

Oracle Utilities Customer Cloud Service

End-User Provisioning Guide

Release 17.1

E90887-01

December 2017

Copyright © 2017 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

Oracle Utilities Cloud Service End-User Provisioning	1-1
Introduction.....	1-2
Prerequisites	1-2
Confirm Access to Oracle Identity Management.....	1-2
First Time Logging into Oracle Identity Management.....	1-2
Initial Setup	1-4
User Management Procedures.....	1-6
Create a New User	1-6
Provision Users.....	1-9
Verify User Access	1-15
Reset Password.....	1-16
Disable User.....	1-17
Delete User.....	1-18
Accounts to Create.....	1-19
Pre-Defined Roles.....	1-19
Available Accounts	1-19
Cloud Service Foundation Accounts	1-20
Integration Accounts	1-20
Personal Accounts.....	1-21

Chapter 2

Using Federated Single Sign-On	2-1
Adding Oracle Utility Application Authorization	2-2
User record created in Oracle Identity Management.....	2-2
User Record is not created in Oracle Identity Management	2-2
Supporting Role-based Authorization	2-3

Chapter 1

Oracle Utilities Cloud Service End-User Provisioning

This chapter provides instructions for Security Administrators to set up user accounts for Oracle Utilities cloud services.

- [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](#)
- [Confirm Access to Oracle Identity Management](#)
- [First Time Logging into Oracle Identity Management](#)
- [Initial Setup](#)

Prerequisites

The following are prerequisites to working with Oracle Identity Management for Oracle Utilities cloud services:

- The account for the Security Administrator has been created as part of the post-provisioning steps.
- The Security Administrator has been provisioned to all instances of business applications within the subscription

Confirm Access to Oracle Identity Management

Before you can create users in Oracle Identity Management, you must first verify the Security Administrator's access.

In order to perform user management tasks you should have the following information:

- User Name and Password for Oracle Identity Management Self-Service (you'll be asked to change the password the first time you log into OIM, and create security questions and answers)
- The URL of the Oracle Identity Management Self-Service. It is usually composed as `http://<host>/identity`

First Time Logging into Oracle Identity Management

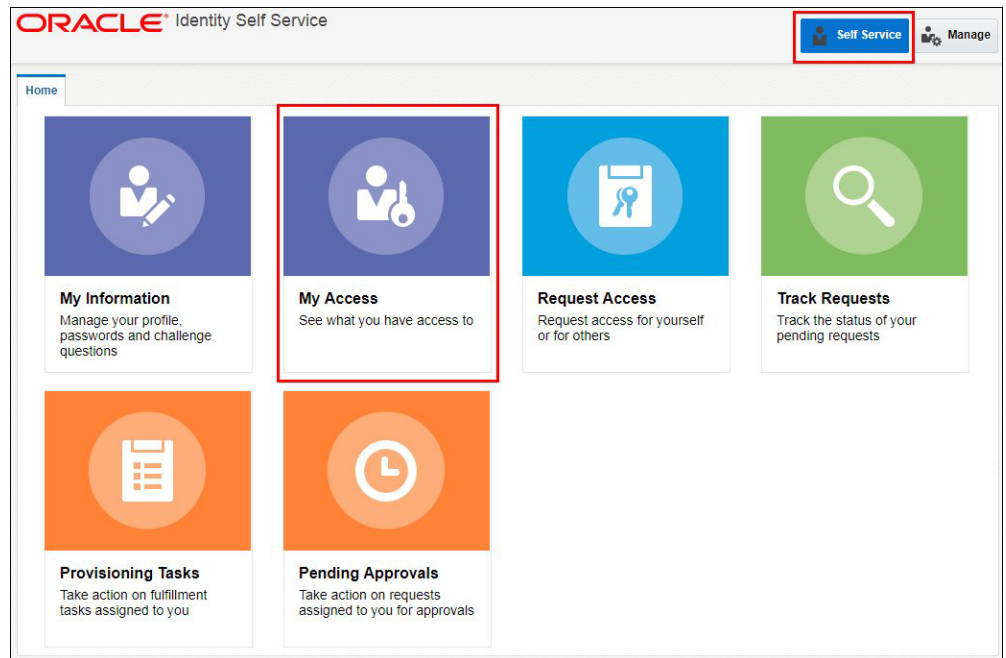
Use the following procedure the first time you log into Oracle Identity Management

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

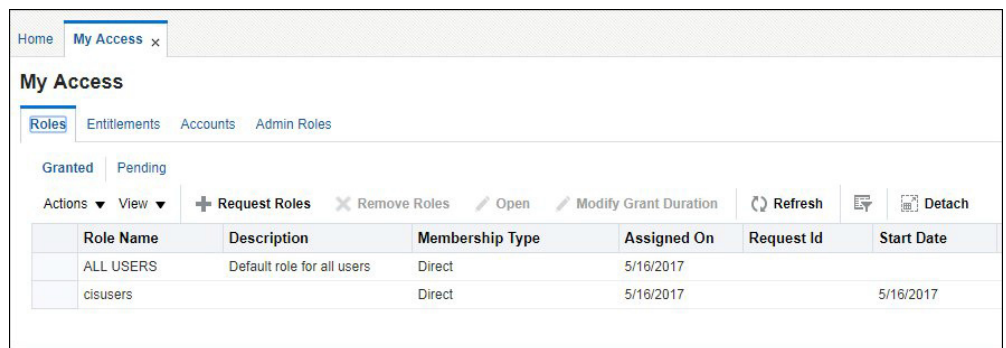
On the first login attempt you will be prompted to re-set the temporary password. The instructions for password format are displayed on-screen.

2. Enter and confirm the new password.
3. Select three security questions and provide the answers to those questions.
4. You (Security Administrator) will need access to the business applications for verification purposes.

Verify your 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 **Provision Users** on page 1-9 steps below).

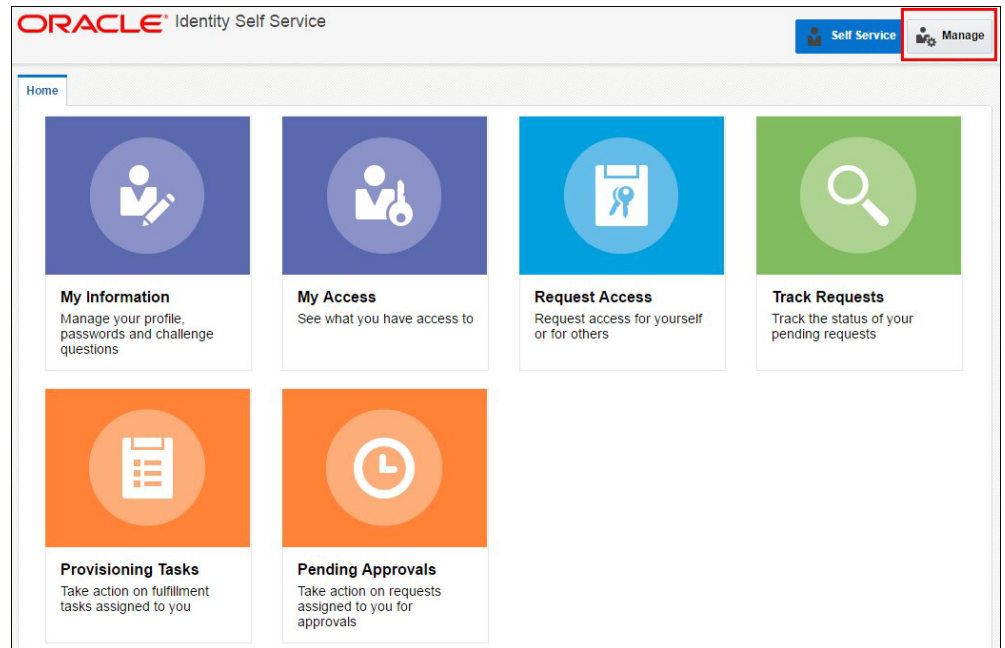
Initial Setup

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

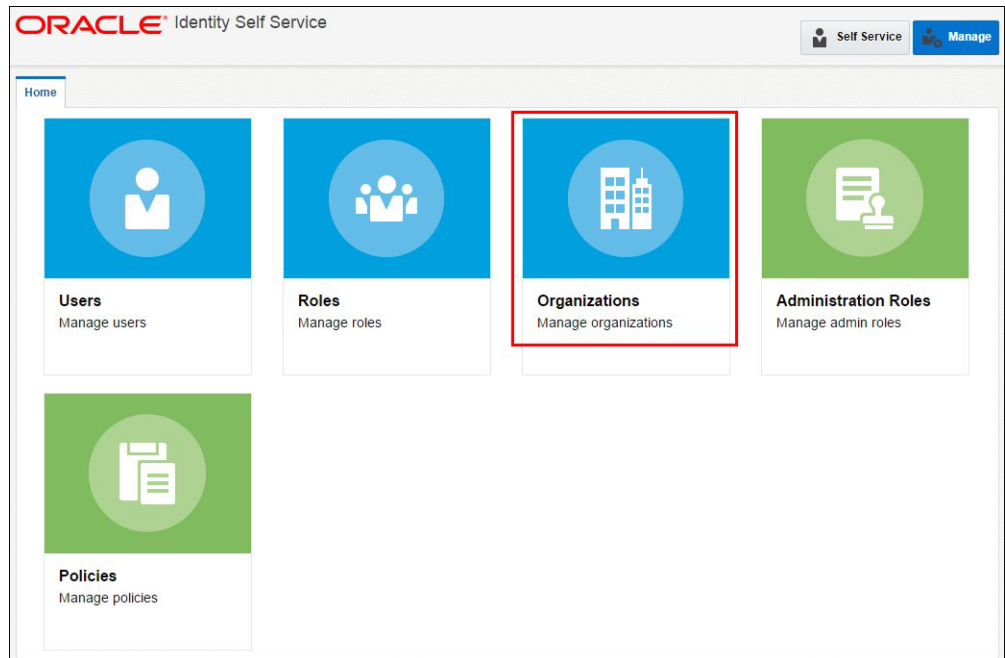
1. Login to Oracle Identity Management.

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

Role Name	Organization Name
cisusers	Subscriber Users
IntegrationAdmin	Subscriber Users
ExternalIntegration	Subscriber Users

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.

Account Name	Description	Account Type	Organization Name
TargetEnvironment_GTC	TargetEnvironment GTC	DOBBased	Subscriber Users

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

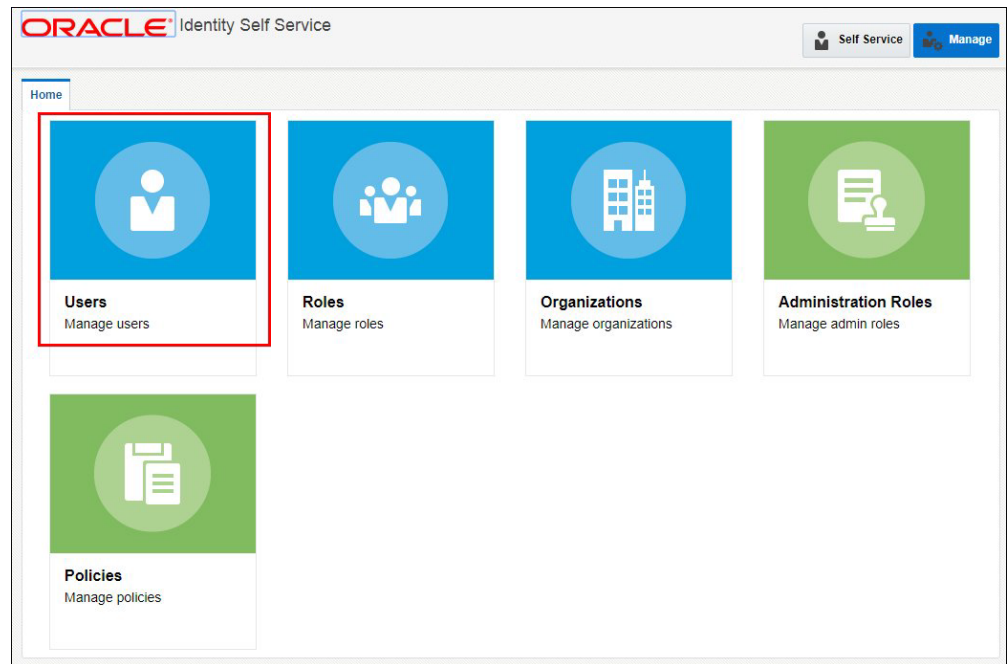
This section describes procedures related to user management, including:

- [Create a New User](#)
- [Provision Users](#)
- [Verify User Access](#)
- [Reset Password](#)
- [Disable User](#)
- [Delete User](#)

Create a New User

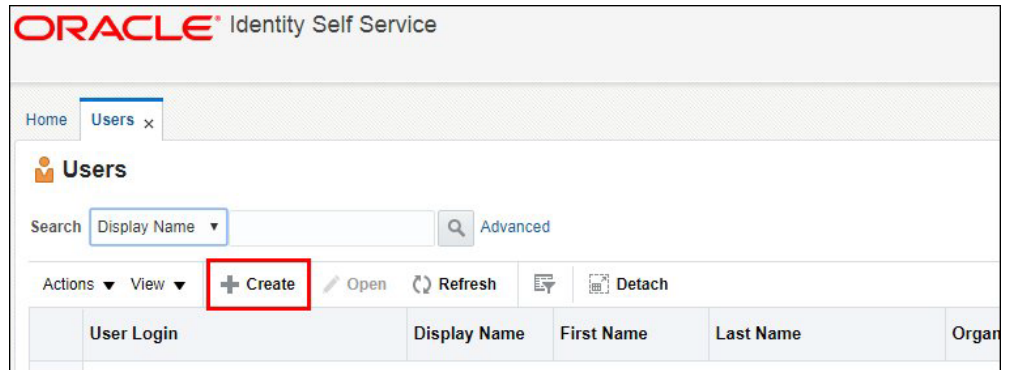
Use the following procedure to create a new a user in Oracle Identity Management.

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.

- Click **Create**.



The **Create User** page opens.

- Populate basic user information as shown below:

Required Attributes:

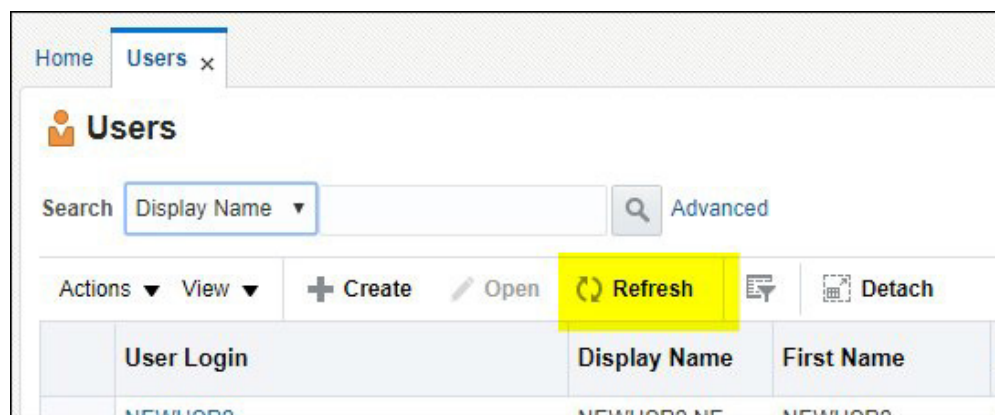
- **Last Name:** The last name of the user being created.
- **User Login:** For Oracle Utility products users the login ID size cannot exceed 8 chars and cannot contain special characters.
- **Organization:** Select “Subscriber Users” from the search.
- **User Type:** This is a required attribute in 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 [Reset Password](#) feature.
6. Click **Submit** in the top right corner of the screen.
 7. Return to the **Users** tab and click **Refresh**.

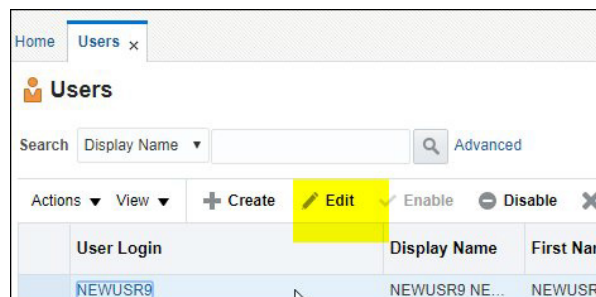


The newly created user record appears in the list.

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.

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

Provision Users

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

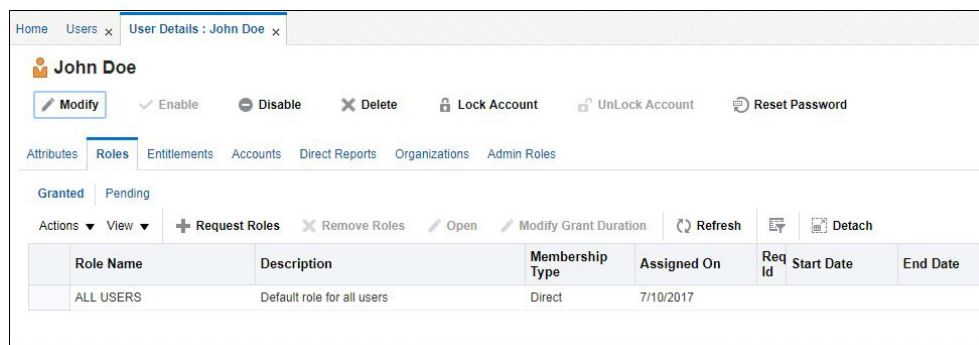
- [Assign Roles](#)
- [Provision Accounts](#)

Assign Roles

Use the following procedure to assign roles to users.

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

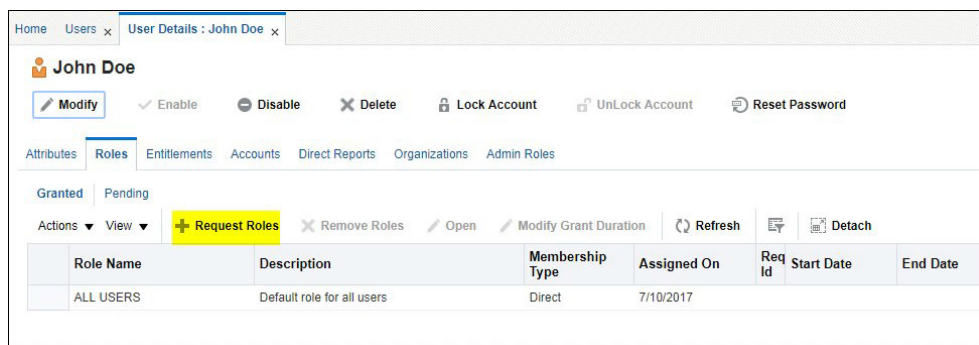
Note that the "*ALL USERS*" role has already been assigned to this user by default.



The screenshot shows the 'User Details' page for 'John Doe'. The 'Roles' tab is selected, and the 'Request Roles' button is highlighted in yellow. The table below shows the current role assignment.

Role Name	Description	Membership Type	Assigned On	Req Id	Start Date	End Date
ALL USERS	Default role for all users	Direct	7/10/2017			

- Click **Request Roles**.

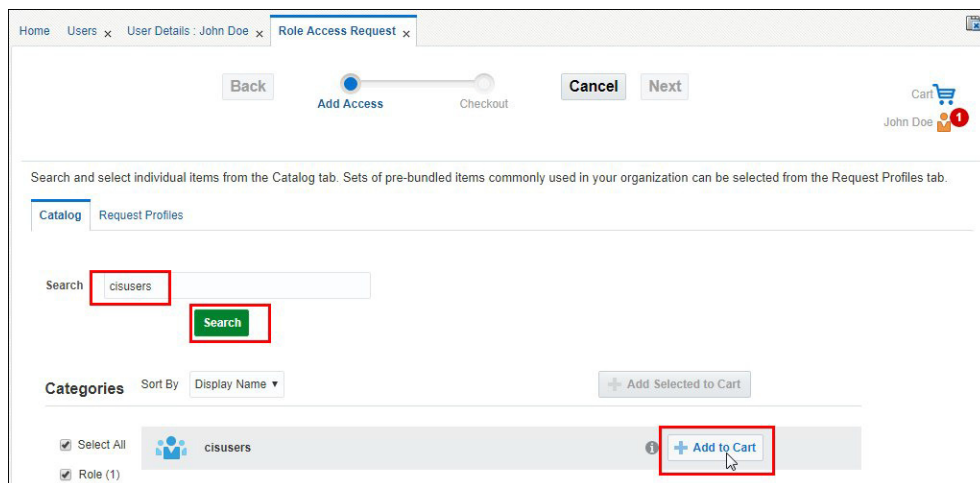


The screenshot shows the 'User Access Request' page for 'John Doe'. The 'Request Roles' button is highlighted in yellow. The table below shows the list of pre-defined roles.

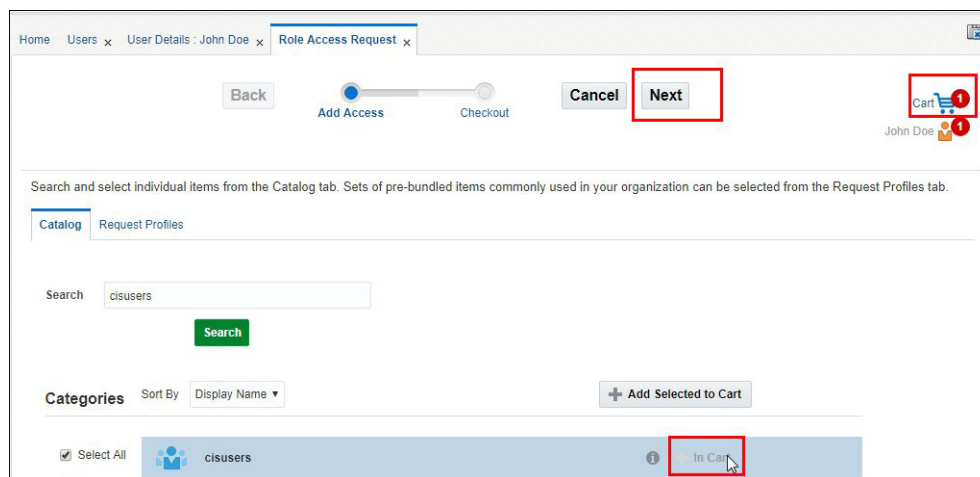
Role Name	Description	Membership Type	Assigned On	Req Id	Start Date	End Date
ALL USERS	Default role for all users	Direct	7/10/2017			

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**.

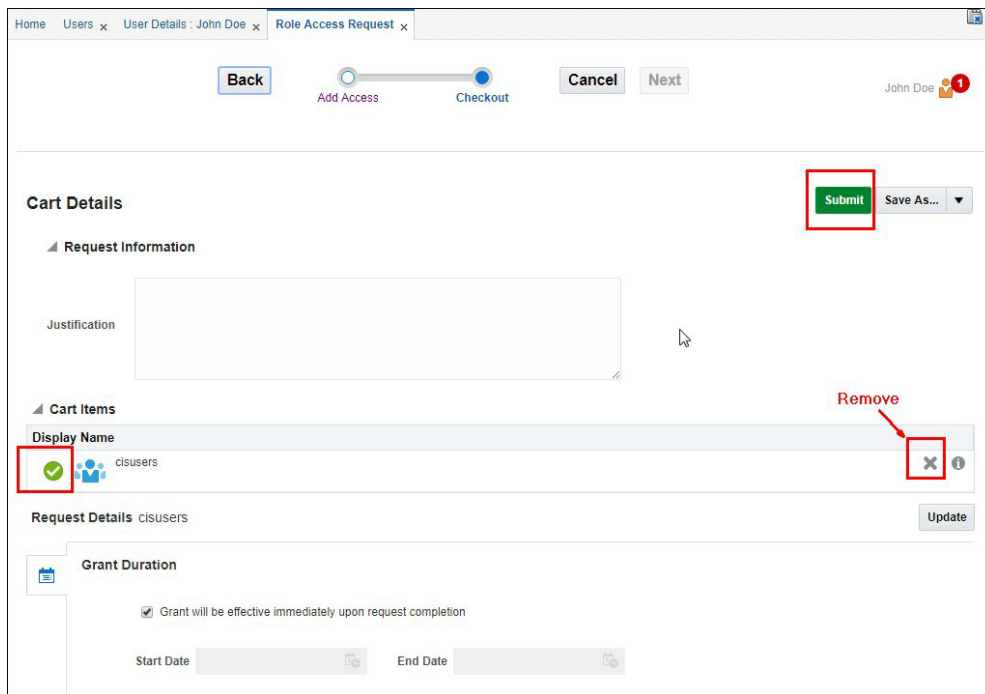


6. Review the request.

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

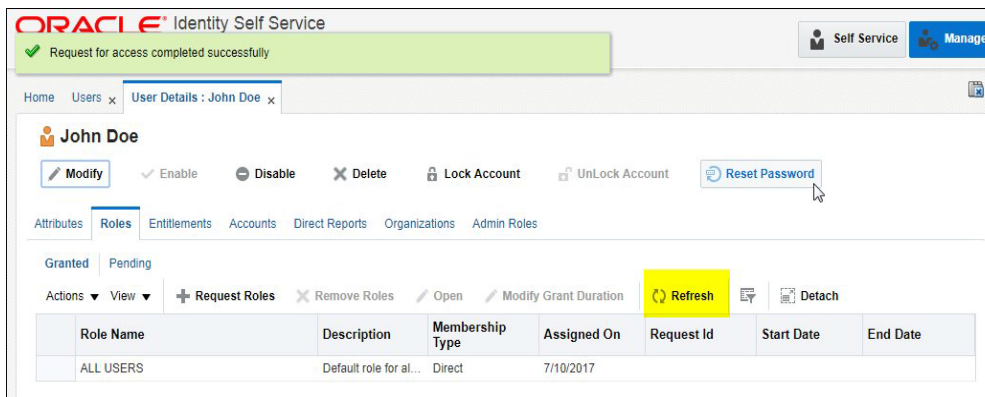
The **check mark** icon next to the role indicates that no additional information is required for the role assignment.

Click **Remove** to remove the role from the cart.

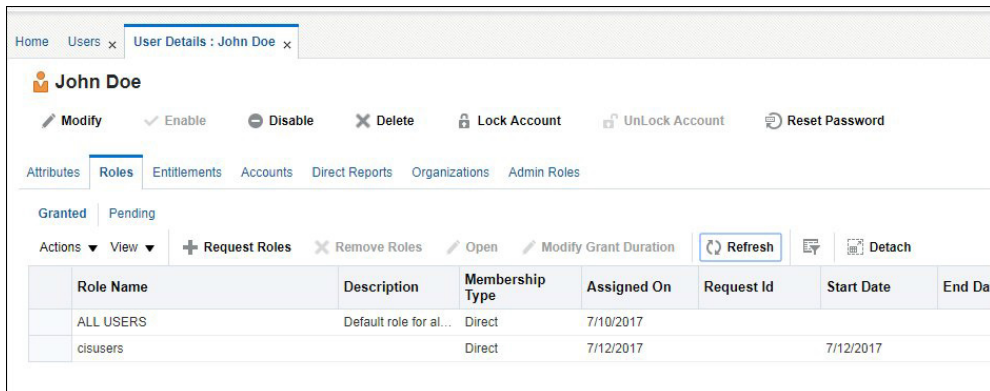


7. Click **Submit** to complete the request. You will be redirected back to the **Roles** tab on the **User Details** page.

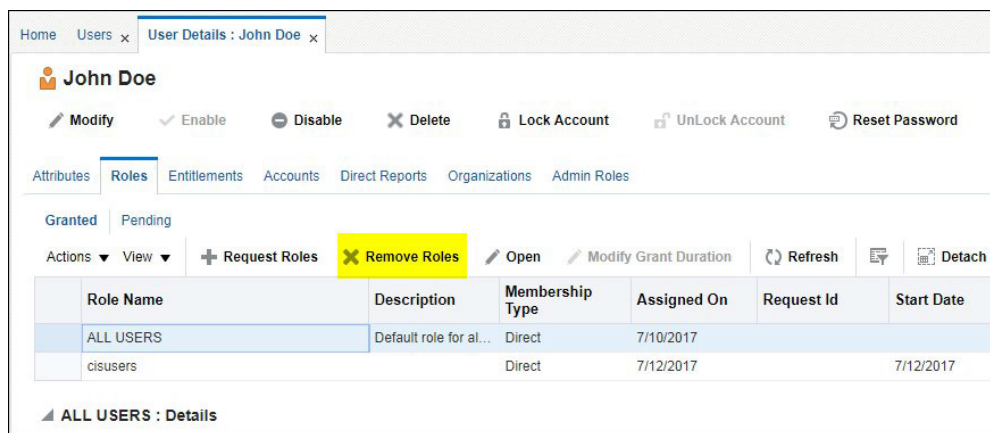
8. Click **Refresh**.



The new role appears on the list.



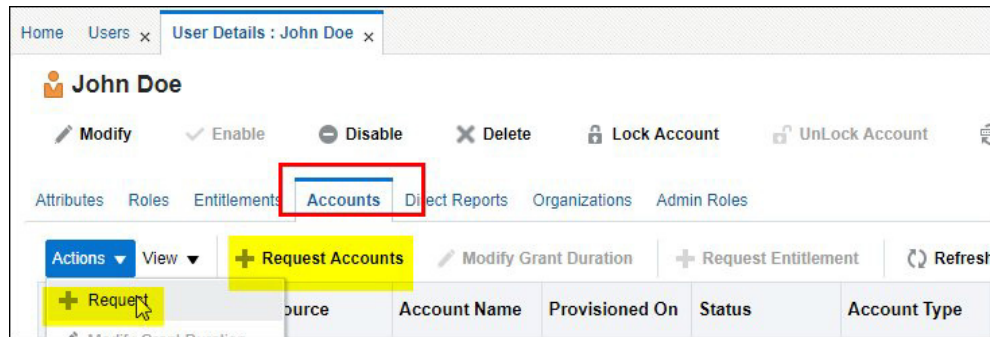
- Roles can be removed by selecting the role to be removed and clicking **Remove Roles**.



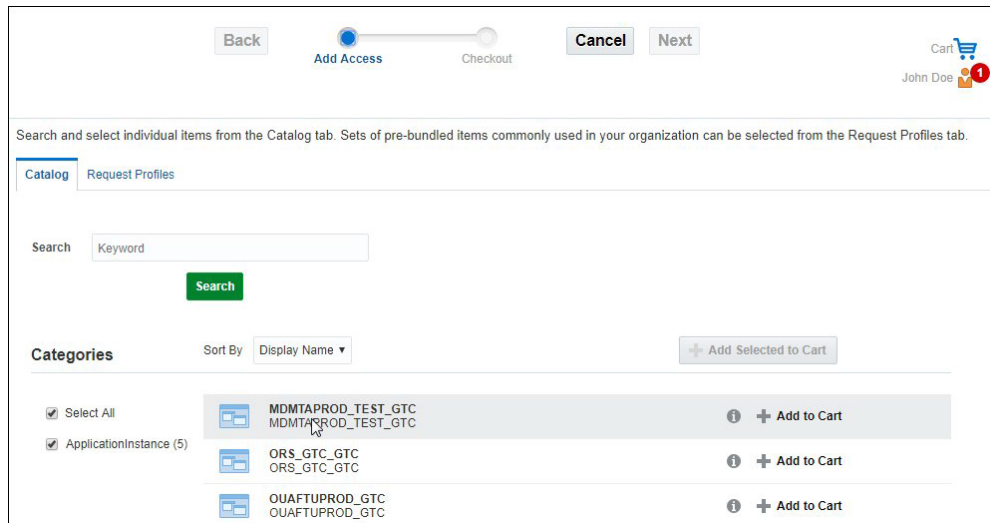
Provision Accounts

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

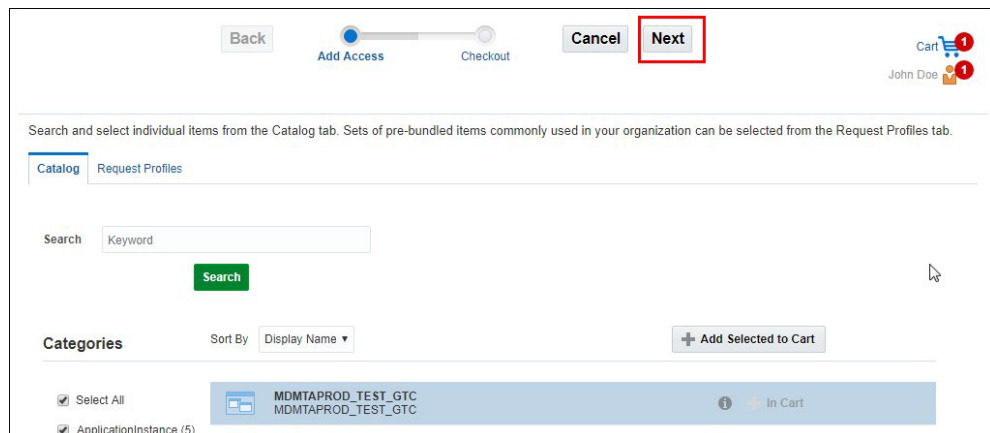
- Click on the **Accounts** tab.
- Click **Request Accounts** or select **Request** from the **Actions** drop-down list.



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.

Click **Remove** to remove the Application Instance from the cart.

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

The screenshot shows the 'Request Details' section of the 'Cart Details' view. At the top, there are navigation buttons: 'Back', 'Add Access', 'Checkout', 'Cancel', and 'Next'. The user's name 'John Doe' is visible in the top right. The 'Cart Details' section includes a 'Submit' button and a 'Save As...' dropdown. The 'Request Information' section has a 'Justification' field. The 'Cart Items' section shows a card for 'MDMTAPROD_TEST_GTC' with a warning icon. The 'Request Details' section shows 'MDMTAPROD_TEST_GTC' with an 'Update' button. The 'Grant Duration' section has a checkbox for 'Grant will be effective immediately upon request completion' and 'Start Date' and 'End Date' fields. A red box highlights the warning icon in the 'Cart Items' section and the 'Grant Duration' section.

- Populate the **Template** field with Template User name, which is the user record in the 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.

The screenshot shows the 'Request Details' section of the 'Cart Details' view. The 'Request Details' section shows 'MDMTAPROD_TEST_GTC' with an 'Update' button. The 'Details' section shows 'containerID', 'objectclass' (User), 'ID', 'template' (SYSUSER), and 'Service Account' fields. A red box highlights the 'Update' button and the 'template' field.

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

- Click **Submit** to complete the request

Cart Details

Request Information

Justification

Cart Items

Display Name	Resource	Account Name	Provisioned On	Status	Account Type	Request ID	Start Date
MDMTAPROD_TEST_GTC	MDMTAPROD_TEST_GTC	701	7/12/2017	Provisioned	Primary		7/12/2017

Request Details MDMTAPROD_TEST_GTC

Details

containerID

objectclass | User

- 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.

John Doe

Modify Enable Disable Delete Lock Account UnLock Account Reset Password

Attributes Roles Entitlements **Accounts** Direct Reports Organizations Admin Roles

Actions View Request Accounts Modify Grant Duration Request Entitlement Refresh Detach

Application Instance	Resource	Account Name	Provisioned On	Status	Account Type	Request ID	Start Date
MDMTAPROD...	MDMTAPROD...	701	7/12/2017	Provisioned	Primary		7/12/2017

The user can now successfully login to the target application.

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 user with high-level authorization access to all the services in the target application. It is recommended to setup additional Template Users with lesser privileges prior to creating and provisioning implementers, test and production users.

Verify User Access

As soon as the account is provisioned, the user should be able to login to the environment. Use the following procedure to verify the user's access:

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 the user provisioned in the previous steps in the Oracle Utilities cloud service application.

The screenshot displays the 'User' configuration page in the Oracle Utilities cloud service application. The page is titled 'User' and has a navigation bar with 'Home', 'Menu', 'Admin', and 'History'. Below the navigation bar are tabs for 'Main', 'To Do Roles', 'Access Security', 'Portal Preferences', 'Bookmarks', 'Favorite Links', 'Favorite Scripts', 'Characteristics', and 'Miscellaneous'. The 'Main' tab is active, showing the user's details for 'JOE'. The fields are as follows:

- User ID: JOE
- Login ID: JOHNDOE
- Last Name: Doe
- First Name: John
- Language: English
- Display Profile ID: NORTHAM (North America)
- Time Zone: (empty)
- Email Address: john.doe@company.com
- Dashboard Width: 200
- Home Page: CI0000000574 (User +)

Below the fields is a 'To Do Summary Age Bar' section with two input fields:

- Lower Age Limit for Yellow Bar: 50
- Upper Age Limit for Yellow Bar: 100

At the bottom, there is a table with the following data:

User Group	Expiration Date	Owner
ALL_SERVICES (System User Group)	01-01-2100	Customer Modification

Reset 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 screenshot shows the 'Users' list in the Oracle Utilities cloud service application. The page is titled 'Users' and has a search bar with 'Display Name' selected. The search results are as follows:

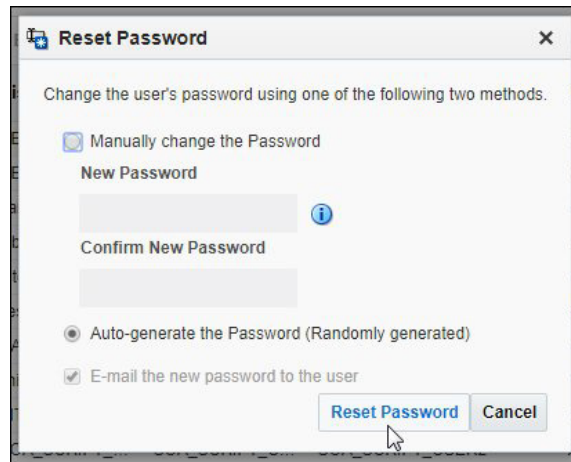
User Login	Display Name	First Name	Last Name	Organization	Telephone Number	E-mail
NEWUSR9	NEWUSR9 NE...	NEWUSR9	NEWUSR9	NEWU...

The 'Reset Password' option is highlighted in yellow in the 'Actions' column for the user 'NEWUSR9'.

The **Reset Password** window opens.

3. Select the appropriate option: Options include:
 - Manually change this Password
 - Enter and confirm the new password.

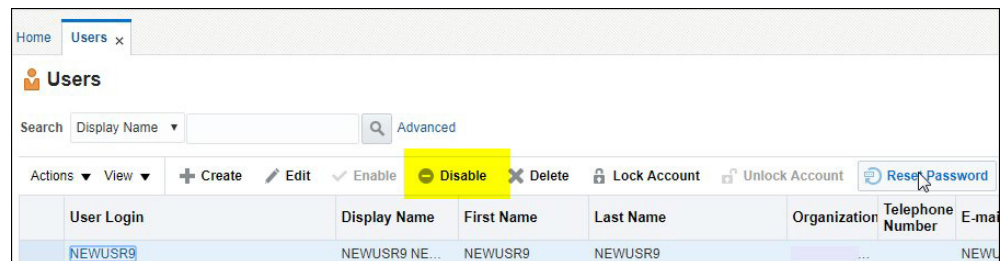
- Auto generate the password (Randomly generated)
4. Click **Reset Password**.



Disable User

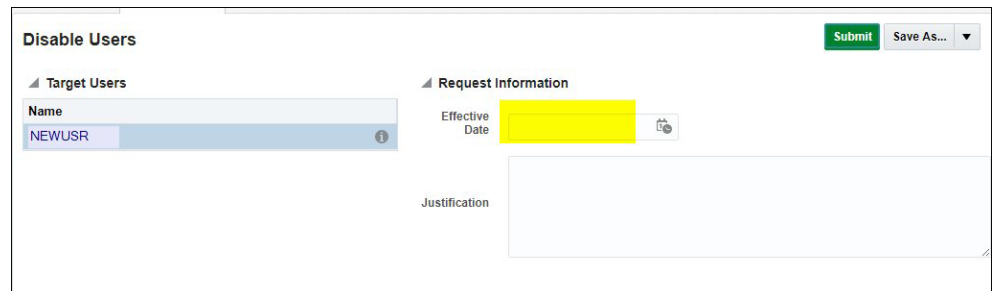
Use the following procedure to disable an active user.

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.

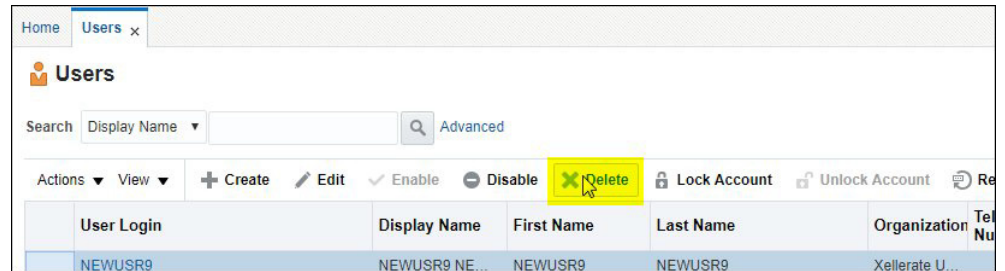


4. Click **Submit**.
5. Verify that the user is unable to login to the target environment.

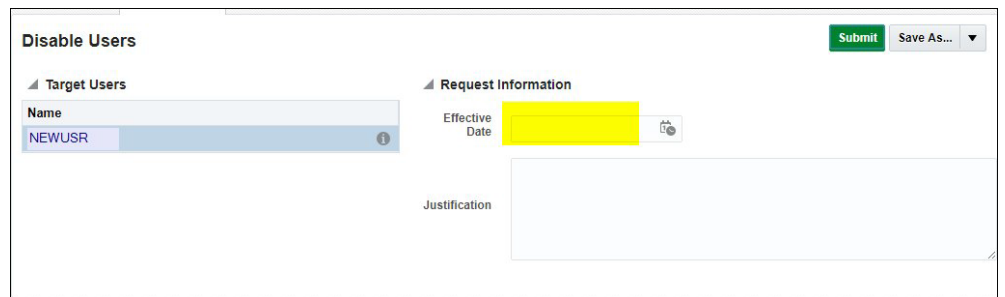
Delete User

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

This section outlines the different types of accounts you will create as a system administrator. 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:** this role provides users with access to one of the Oracle Utilities cloud services. Appropriate for both personal and integration/API accounts.
- **IntegrationAdmin:** this role provides access to Integration Cloud Connector services. Appropriate for integration accounts.
- **ExternalIntegrationUsers:** this role 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 Utility Analytics services. It typically includes three roles per product, with different authorization level:
 - **report author:** the role with highest authorization level that allows user to develop new reports
 - **analyst:** this role allows user to modify and run reports
 - **consumer role:** this 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. 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

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.

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

User	Roles	Accounts
CSF Integration User Login ID:	<ul style="list-style-type: none"> • IntegrationAdmin • cisusers 	Provision to <i>all available instances</i> of OUAF-based applications included in the subscription. Template User: <i>K1PAUSER</i>
<ul style="list-style-type: none"> • Alphanumeric • No more than 8 chars • No special characters 		

Integration Accounts

Integration accounts support web service communications between business applications within the subscription and with external systems. 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	<ul style="list-style-type: none"> IntegrationAdmin 	
Login ID:	<ul style="list-style-type: none"> cisusers 	
<ul style="list-style-type: none"> Alphanumeric 		
	<ul style="list-style-type: none"> External Integration Account (non-human) 	
<p>The credentials of this account are used by the messages sent to the SOA composites within the integration layer.</p>		

User	Roles	Accounts
External Integration User	<ul style="list-style-type: none"> ExternalIntegrationUsers 	
Login ID:		
<ul style="list-style-type: none"> Alphanumeric 		

Personal Accounts

Upon request, create and provision personal user accounts for Development, Test and later, Production 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	<ul style="list-style-type: none"> cisusers 	Provision to all applicable instances of the business application within the subscription.
Login ID:		Specify a Template User according to user's intended implementation or business role.
<ul style="list-style-type: none"> Alphanumeric No more than 8 chars No special characters 		

Chapter 2

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 Utility 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 Utility 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.

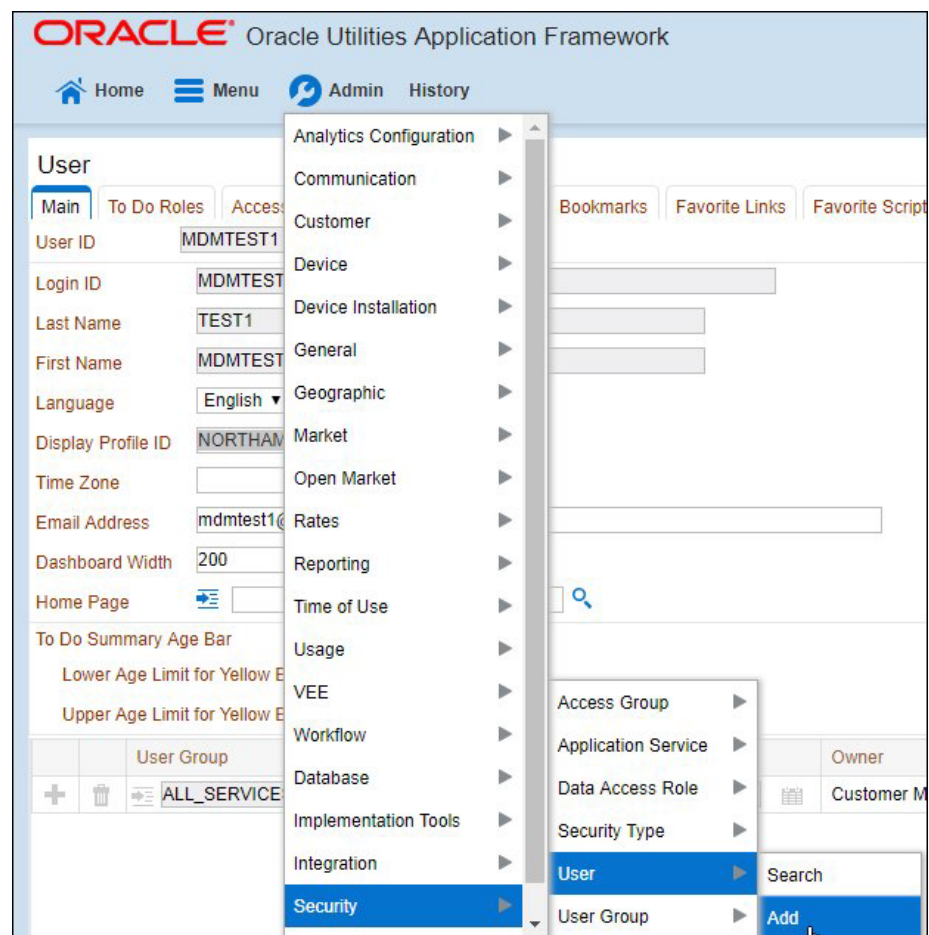
There are two possibilities to provide user with access to the target environment, depending on whether you maintain the local list of users in Oracle Identity Management.

User record created in Oracle Identity Management

- Login to the Oracle Identity Management and locate the user record. 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

- Login to each of the Oracle Utility product environments within the subscription, navigate to **Admin > Security > User > Add**, and manually add the user record.



- Make sure that the entry in the **Login ID** field is exactly matching 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 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 [Assign Roles](#) in Chapter 1.