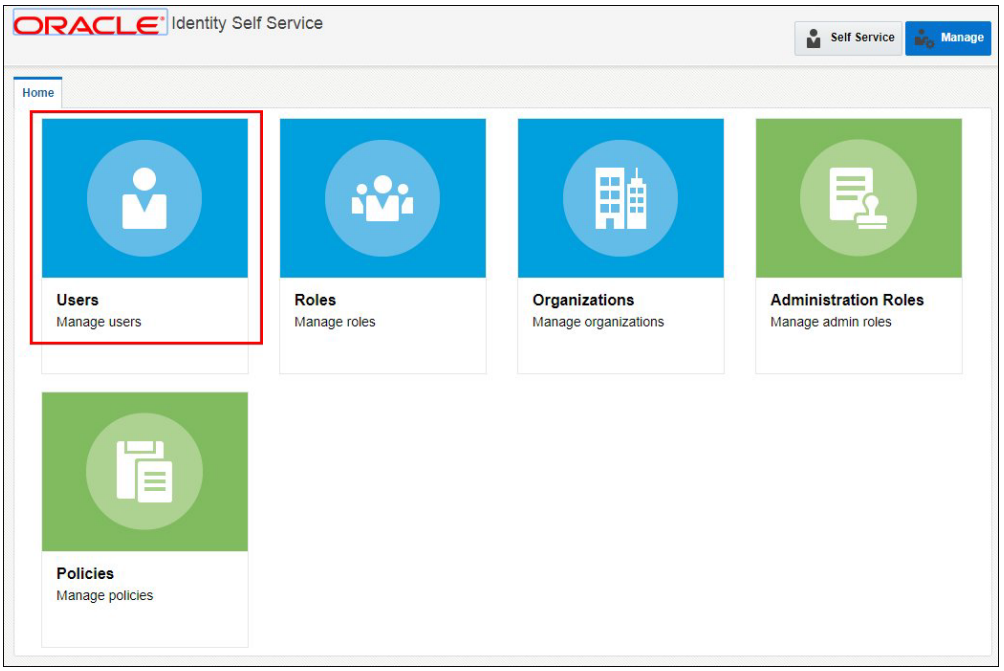
Use the following procedure to create a new a user in Oracle Identity Management.

1. Login to Oracle Identity Management.

   Upon successful login, the **Identity Self-Service** home page opens.

2. Click the **Manage** button in the top right corner to open the **Management** home page.

3. Click **Users** to open the **Users** page.

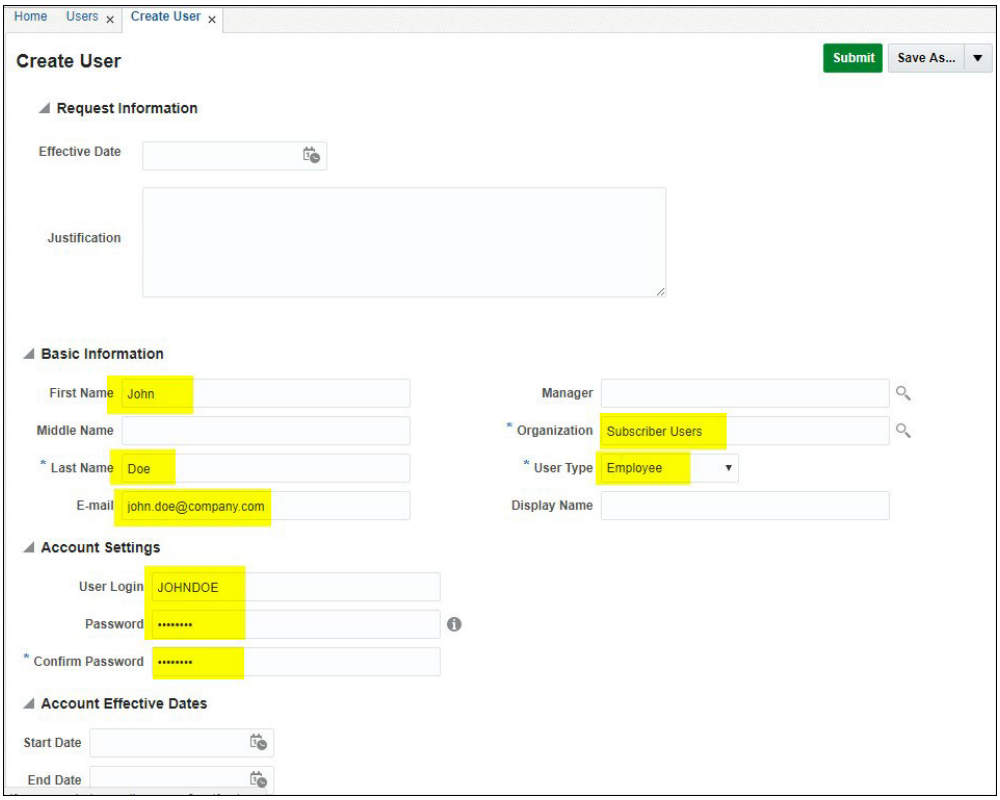


The **Users** tab opens.

4. Click **Create**.

The **Create User** page opens.

5. Populate basic user information as shown below:



Required Attributes:

- **Last Name**: The last name of the user being created.
- **User Login**: For Oracle Utility products users the login ID size cannot exceed 8 chars and cannot contain special characters.
- **Organization**: Select "Subscriber Users" from the search.
- **User Type**: This is a required attribute in OIM but it has no correlation with any user attributes in the target application. Select any value.

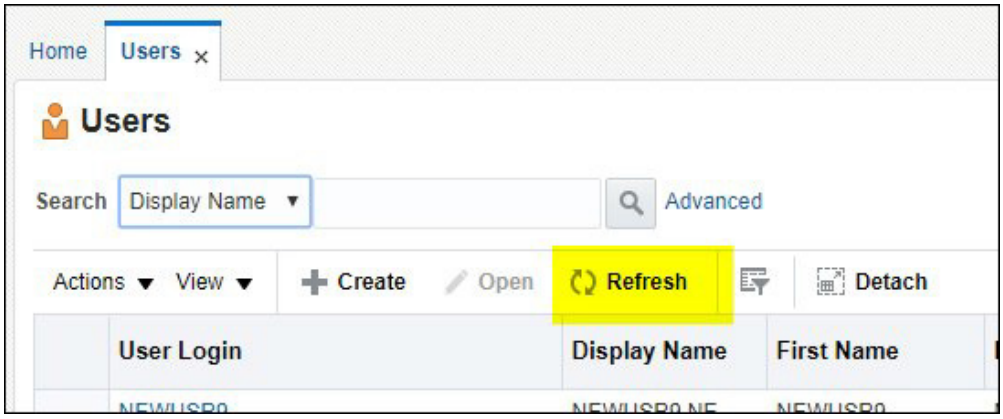
Optional Attributes:

- **Email Address**: Email address is required for personal (human) accounts. This email address is used by OIM for event notifications such as password expiration and other user-related events.
- **First Name**: Optional. It is recommended to populate it for personal accounts for the display and search purposes
- **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.

  There are two methods available for the initial user password setting:

  - Populate at user creation time. You can specify the initial password when creating the user.
  - Using the Resetting a Password feature.

6. Click **Submit** in the top right corner of the screen.
7. Return to the **Users** tab and click **Refresh**.

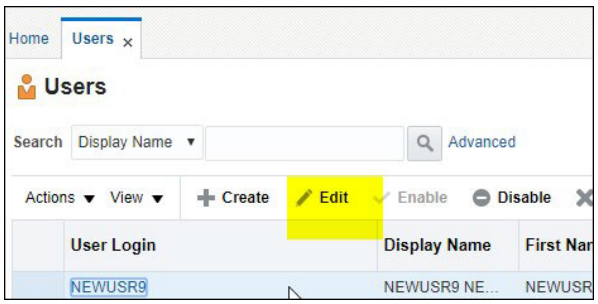


The newly created user record appears in the list.

Modifying an Existing User

Use the following procedure to modify an existing user.

1. Locate and highlight the user to be modified on the list.
2. Click **Edit** to open the user record.



3. Edit the user's attributes as appropriate.

   Most of the user's attributes can be modified.

The **Password** is not available for editing.

4. Click **Submit** in the top right corner of the screen to save your changes.

Provisioning Users

Provisioning is a process of defining a user's access to various applications within the subscription, and involves the following:

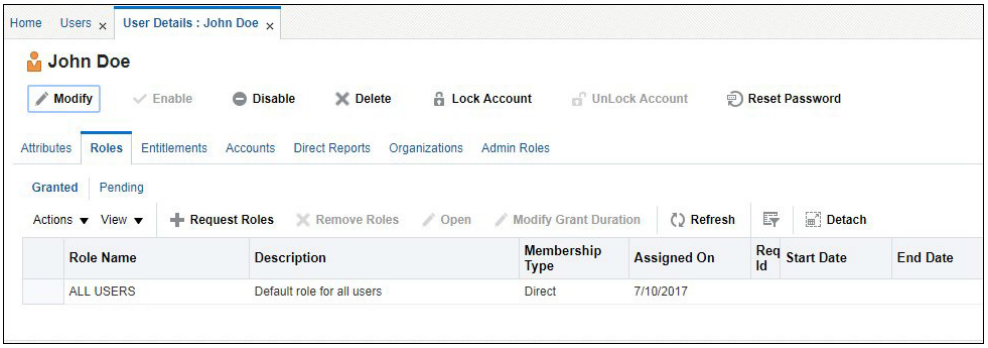
- Assigning Roles
- Provisioning Accounts

Assigning Roles

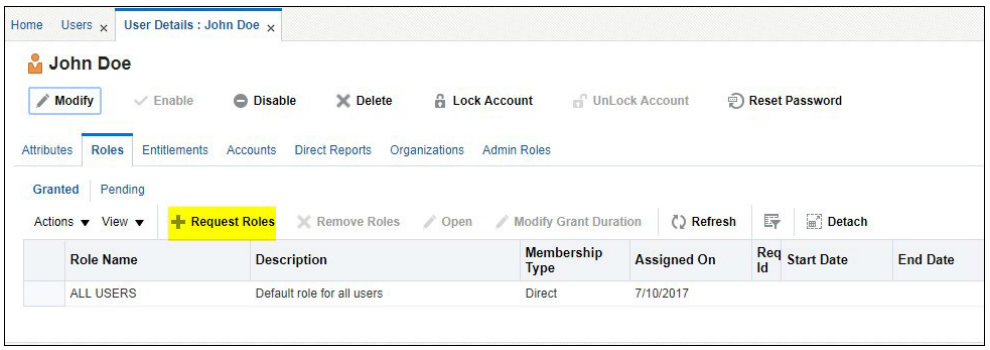
Use the following procedure to assign roles to users.

1. On the **User** tab, click the user to which you wish to assign a role.
2. Click on the **Roles** tab.

   Note that the *"ALL USERS"* role has already been assigned to this user by default.

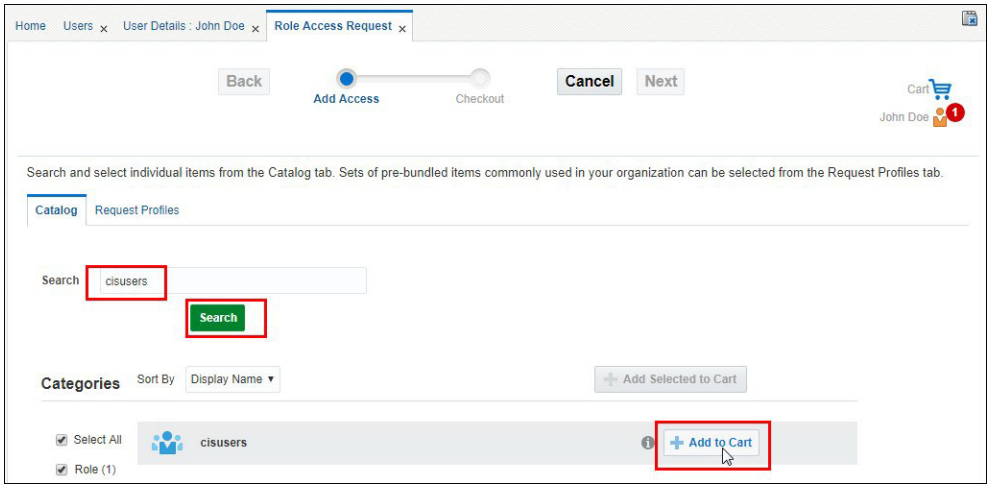


3. Click **Request Roles**.

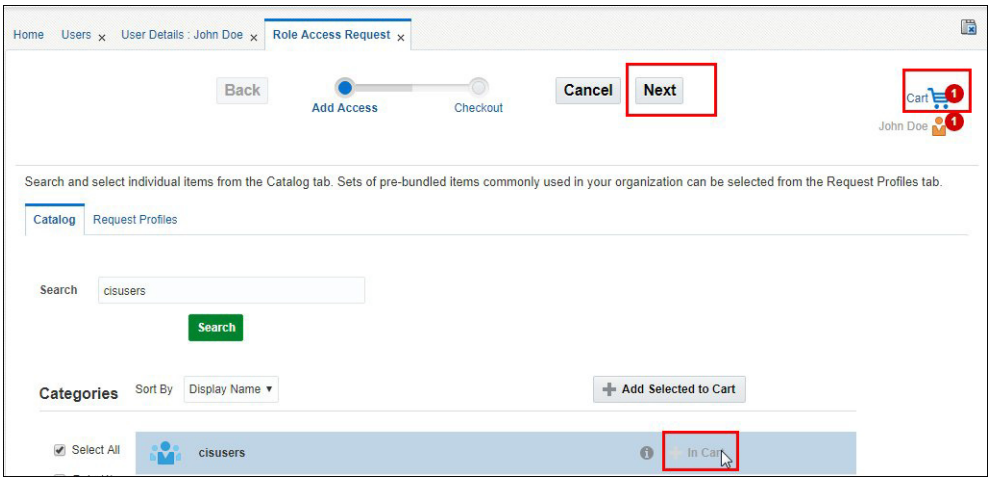


The **User Access Request** page opens, displaying a list of pre-defined roles.

4. Click **Add to Cart** button for the role you are assigning to the user. You can add several roles in one request. You can also search for the specific role name.



5. Once the role (or roles) are in the cart, click **Next**.

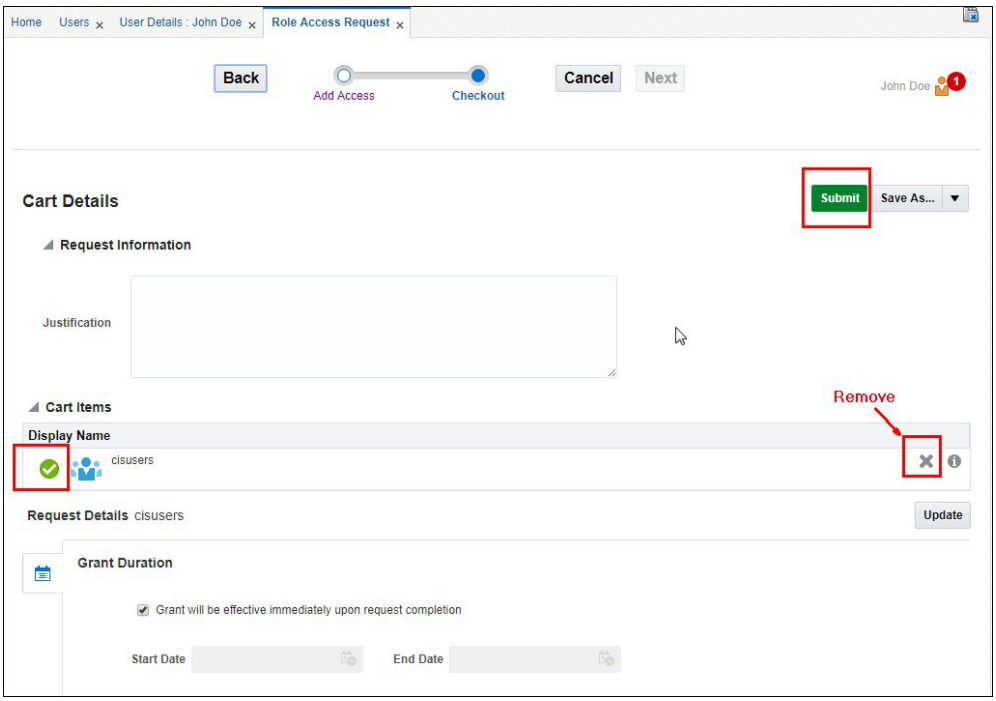


6. Review the request.

   At this step you can enter the justification for the role assignment and also set the effective start and end date.

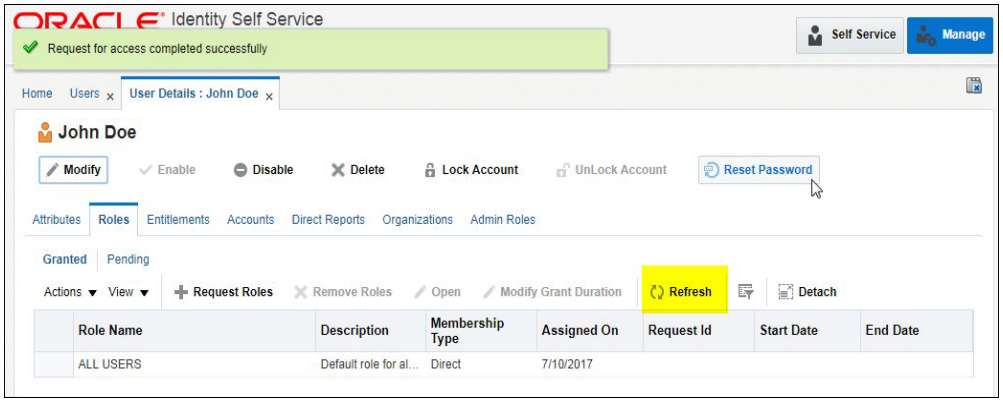
   The **check mark** icon next to the role indicates that no additional information is required for the role assignment.

   To remove the role from the cart if needed, click **Remove**.

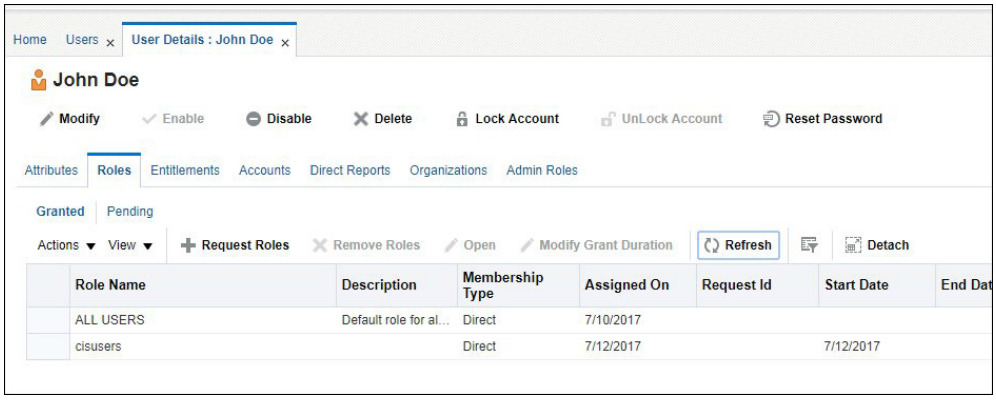


7. Click **Submit** to complete the request. You will be redirected back to the **Roles** tab on the **User Details** page.

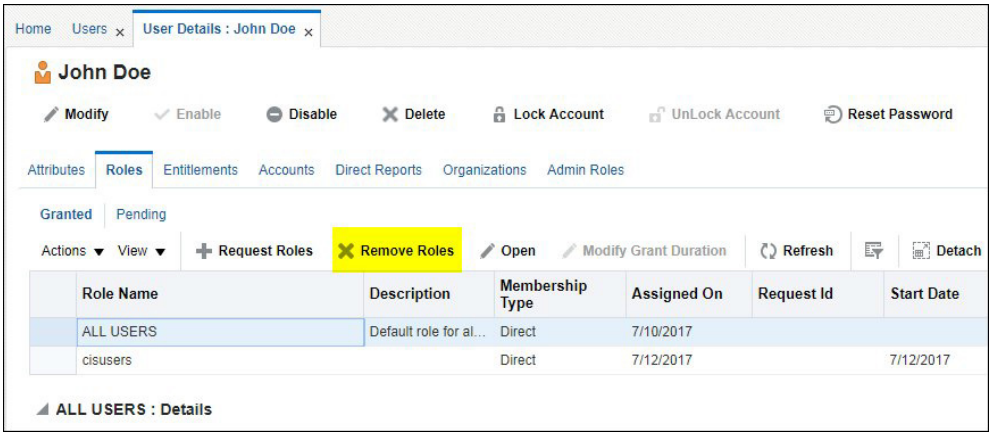
8. Click **Refresh**.



The new role appears on the list.



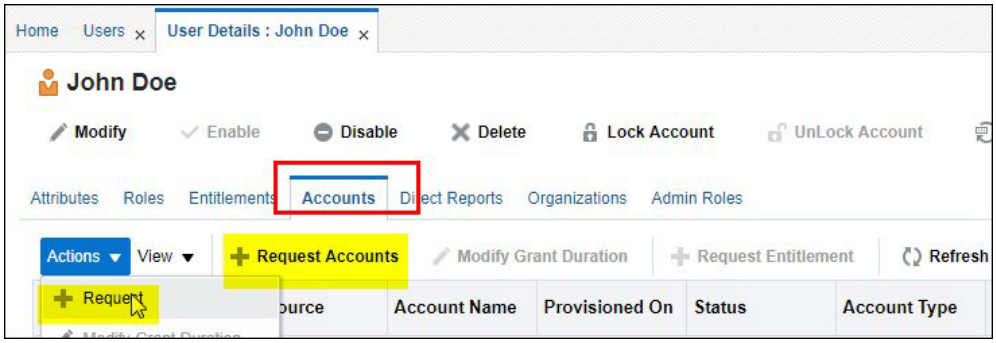
9. Roles can be removed by selecting the role to be removed and clicking **Remove Roles**.



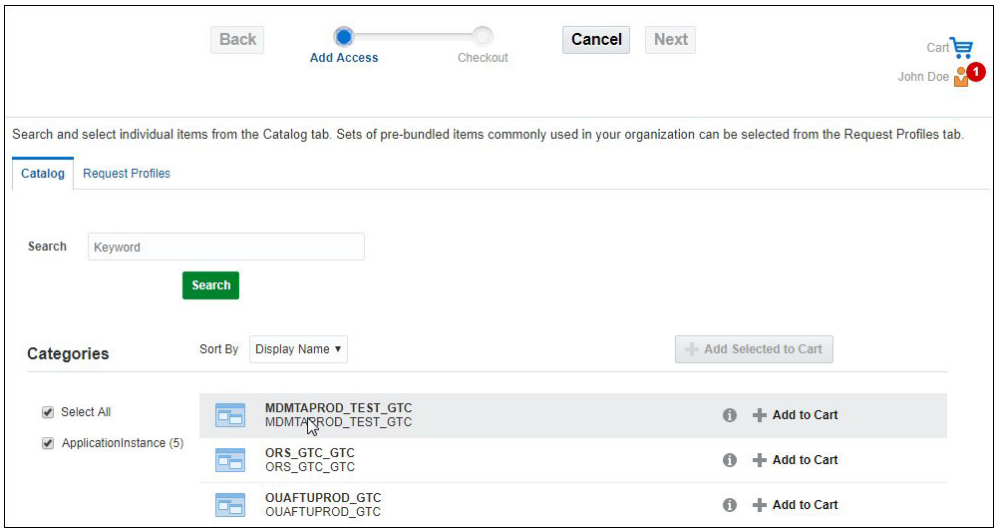
Provisioning Accounts

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

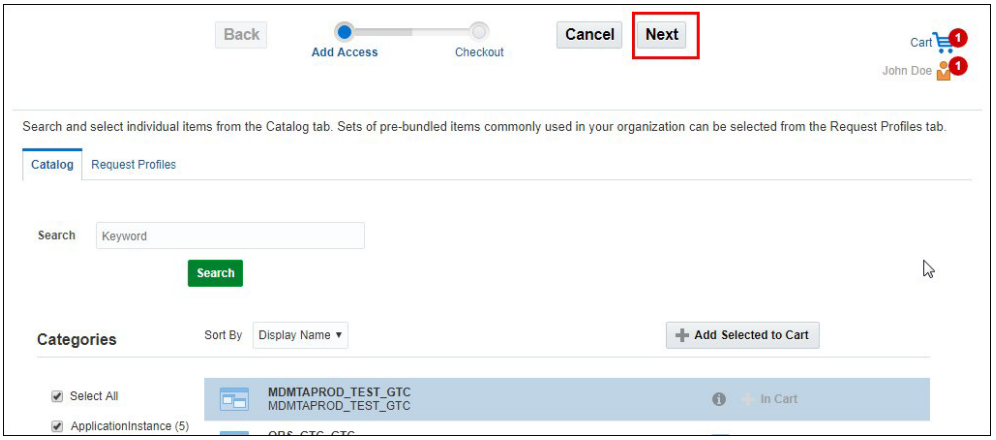
1. Click on the **Accounts** tab.
2. Click **Request Accounts** or select **Request** from the **Actions** drop-down list.



A list of available Application Instances is displayed. Application Instances represent the connection between Oracle Identity Manager and the target application included in the subscription.



3. Click **Add to Cart** to add a specific Application Instance to your cart.
4. Click **Next**.



5. Review the request.

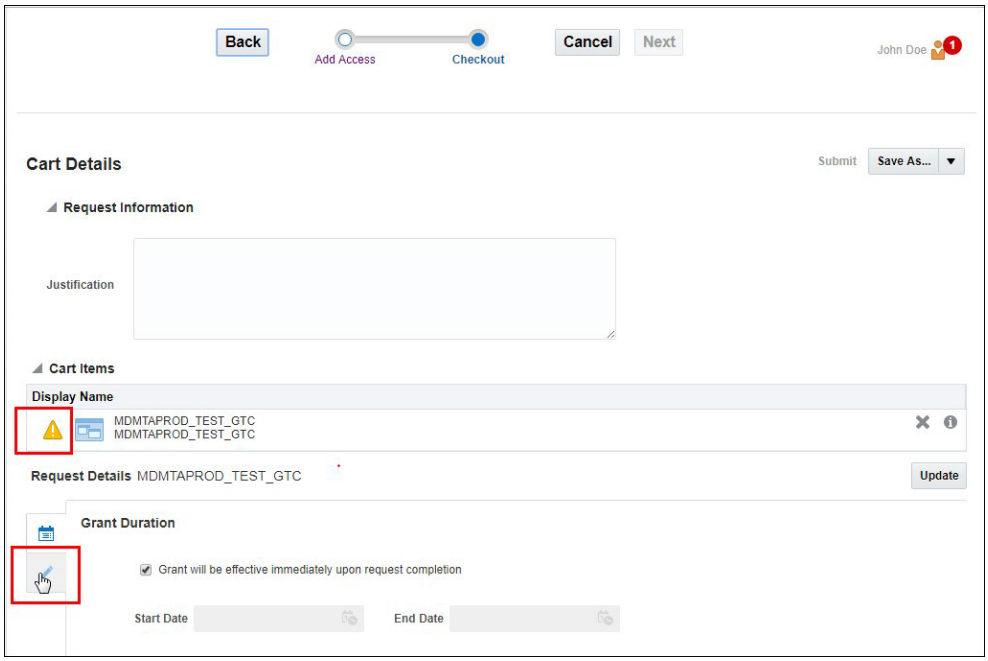
   At this step you can enter the justification for the account provisioning and also set the effective start and end date.

   The warning (!) icon next to the Application Instance name indicates that additional information is required to complete the request.

   To remove the Application Instance from the cart if needs, Click **Remove**.

   Note: Steps 6 - 8 are not applicable for Oracle DataRaker account provisioning.

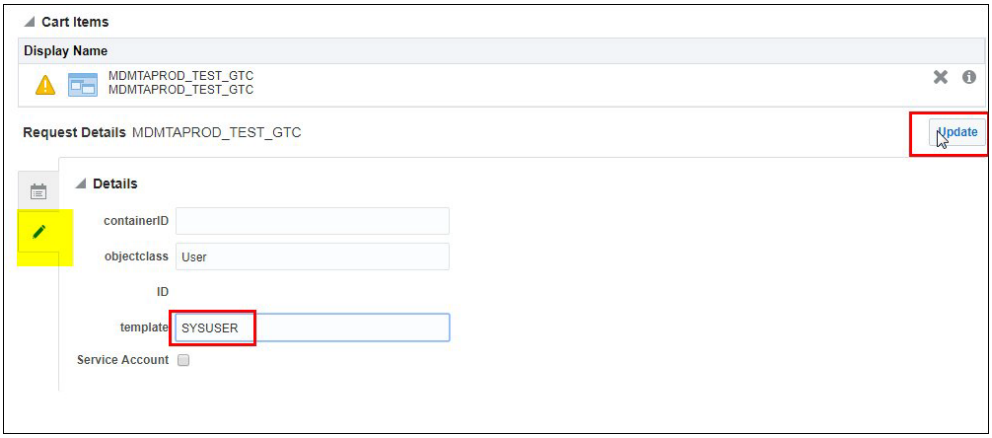
6. Click the **Edit** tab in the **Request Details** section to complete the missing information



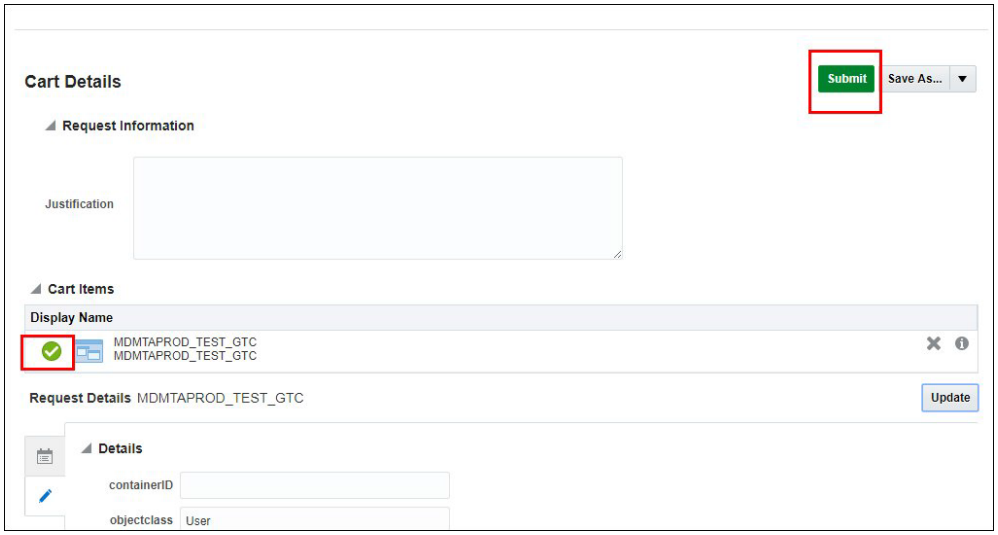
7. Populate the **Template** field with the User ID (not a Login ID) of the user record in the Oracle Utilities application that represents the typical user profile and authorization level.

   Note that initially only the "SYSUSER" template is available. Additional Template Users will become available as they are defined by the implementation or imported from product or implementation accelerators.

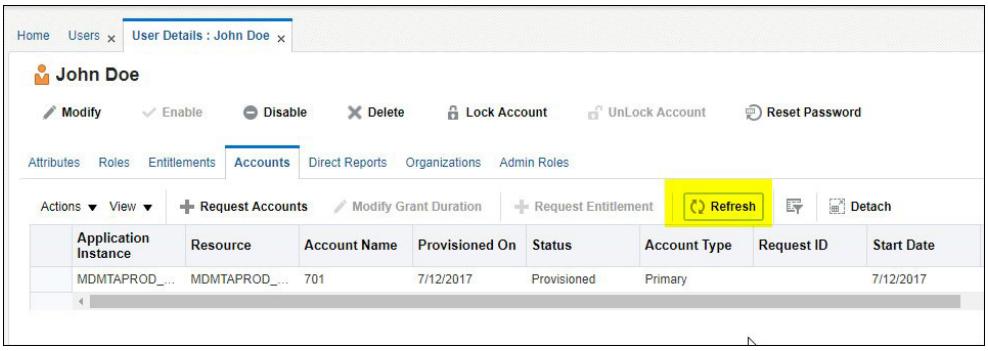
8. Click **Update**. Note that the request information is now sufficient and the **Submit** option is now enabled.



9. Click **Submit** to complete the request.



10. The request is now submitted and you will be redirected back to the **Accounts** tab. on the **User Details** page. Click **Refresh** and note that Application Instance was added to the list of accounts and in the "Provisioned" status.



The provision process is completed and the corresponding user record is created in the Oracle Utility or Oracle DataRaker application. The user is now granted login access to the target application instance.

Notes on User Provisioning

- You can request multiple roles and/or accounts at once. Simply add them to the cart and then update the details of each account, if needed.
- The system is configured to approve roles and account requests automatically, which means that the user can login into the target application immediately. If you wish to perform additional verification(s), consider un-checking the "Grant will be effective immediately…" indicator and setting the effective date manually.
- Provisioning with the "SYSUSER" Template User provides users with high-level authorization access to all the services in the target Oracle Utilities application (does not apply to Oracle DataRaker). It is recommended to setup additional Template Users with lesser privileges prior to creating and provisioning implementers, test and production users.

Verifying User Access

As soon as the account is provisioned, the user should be able to successfully log in. Use the following procedure to verify the user's access to the Oracle Utilities application:

1. Create a new "test" user using your own email address; assign the role(s) and provision the user to Development environment.

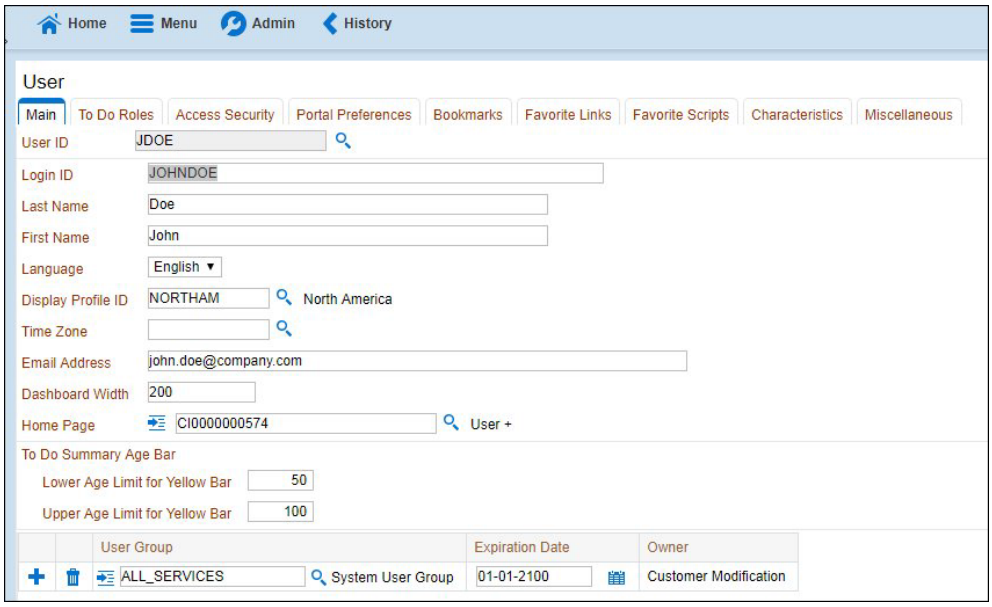
   You should receive a "New User Creation" notification email that contains the newly created login id and a one-time password.

2. Login into the Development environment with newly created user name and password.

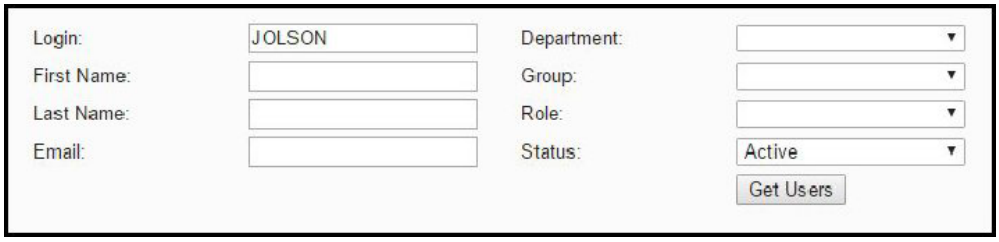
3. Perform all the steps of the first-time login flow and access the target environment.

   The illustration below shows how the user provisioned in the previous steps appears in the Oracle Utilities or Oracle DataRaker cloud service application.

   Oracle Utilities cloud service:



   Oracle DataRaker cloud service:

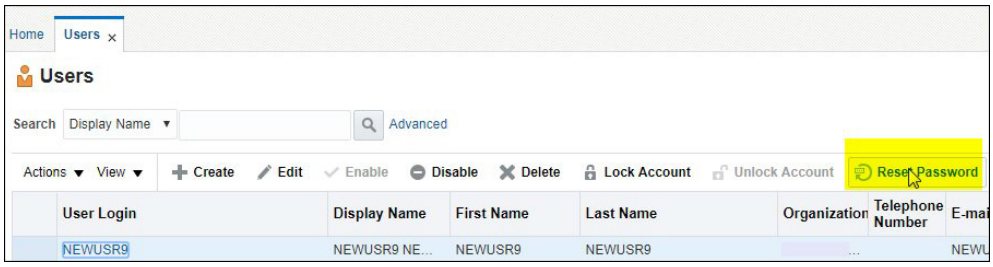


Resetting a Password

Use the following procedure to reset a user's password.

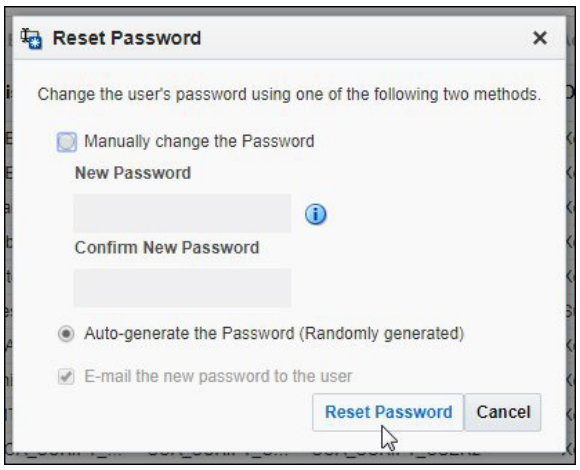
1. Locate the user's record in the list and highlight it. The **Reset Password** option becomes available.

2. Click **Reset Password**.



The **Reset Password** window opens.

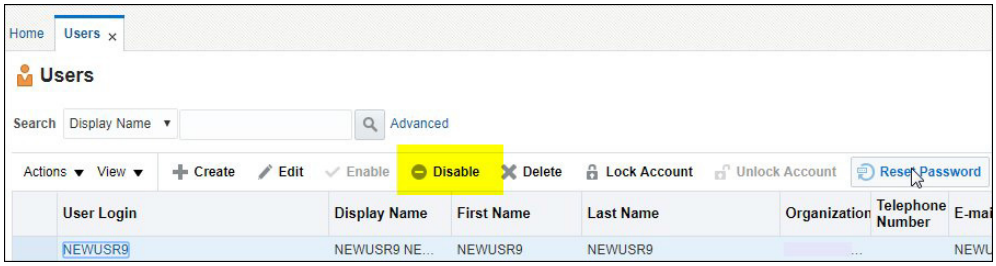
3. Select the appropriate option: Options include:
   - Manually change this Password
     - Enter and confirm the new password.
   - Auto generate the password (Randomly generated)
4. Click **Reset Password**.



Disabling a User

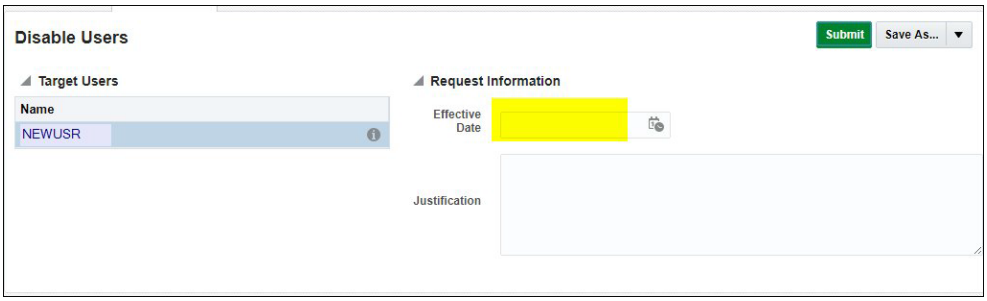
Use the following procedure to disable an active user.

1. Locate the user record you wish to disable in the list and highlight it. The **Disable** option becomes available.
2. Click **Disable**.



3. Enter the **Effective Date** and **Justification**.

   If a target effective date is not entered, the user is disabled effective immediately.

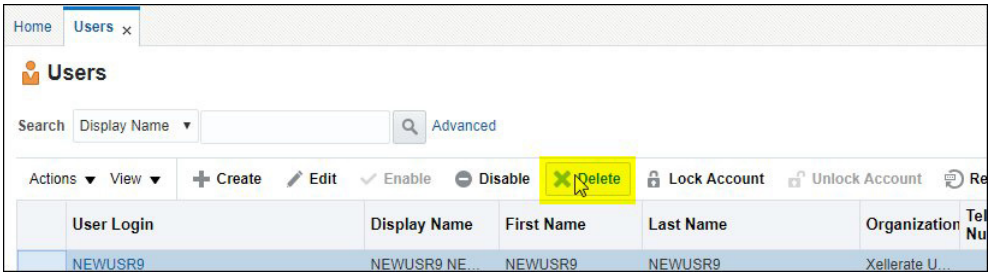


4. Click **Submit**.
5. Verify that the user is unable to login to the target environment.

Deleting a User

Use the following procedure to remove a user from the system.

1. Locate the user record you wish to delete in the list and highlight it. The **Delete** option becomes available.
2. Click **Delete**.



3. Enter an **Effective Date** and **Justification**.

   If a target effective date not entered, the user is deleted immediately.
4. Click **Submit**.
5. Verify that the user is unable to login to the target environment.

Accounts to Create

In Oracle Identity Management an account represents a user's entitlement to access a specific application instance. A user can also be a member of one or multiple application roles. This section outlines the different types of user accounts created by system administrators. This includes:

- Pre-Defined Roles
- Available Accounts
- Cloud Service Foundation Accounts
- Integration Accounts
- Personal Accounts

Pre-Defined Roles

The following roles are pre-defined and should be available for assignment to users:

- **cisusers**: Provides users with access to one of the Oracle Utilities cloud services. Appropriate for both personal and integration/API accounts.
- **IntegrationAdmin**: Provides access to Integration Cloud Connector services. Appropriate for integration accounts.
- **ExternalIntegrationUsers**: Supports communication with external systems via web services. Appropriate for integration accounts supporting communication with SOA composites.
- In addition to the roles listed above, the list may contain a set of roles necessary to access Oracle BI Publisher. It typically includes three roles per product, with different authorization level:
  - **report author**: The highest authorization level that allows user to develop new reports
  - **analyst**: Allows user to modify and run reports
  - **consumer role**: Default role allows users to view the existing reports
- Possible roles for specific Oracle Utilities cloud services include:
  - Meter Solution Cloud Service (MSCS): MDMAUTHOR, MDMANALYST,MDMBICONSUMER (MDMCONSUMER)
  - Customer Solution Cloud Service (CSCS): CCBAUTHOR, CCBANALYST, CCBBICONSUMER (CCBCONSUMER)
  - Work and Asset Solution Cloud Service (WACS): WAMAUTHOR, WAMANALYST, WAMBICONSUMER(WAMCONSUMER)
  - Mobile Workforce Cloud Service (MWCS): MWMAUTHOR, MWMANALYST, MWMBICONSUMER(MWMCONSUMER)

Available Accounts

Oracle Identity Management can be connected to one or more target business applications.

For Oracle Utilities applications, these connections are pre-configured and the name of the application instance is composed as follows:

<abbreviated target product name>-TU-**<application instance type>**_GTC

where

- **<abbreviated target product name>** is an abbreviation for a specific Oracle Utilities cloud service. For example, "MDM" is an abbreviated target product name for Oracle Utilities Meter Solution Cloud Service.
- **<application instance type>** is a designation for a specific type of application instance. Possible instance types include:
  - DEV - Development environment
  - TEST - Test environment
  - PROD - Production

Example:

The name for an Oracle Utilities Meter Solution Cloud Service Development environment would be as follows:

MDM-TU-DEV_GTC

For Oracle DataRaker, the account name will typically include "O".DR

Cloud Service Foundation Accounts

Your Oracle Utilities cloud services include a set of tools that facilitate several implementation and management tasks. In order to enable these tools you need to create at least one internal Cloud Service Foundation Integration Account (non-human). The credentials of this account are used by the outbound messages sent by the instances of the target application.

> **Note**: Cloud Service Foundation accounts apply to Oracle Utilities applications, but do not apply to Oracle DataRaker

Upon successful creation of this account, communicate the user credentials to the application configuration administrator.

User	Roles	Accounts
CSF Integration User Login ID: • Alphanumeric • No more than 8 chars • No special characters	• IntegrationAdmin • cisusers	Provision to all available instances of OUAF-based applications included in the subscription. Template User: *K1PAUSER*

Integration Accounts

Integration accounts support web service communications between business applications within the subscription and with external systems.

Note: Integration accounts apply to Oracle Utilities applications, but do not apply to Oracle DataRaker

You should create the following integration accounts:

- Integration Cloud Connector (ICC) Account (non-human)

  This user's credentials are specified in the connection configuration of SOA Composites.

User	Roles	Accounts
ICC User Login ID: • Alphanumeric	• IntegrationAdmin • cisusers	

- External Integration Account (non-human)

  The credentials of this account are used by the messages sent to the SOA composites within the integration layer.

User	Roles	Accounts
External Integration User Login ID: • Alphanumeric	• ExternalIntegrationUsers	

Personal Accounts

Upon request, create and provision personal user accounts for all Oracle Utilities and Oracle DataRaker environments.

Users have to be provisioned to all target application environments they need to access.

For each user, collect and specify basic information:

- Last Name
- First Name
- Email address

Assign Roles and Accounts as follows:

User	Roles	Accounts
Application User Login ID: • Alphanumeric • No more than 8 chars • No special characters	• cisusers	Provision to all applicable instances of the business application within the subscription. Specify a Template User according to user's intended implementation or business role.

Chapter 3

Using Federated Single Sign-On

Federated Single Sign-On (SSO) allows your organization to use an external identity management system to provide online authentication for the application instances within your cloud subscription. The configuration and verification of the Federated Single Sign On is performed by Oracle upon request from the customer and should be available after the subscription is live.

This chapter includes:

- Adding Oracle Utilities and Oracle DataRaker Application Authorization
- Supporting Role-based Authorization

Note: The user setup specifics for Federated Single Sign-On only concerns online access; it is not applicable for the integration and other non-human accounts.

Adding Oracle Utilities and Oracle DataRaker Application Authorization

In order to be authorized to access the Oracle Utilities cloud services, a user record has to be defined in the application instance.

The procedure for providing users with access is different depending on whether you maintain the local list of users in Oracle Identity Management.

User Record is Created in Oracle Identity Management

1. Login to the Oracle Identity Management.
2. Locate the user record.
3. Follow the steps outlined under Provision Accounts in Chapter 1 to add the user to all target application instances

User Record is Not Created in Oracle Identity Management

1. Login to each of the Oracle Utilities and/or Oracle DataRaker product applications within the subscription.
2. Manually add the user record.
   - Make sure that the value in the **Login ID** field exactly matches the user name in your external identity management system
   - Add at least one user group so the user will be able to access the transactions that are appropriate for the user's business role.

Supporting Role-based Authorization

In order to provide online access to Oracle Utilities Analytics and other products that require role assignment, create a user record in Oracle Identity Management and follow the steps outlined under Assigning Roles in Chapter 1.

Chapter 4

Oracle DataRaker End User Provisioning Tasks

Once a user has been created in Oracle Identity Management, the user record is created in the Oracle DataRaker user list, and is ready to be configured and assigned to DataRaker groups and roles. Groups and roles determine the user features and functionality available to each user.

This chapter outlines specific steps that need to be performed to configured users in Oracle DataRaker, including:

- Locating Provisioned Users in Oracle DataRaker
- Assigning Groups and Roles in Oracle DataRaker

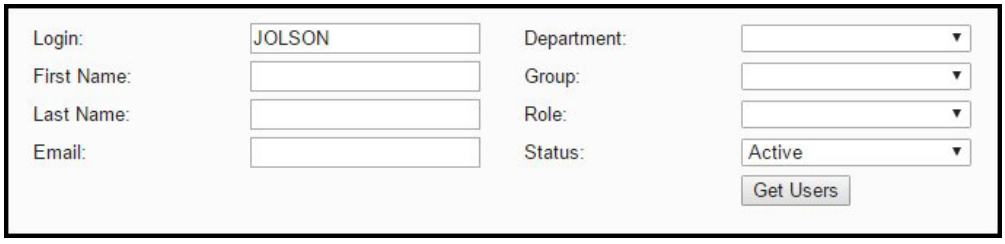
Locating Provisioned Users in Oracle DataRaker

Once a user has been created in Oracle Identity Management, it will appear in the Oracle DataRaker user list. See **Provisioning Users** on page 2-9.

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.

Use the following procedure to locate a user.

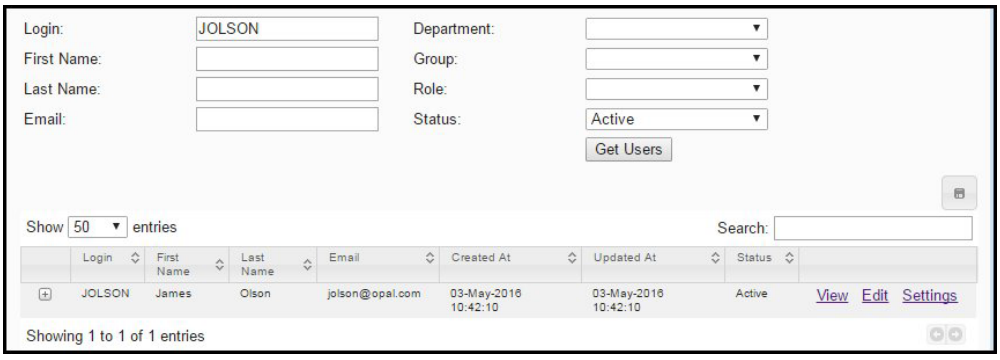
1. Log in to Oracle DataRaker.
2. Select **Administer > Security> Users** to navigate to the **Administer Users** page.
3. Search for the user you created in Oracle Identity Management by completing one of the user information fields and then clicking the **Get Users** button.



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.



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.

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

Use the following procedure to assign a user to a group:

1. Locate the user in Oracle DataRaker and open the **Manage User** dialog box for the user. See **Locating Provisioned Users in Oracle DataRaker** on page 4-2.
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

Use the following procedure to remove group assignments:

1. Open the **Manage User** dialog box for the user. See **Locating Provisioned Users in Oracle DataRaker** on page 4-2.
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.

Use the following procedure to assign user Role permissions:

1. Open the **Manage User** dialog box for the user. See **Locating Provisioned Users in Oracle DataRaker** on page 4-2.
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

Use the following procedure to remove user role permissions:

1. Open the **Manage User** dialog box for the user. See **Locating Provisioned Users in Oracle DataRaker** on page 4-2.
2. Click the **Remove** link next to the role.

Chapter 5

Meter Solution Cloud Service Itron Integration Tasks

This chapter outlines specific steps that need to be performed in order to support integration with the Itron OpenWay head-end system when using Oracle Utilities Meter Solution Cloud Service, including:

- Enabling Itron Integration
- Updating Certificate Used in Itron Integration
- Deleting Certificate Used in Itron Integration

Enabling Itron Integration

Perform the following steps to enable integration with Itron OpenWay:

- Creating an Integration Account
- Creating an X.509 Certificate
- Creating a Service Request to Enable Itron Integration
- Verifying Integration Access

Creating an Integration Account

You must create a separate integration account for integration with the Itron head-end system.

1. Create an External Integration Account (non-human) account.

   The credentials of this account are used to process the messages originated from the Itron system. This user's information will be used to upload the security certificate.

User	Roles
Itron Integration User Login ID: • Alphanumeric	• ExternalIntegrationUsers

Creating an X.509 Certificate

The Oracle Utilities Meter Solution Cloud Service Itron Openway Adapter supports X.509 authentication (certificate over transport). The certificate is owned and created by the customer. The public key portion is provided to the MSCS system to perform the authentication. The CN of the user must match the values of First Name + Last Name entered in Identity Self Service.

Keytool is the most readily-available certificate creation tool, though there are others.

1. Create a certificate using a command similar to this, but unique to the customer's organization:

```
keytool -genkey -alias {host name} -keyalg RSA -keystore {keystore
name}.jks -keysize 2048 -validity 730 -dname
"C=US,ST=California,L=Redwood City,O=High Efficiency
Energy,OU=Commercial Meters,CN=Joe User"
```

   A new certificate will be created in a keystore with the provided name. This new certificate should be signed by a certificate signing authority. Consult the Keytool documentation for the commands to extract a CSR and to re-import the signed key.

   The certificate will be used in the messages from the Itron OpenWay head end system to the MSCS SOA server.

Creating a Service Request to Enable Itron Integration

Create a service request with Oracle requesting enabling of the Itron integration and attach the certificate (signed by a certificate signing authority) created in the previous step.

Verifying Integration Access

Verify that the cloud service can be accessed as desired. This step should be performed after the service request has been updated that the Itron Integration has been enabled. Update the service request with the results of the verification.

Updating Certificate Used in Itron Integration

Use the following procedure if a certificate that is currently used in the Itron Integration has been revoked and a new certificate needs to be applied.

1. Create a new certificate to update the revoked certificate. See **Creating an X.509 Certificate** on page 5-2 for details about creating a new certificate.
2. Create a service request with Oracle requesting that the certificate used in the Itron integration be updated, and attach a certificate signed by a certificate signing authority.
3. Verify that the cloud service can be accessed as desired.

   This step should be performed after the service request has been updated that the Itron Integration has been enabled.
4. Update the service request with the results of the verification.

Deleting Certificate Used in Itron Integration

Use the following procedure if a customer needs to delete a certificate that is currently used in the Itron Integration.

1. Create a service request with Oracle requesting to delete the certificate used in the Itron integration.

   Provide the "CN" attribute from the certificate that is currently in use with the Itron Integration.

2. Verify that the cloud service cannot be accessed by using the existing certificate.

   This step should be performed after the service request has been updated that the Itron Integration has been disabled.

3. Update the service request with the results of the verification.