Oracle Utilities Analytics Cloud Service

End-User Provisioning Guide

Release 17.1 E90910-01

January 2018



Oracle Utilities Analytics Cloud Service Release 17.1 End-User Provisioning Guide

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	
Introduction	
Prerequisites	
Confirm Access to Oracle Identity Management	
First Time Logging into Oracle Identity Management	
Initial Setup	
User Management Procedures	
Create a New User	
Provision Users	
Verify User Access	
Reset Password	
Disable User	
Delete User	
Accounts to Create	
Pre-Defined Roles	1-19
Available Accounts	1-19
Cloud Service Foundation Accounts	
Integration Accounts	
Personal Accounts	
Chapter 2	
Using Federated Single Sign-On	
Adding Oracle Utility Application Authorization	
User record created in Oracle Identity Management	
User Record is not created in Oracle Identity Management	
Supporting Role-based Authorization	

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 postprovisioning 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 Identify 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.

Access							
oles Entitle	ments Acc	counts Admin Roles					
Granted Actions 👻	°ending ∕iew ▼ =	Request Roles X Remo	ove Roles 🖉 Open 🎤 I	Modify Grant Duration	() Refresh	Ę	Detacl
Granted Actions V Role	Pending √iew ▼ = Name	Request Roles X Remo	Wembership Type	Modify Grant Duration Assigned On	(2) Refresh Request Id	Ę	Detacl
Granted Actions V Role ALL U	Pending √iew ▼	Request Roles Remo Description Default role for all users	Membership Type Direct	Modify Grant Duration Assigned On 5/16/2017	 ⟨) Refresh Request Id 	Gy (Detacl Start Date

6. If not yet assigned, request the role of cisusers 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 Identify 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

Home O	rganization x Organization : Subscriber x	
C Dis	sable 🌿 Create Sub-org 🕂 Create User 🗙 Delete s Children Members Available Roles Admin Roles Available Accounts Provisione	d Accounts Available Entitlements
View	▼ Č) Refresh 🔄 🖃 Detach	
	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.

Home Orga	nization × Organ	nization : Subscriber ×			C
Disable	e 🦓 Create Su	ib-org 🕂 Create Use	r 🗙 Delete		
Attributes	Children Membe	ers Available Roles A	dmin Roles Available Accounts Prov	isioned Accounts Available Entitlements	
View -	() Refresh	🔄 📄 Detach			
Acc	count Name		Description	Account Type	Organization Name
Tar	rget Environment_	GTC	Target Environment 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 Identify 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.

	Self Service		Self Service Manage
Home			
			E
Users Manage users	Roles Manage roles	Organizations Manage organizations	Administration Roles Manage admin roles
Policies Manage policies			

The Users tab opens.

4. Click Create.

ORACLE [®] Identity Self S	ervice			
Home Users x				
Search Display Name	Q Advance	d		
Actions 🔻 View 👻 🕂 Create 🧪 Ope	n () Refresh	Detach		
User Login	Dis <mark>play Name</mark>	First Name	Last Name	Orga

The **Create User** page opens.

5. Populate basic user information as shown below:

Create User				Submit	Save As
Request Information					
Effective Date	Ťœ				
Justification					
			11		
a Basic Information					
First Name John		Manager			0
Middle Name		* Organization	Subscriber Users		0
* Last Name Doe		* User Type	Employee		
E-mail john.doe@compa	any.com	Display Name			
Account Settings					
a Account cettings					
User Login JOHNDOE					
User Login JOHNDOE Password		0			
User Login JOHNDOE Password		0			
User Login JOHNDOE Password * Confirm Password		0			
User Login JOHNDOE Password * Confirm Password A Account Effective Dates Start Date	Ĕ	0			

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.

Home Users ×	
Search Display Name 🔻	Advanced
Actions View Create O	pen 🕻 Refresh 🔄 🖃 Detach
User Login	Display Name First Name
NEWHSDO	

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.

Provision Users

Provisioning is a process of defining 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.

- 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.

🟅 John Doe						
Modify V Enable	Disable X Delete	🔒 Lock Account 👩 Un	nLock Account) Reset P	assword	
tributes Roles Entitlements	Accounts Direct Reports Or	ganizations Admin Roles				
Granted Pending						
			a north	E	Detach	
Actions View Ree	uest Roles 🛛 🗙 Remove Roles	Open Modify Grant Du	Iration () Refresh	ΞŢ	Detuch	
Actions View Role Name	quest Roles X Remove Roles Description	Membership Type	Assigned On	Req S	Start Date	End Da

3. Click Request Roles.

🎽 John Doe						
Modify V Enable	🖨 Disable 🗙 Delete 🔒 L	ock Account	ock Account) Reset	Password	
ttributes Roles Entitlemen	ts Accounts Direct Reports Organizations	s Admin Roles				
Granted Pending						
Granted Pending Actions ▼ View ▼ 🕂 R	<mark>equest Roles</mark> 🗙 Remove Roles 💉 Ope	en 🧳 Modify Grant Dura	tion 🗘 Refresh	Ę	Detach	
Granted Pending Actions ▼ View ▼ 📲 R Role Name	equest Roles X Remove Roles Op	en 🖋 Modify Grant Dura Membership Type	tion () Refresh Assigned On	Req Id	Detach Start Date	End Dat

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.

Duck	Add Access	Checkout	Cancel	Next	Cart
	Aug Access	CHECKUL			John Doe
arch and select individual items from the Ca	italog tab. Sets of pre-bur	dled items commonl	y used in your or	anization can be selecte	ed from the Request Profiles tab.
atalog Request Profiles					
earch cisusors					
Search cisusers					
Search cisusers Search					
search cisusers Search					

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

Bac	k Add Access	Checkout	Cancel Next	Cart John Doe
earch and select individual items from th	e Catalog tab. Sets of pre-bun	dled items commonl	y used in your organization can be selec	ted from the Request Profiles tak
Catalog Request Profiles				
Search cisusers Search				

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.

me Users _× User [Details : John Doe 🗙	Role Access Request 🗙				[
	Back	Add Access	Checkout	Cancel	Next	John Doe <mark>२</mark>
Cart Details						Submit Save As 🔻
Request Information	mation					
Justification						
Cart Items				li.		Remove
Display Name						
O Cisusers	3					× 0
Request Details cis	users					Update
Grant Durat	tion					
	Grant will be effective i	mmediately upon request	completion			
22.0						

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

ome Us	sers x User Details : John Doe x						
🔓 Jol	hn Doe						
_	And the second se				in the second		
/ Mo	dify VEnable Disable	× Delete	Lock Account	UnLock A	count 🔊 Re	eset Password	
						13	
ttributes	Roles Entitlements Accounts Dire	ect Reports Organi	izations Admin Rol	es		143	
Attributes	Roles Entitlements Accounts Dire	ect Reports Organi	izations Admin Rol	les		6	
Attributes Granter	Roles Entitlements Accounts Directory difference of the second se	ect Reports Organi	izations Admin Rol	les		И	
Attributes Grantee Actions	Roles Entitlements Accounts Din d Pending • View + Request Roles	ect Reports Organi Remove Roles	izations Admin Rol	les lify Grant Duration	() Refresh	G Detach	
Attributes Grantee Actions	Roles Entitlements Accounts Direction d Pending a View	ect Reports Organi Remove Roles	izations Admin Rol	les	🗘 Refresh	Detach	

The new role appears on the list.

🍰 Je	ohn Doe								
/ N	Modify 🗸 Enable	Disable	🗙 Delete	Lock Account	UnLock Ac	count 🛒	Reset Pa	issword	
Attribut	tes Roles Entitlements	Accounts Dire	ect Reports Organiz	ations Admin Rol	es				
Gran Actio	nted Pending ons ▼ View ▼ + Requ	iest Roles 🗙	Remove Roles	Öpen 🧪 Mod	ify Grant Duration	Ç) Refresh	F	Detach	
Gran Actio	nted Pending ons ▼ View ▼ + Requ Role Name	est Roles 🗙	Remove Roles	Open Mod Membership Type	ify Grant Duration Assigned On	Refresh Request Id	st	Detach	End Da
Gran Actio	tted Pending ons ▼ View ▼ Pequ Role Name ALL USERS	iest Roles 🗙	Remove Roles Description Default role for al	Open Mod Membership Type Direct	ify Grant Duration Assigned On 7/10/2017	्रे Refresh Request Id	I St	Detach	End Da

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

🔓 John D	oe							
/ Modify	✓ Enable	Disable	🗙 Delete	Lock Account	UnLock Ac	count 🔊	Reset	Password
tributos Pol	-							
ROI	es Entitieme	nts Accounts I	Direct Reports Organiz	ations Admin Ro	bles			
Granted Pe Actions V	es Entitieme ending ew v + F	nts Accounts I	X Remove Roles	Open / Mo	dify Grant Duration	ζ) Refresh	Ę	Detac
Granted Pe Actions Vi Role N	ending ew v + F ame	nts Accounts I	Remove Roles	Open / Mon Membership Type	dify Grant Duration Assigned On	ζे Refresh Request Id	Ę	Detac Start Date
Granted Pe Actions Vi Role N ALL US	es Entitieme anding ew ▼ + F ame ERS	nts Accounts I	Remove Roles Description Default role for al	Open Mon Membership Type Direct	dify Grant Duration Assigned On 7/10/2017	⟨2 RefreshRequest Id	Ę	Detac

Provision Accounts

Provisioning allows user 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.

Home Users x User D	Details : John Doe 🗙					
🄓 John Doe						
nt Modify V E	nable 🔵 Disabl	e 🗙 Delete	Lock Ac	count	UnLock Acc	ount
Attributes Roles Enti	itlements Accounts	Di ect Reports	Organizations Ad	min Roles		
Actions View V	+ Request Account	s 🖉 Modify G	rant Duration	- Request	Entitlement	() Refresh
+ Requert	ource	Account Name	Provisioned On	Status	Acco	unt Type

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

	Back	Add Access	Checkout	Cancel	Next	C John I	Cart Doe
arch and select individual ite	ms from the Catal	og tab. Sets of pre-bu	ndled items common	y used in your org	anization can be	selected from the Request Profile	es tab
Search Keyword							
	Search						
ategories	Sort By Display	Name 🔻			- Add S	elected to Cart	
Select All	MDM	TAPROD_TEST_GTC			0	+ Add to Cart	
 ApplicationInstance (5) 	ORS ORS	_GTC_GTC _GTC_GTC			0	+ Add to Cart	
		FTUPROD_GTC			0	+ Add to Cart	

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

4. Click Next

	Back	Add Access	Checkout	Cancel	Next	J	Cart 📜 ohn Doe 🍟
earch and select individu	ual items from the Ca es	talog tab. Sets <mark>of pre-bu</mark>	ndled items common	y used in your or	ganization can be selected	from the Request P	rofiles tab.
Search Keyword	_						N
Categories	Search Sort By Disp	lay Name 🔻			+ Add Selected to	o Cart	43
Select All		DMTAPROD_TEST_GTC DMTAPROD_TEST_GTC			0 🕂 in (Cart	

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.

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

Back	Add Access	Checkout	Cancel Next	John Doe 👥
Cart Details				Submit Save As 🔻
Request Information				
Justification			<i>h</i>	
Cart Items				
Display Name				
MDMTAPROD_TEST_GTC MDMTAPROD_TEST_GTC				× 0
Request Details MDMTAPROD_TEST_GT	c 📩			Update
Grant Duration				
Grant will be effective imm	ediately upon request c	ompletion		
Start Date	io Enc	d Date	tio	

7. 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. Note that initially on the SYSUSER template is available. Additional template will become available as they are defined by the implementation or load from product or implementation accelerators. More Template Users might be created manually by Oracle Consulting.

Name and Address of the owned			
Jispiay Nan	ne		
	MDMTAPROD MDMTAPROD	TEST_GTC TEST_GTC	× 0
Request De	etails MDMTA	ROD_TEST_GTC	Npdate
	Details		
1	containerID		
	objectclass	ser	
	ID		
	template	YSUSER	
Ser	vice Account		

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

Cart Details	Submit Save As 🔻
A Request Information	
Justification	
Cart Items Display Name	
Cart Items Display Name MDMTAPROD_TEST_GTC MDMTAPROD_TEST_GTC	× 0
Cart Items Display Name MDMTAPROD_TEST_GTC MDMTAPROD_TEST_GTC Request Details MDMTAPROD_TEST_GTC	X C
Cart Items Display Name MDMTAPROD_TEST_GTC Request Details Details	X (Upda
Cart Items Display Name MDMTAPROD_TEST_GTC MDMTAPROD_TEST_GTC Request Details MDMTAPROD_TEST_GTC Details containerID	Vpdat

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.

	nin Doe							
/ M	odify 🗸 Ena	ble Oisab	le 🗙 Delete	Lock Acco	ount 🔐 Ur	nLock Account	Reset Passwor	rd
	-							
ribute	s Roles Entitle	ments Accounts	Direct Reports	Organizations Adm	in Roles			
	view -	Request Accoun	ts 📝 Modify G	rant Duration	- Request Entitle	ement () Refres	h 🕞 🖾	Detach
Action						Contraction of the second s		
Action								
Action	Application Instance	Resource	Account Name	Provisioned On	Status	Account Type	Request ID	Start Date
Action	Application Instance		Account Name	Provisioned On	Status Provisioned	Account Type	Request ID	Start Date

The user can now successfully login to the target application.

Notes on User Provisioning

- 1. 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.
- 2. 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.
- 3. 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.

Main To Do Rol User ID	Access Security	Portal Preferences	Bookmarks	Favorite Links	Favorite Scripts	Characteristics	Miscellaneous
Login ID	JOHNDOE						
Last Name	Doe						
First Name	John						
Language	English V						
Display Profile ID	NORTHAM	North America					
Time Zone	0						
Email Address	john.doe@company.co	om					
Dashboard Width	200						
Home Page	E CI000000574		Q User +				
To Do Summary Ag Lower Age Limi Upper Age Limi	ge Bar t for Yellow Bar	50					
User (Group		Expira	tion Date	Owner		
1 🔿 🖂 🗛		O O otrate a United Ora	01.01	2100	Customor Mod	fication	

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.

Home	Users x						
🔓 Us	ers						
Search	Display Name 🔻	Q Advance	ed				
Actions	s 🔻 View 👻 🕂 Create 🧪 Edi	t 🗸 Enable 🖨 D	Disable 🗙 Delete	🔒 Lock Account 🛛 🕤 U	Inlock Account) Reset Pass	sword
	User Login	Display Name	First Name	Last Name	Organization	Telephone Number	E-mai
1	NEWUSR9	NEWUSR9 NE	NEWUSR9	NEWUSR9			NEWL

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.

Reset Password		×
Change the user's password using	one of the following two	o methods.
Manually change the Passw	ord	
New Password		
	1	
Confirm New Password		
Auto-generate the Password	d (Randomly generated))
E-mail the new password to	the user	
	Reset Password	Cancel

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.

Home	Users ×					
🄓 Us	ers					
Search	Display Name 🔻	Q Advance	d			
Actions	s 🔻 View 👻 🕂 Create 🧪 Edi	it 🗸 Enable 🕒 🕻	<mark>)isable </mark> Delete	Lock Account	Unlock Account) ResexPassword
	User Login	Display Name	First Name	Last Name	Organization	Telephone E-ma
	NEWUSR9	NEWUSR9 NE	NEWUSR9	NEWUSR9		NEWU

3. Enter the Effective Date and Justification.

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

Disable Users				Submit Save As
Target Users		A Request Information		
Name		Effective	<u> </u>	
NEWUSR	0	Date	10	
		Justification		

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.

Home	Users _×				
Search	Display Name 🔻	Q Advance	d		
Action	s 🔻 View 👻 🕂 Create 🧪 Edit	🗸 Enable 🛛 🖨 🗖	isable Xgelete	🔒 Lock Account 📑	Unlock Account 🕤 Re
	User Login	Display Name	First Name	Last Name	Organization Tel
	NEWUSR9	NEWUSR9 NE	NEWUSR9	NEWUSR9	Xellerate U

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

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

Disable Users			Submit Save As 🔻
▲ Target Users	Request Information		
Name	Effective		
NEWUSR	Date	10	
	Justification		

- 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	•	IntegrationAdmin	Provision to all available
Login ID:	•	cisusers	<i>instances</i> of OUAF-based applications included in
• Alphanumeric			the subscription.
• No more than 8			Template User:
chars			KIPAUSEK
No special characters			

Integration Accounts

Integration accounts support web service communications between business applications within the subscription and with external systems. You should created 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	•	IntegrationAdmin				
Login ID:	•	cisusers				
• Alphanumeric						
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	•	ExternalIntegrationUsers	
Login ID:			
• 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	• cisusers	Provision to all applicable instances of the business
Alphanumeric		application within the subscription.
• No more than 8 chars		Specify a Template User according to user's
• No special characters		intended implementation or business role.

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 Utility products, 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.

	_ E Ora	Admin History	ation	Framework		
User ID Login ID Last Name First Name Display Profile ID Time Zone	Menu MDMTEST1 MDMTEST1 TEST1 MDMTEST English V NORTHAW	Analytics Configuration Communication Customer Device Device Installation General Geographic Market Open Market Batos	* * * * * * * * *	Bookmarks Fa	vorite Lin	ks Favorite Scrip
Dashboard Width Home Page To Do Summary A Lower Age Lim	200 The second	Reporting Time of Use Usage VEE	* * * *	Access Group	•	
User 4	Group	Workflow Database Implementation Tools Integration		Application Servic Data Access Role Security Type User		Owner Customer M Search
		Security	•	User Group	×	Add

- 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.