Oracle Financial Services Revenue Management and Billing Cloud Service, Premium Edition

OR

Oracle Insurance Revenue Management and Billing Cloud Service, Premium Edition

Version 5.1.0.0.0

Administration Guide

Revision 1.3

F82310-04

June 2023

ORACLE

Oracle Financial Services Revenue Management and Billing Cloud Service, Premium Edition/Oracle Insurance Revenue Management and Billing Cloud Service, Premium Edition Version 5.1.0.0.0 Administration Guide

Note: To improve the content readability, the above two products are collectively referred to as Oracle Revenue Management and Billing Cloud Service, Premium Edition throughout this document.

F82310-04

Hazardous Applications Notice

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.

Trademark Notice

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

Intel and Intel Inside 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, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

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.

Preface

About This Document

This document explains how to manage the user accounts and their access for Oracle Revenue Management and Billing Cloud Services (ORMBCS) using Identity and Access Management with or without identity domains on Oracle Cloud Infrastructure (OCI).

Intended Audience

This document is intended for the following audience:

- End-Users
- System Administrators
- Consulting Team
- Implementation Team

Organization of the Document

The information in this document is organized into the following sections:

Section No.	Section Name	Description
Section 1	Identity and Access Management	Describes how security administrators can set up user accounts for Oracle Revenue Management and Billing Cloud Services, manage end-to-end lifecycle of user identity, and govern user authentication in multiple business applications on OCI using IAM without identity domains.
Section 2	Object Storage Setup	Lists the various tasks that are required to connect the system to object storage on OCI using IAM without identity domains.
Section 3	Identity and Access Management with Identity Domains	Describes how security administrators can set up user accounts for Oracle Revenue Management and Billing Cloud Services, manage end-to-end lifecycle of user identity, and govern user authentication in multiple business applications on OCI using IAM with identity domains.
Section 4	Object Storage Setup with Identity Domains	Lists the various tasks that are required to connect the system to object storage on OCI using IAM with identity domains.
Section 5	Cloud Monitoring	Explains how to monitor Oracle Revenue Management and Billing Cloud Services.

Conventions

The following conventions are used across this document:

Convention	Meaning
boldface	Boldface indicates graphical user interface elements associated with an action, or terms defined in the text.
italic	Italic indicates a document or book title.
`monospace`	Monospace indicates commands within a paragraph, URLs, code in examples, text that appears on the screen or entered in the application.

Acronyms

The following acronyms are used in this document:

Acronym	Meaning
CLI	Command Line Interface
DEV	Development Environment
DR	Disaster Recovery
IAM	Oracle Identification and Access Management
IDCS	Oracle Identity Cloud Service
OCI	Oracle Cloud Infrastructure
OCI Console	Oracle Cloud Infrastructure Console
OCID	Oracle Cloud ID
ORDS	Oracle REST Data Services
ORMB	Oracle Revenue Management and Billing
ORMBCS	Oracle Revenue Management and Billing Cloud Services
OUAF	Oracle Utilities Application Framework
SSO	Single Sign On

Related Documents

You can see the following documents for more information:

Document Name	Description
Oracle Revenue Management and Billing Cloud Service, Premium Edition Frequently Asked Questions Guide	Lists various frequently asked questions (FAQs) regarding the implementation and operations of Oracle Revenue Management and Billing Cloud Services.
Oracle Revenue Management and Billing Cloud Service, Premium Edition Implementation Guide	Provides information on how to implement the Oracle Revenue Management and Billing Cloud Service.
Oracle Revenue Management and Billing Cloud Service, Premium Edition Operations Guide	Provides information regarding different types of service requests (SRs) customers can submit to the Oracle Revenue Management and Billing Cloud Operations team during implementation and operations of the Oracle Revenue Management and Billing Cloud Services.
Oracle Revenue Management and Billing Cloud Service, Premium Edition Live Operations Guide	Provides guidelines regarding live operations of Oracle Revenue Management and Billing Cloud Services.
Oracle Revenue Management and Billing Chatbot Configuration Guide	Explains how to integrate Oracle Digital Assistant (ODA) with the ORMB Cloud Service.
Oracle Revenue Management and Billing Chatbot User Guide	Explains how to use the menu based Chatbot introduced in the ORMB Cloud Service.
Oracle Revenue Management and Billing ML Integration Guide	Explains how to integrate Machine Learning (ML) with the ORMB Cloud Service for anomaly detection.

Access to Oracle Support

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

Change Log

Revision	Last Update	Updated Section	Comments
1.1	01-Aug-2023	Cover Page	Updated Information
		Copyright Notice	Updated Information
		Preface	Added Information
		Section 1.5.2: Pre-Defined Application Roles	Updated Information
		Section 1.5.4.5: Setting Up a User with Access to Analytics Publisher and Data Visualization	Updated Information

Revision	Last Update	Updated Section	Comments
		Section 1.6: Using Federated Single Sign-On	Added Section
		Section 2.1.2: Security and Access Management	Updated Information
		Section 2.1.2.3: Managing Users	Updated Information
		Section 2.3.3: Recommended Setup for Multiple Cloud Services	Updated Information
		Section 2.4: Initial Testing of Object Storage Connectivity	Updated Information
		Section 3.5.2: Pre-Defined Application Roles	Updated Information
		Section 3.5.4.5 Setting Up a User with Access to Analytics Publisher and Data Visualization	Updated Information
		Section 3.6: Using Federated Single Sign-On	Added Section
		Section 4.3.3: Recommended Setup for Multiple Cloud Services	Updated Information
		Section 4.4: Initial Testing of Object Storage Connectivity	Updated Information
1.2	27-Jul-2024	Section 1: Identity and Access Management	Added Hyperlinks
		Section 2: Object Storage Setup	Added Hyperlinks
		Section 3: Identity and Access Management with Identity Domains	Added Hyperlinks
		Section 4: Object Storage Setup with Identity Domains	Added Hyperlinks
1.3	08-Oct-2024	Preface	Updated Information

Contents

1. Identity and Access Management

This section provides instructions for Security Administrators to set up user accounts for Oracle Revenue Management and Billing 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, which includes:

- Identity and Access Management Overview
- Quick Start Guide
- Security Administrator Account
- User Management Procedures
- User Provisioning for Oracle Revenue Management and Billing Cloud Services

1.1 Identity and Access Management Overview

End user provisioning involves creating user records and granting appropriate access for users of Oracle Revenue Management and Billing Cloud Services.

This section provides instructions for Security Administrators to set up user accounts for Oracle Revenue Management and Billing Cloud Services, managing the end-to-end lifecycle for user identity, and governing user authentication in multiple business applications. Identity management tasks include creation of the user and user group records, granting users and groups an access to the target business applications, and managing various security settings.

This section also introduces working with Oracle Identity Cloud Service. Identity Cloud Service is provisioned to customers with subscriptions to Oracle Revenue Management and Billing Cloud Services. Customers receive an instance of Identity Cloud Service (also referred to as Identity Cloud Service tenancy). The tenancy is managed exclusively by the customer (see Identity Cloud Service Tenancy for more information).

1.1.1 Identity Cloud Service Tenancy

Identity Cloud Service tenancy is provided to the customer as part of the service subscriptions. The following configurations are defined in Identity Cloud Service:

- **Application**: In Oracle Revenue Management and Billing Cloud Services, the application represents a single environment, Production, or non-Production. Applications are created by the subscription provisioning process.
- **Application Role**: In Oracle Revenue Management and Billing Cloud Services the Application Role represents an entitlement to access a component within the environment. Assigning user to an Application Role provides this user with access to this component. Application Roles are created by the subscription provisioning process.
- **User**: Users represent a human or non-human entity that is accessing the environment. User records are created and managed by the Security Administrator.
- **Group**: Groups comprise of one or more users. Groups are created and managed by the Security Administrator.

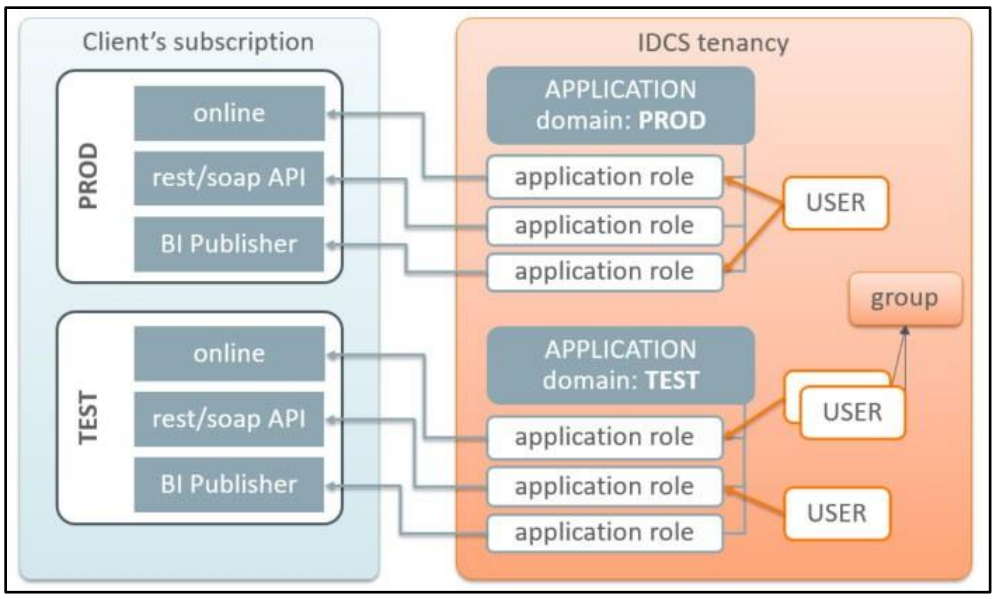

Figure 1: Identity Cloud Service Tenancy

1.2 Quick Start Guide

This section provides an overview of the initial set up of your cloud server user community. It contains the following topics:

- Activate Security Administrator Account
- Adjust the Default Oracle Identity Cloud Service Settings
- Prepare User Community
- Setup Process Summary

1.2.1 Activate Security Administrator Account

Access the Oracle Identity Cloud Service (IDCS) Admin console and perform the verification of the provisioned environments. Follow the steps described in the Security Administrator Account section.

1.2.2 Adjust the Default Oracle Identity Cloud Service Settings

Modify Oracle Identity Cloud Service (IDCS) settings as follows:

- Define your user naming conventions: decide whether the primary email address will be also used as a user name (login).
- You may want to include user name in the communication emails. Update notification(s) accordingly (see Notification Update Example: Welcome Email for an example of updating notifications).
- Update the notifications further to include additional details, for example the contact information of the technical support team.
- Evaluate the default Password Policy and amend according to your organization's requirements.
- Customize the look of the IDCS login page with your company's branding elements (optional).

For more information, see Updating Settings.

1.2.3 Prepare User Community

Explore the Users list. Beside the Security Administrator account you may find a Process Automation user. This is created as part of the service provisioning and usually linked to the Security Administrator's email address. Process Automation is an internal user for inter-domain communications.

Take advantage of the IDCS's user import feature to quickly establish user access to the provisioned environments, using the following steps:

- Determine the list of users who'll be accessing the provisioned environment(s):
    - Provide access to the non-production environments for key members of the implementation team
    - Provide access to the production environment users
- Define IDCS Group(s) for Just-In-Time Provisioning (if required). See Setting Up Groups for Provisioning - Identity Cloud Service for more information).
- Browse the IDCS Applications and determine Application Roles that users will be assigned to.
- Download the bulk upload template files from IDCS and create import files for:
    - Users
    - Groups
    - Application Roles

  See Bulk Upload and Download for more detailed information about uploading and downloading template files.

1.2.4 Setup Process Summary

Note that the following assumes the Security Administrator account has been activated.

- If you wish to delegate the just-in-time provisioning and access/authorization setup, assign the IDCS administrator role to at least one user per environment (see Updating Security Privileges).
- Access the environment and configure Just-In-Time provisioning according to the product's specifications (see Configuring User Provisioning Rules - OUAF).
    - For example, setup the IDCS Integration Master Configuration for ORMBCS. Make sure the IDCS Groups are the same Groups that were used for the User/Group import files.
- Perform import of Users, Groups and Application Roles using the import files prepared above (see Bulk Upload and Download).
- Setup at least one integration (non-human) user per environment of ORMBCS and communicate the credentials to the implementation team (see Setting Up an Integration User for REST/SOAP Web Services).
- Setup access to production environment for those users who are responsible for legacy data migration.

1.3 Security Administrator Account

This section explains how to set up a security administrator account for user provisioning. It contains the following topics:

1.3.1 Setting Up the Security Administrator Account

The account for the Security Administrator is created during the tenancy provisioning. The customer provides the name and the email address of the intended security administrator as part of the service order. Once the order is completed the Security Administrator receives a cloud account activation email. The activation email contains:

- Activation URL
- The user name and the temporary one-time password

Security administrators should use the following procedure the first time logging into the **Oracle Cloud Account Portal**:

1. Press the activation link or copy the link into the internet browser's address.

   You will be redirected to the login page.
2. Enter the user name and the temporary password.
3. Follow the prompts to create a new permanent password.

   Finally, you will be redirected to the **Oracle Cloud Account Portal** dashboard.

1.3.2 Navigating to the Identity Cloud Service Admin Console

The Identity Cloud Service Admin Console can be accessed either directly or via Cloud Account Portal.

1.3.2.1 Accessing via Cloud Account Portal

On the **Oracle Cloud Account Portal** dashboard, click **Users** in the top right corner of the screen. On the **Users** tab, click **Identity Console**. You'll be redirected to the **Identity Cloud Services** console. Click the menu icon at the left top corner to expand the left-side navigation pane.

1.3.2.2 Accessing Identity Cloud Services Admin Console Directly

After navigating to the Admin console for the first time you can copy the URL from the internet browser address bar and bookmark it for the further use. The URL is structured as follows:

`https://<tenancy>/ui/v1/adminconsole`

Where, `<tenancy>` represents the instance of the IDCS that belongs to the customer's subscription. In this scenario the user is re-directed to the **Identity Cloud Services** admin console dashboard. Use the menu icon on the left top corner to expand the navigation pane. You can also browse various help topics listed in the upper section of the page.

1.3.3 Verifying Security Administrator Identity Cloud Service Access

Expand the **Security** topic on the navigation pane and click **Administrators**.

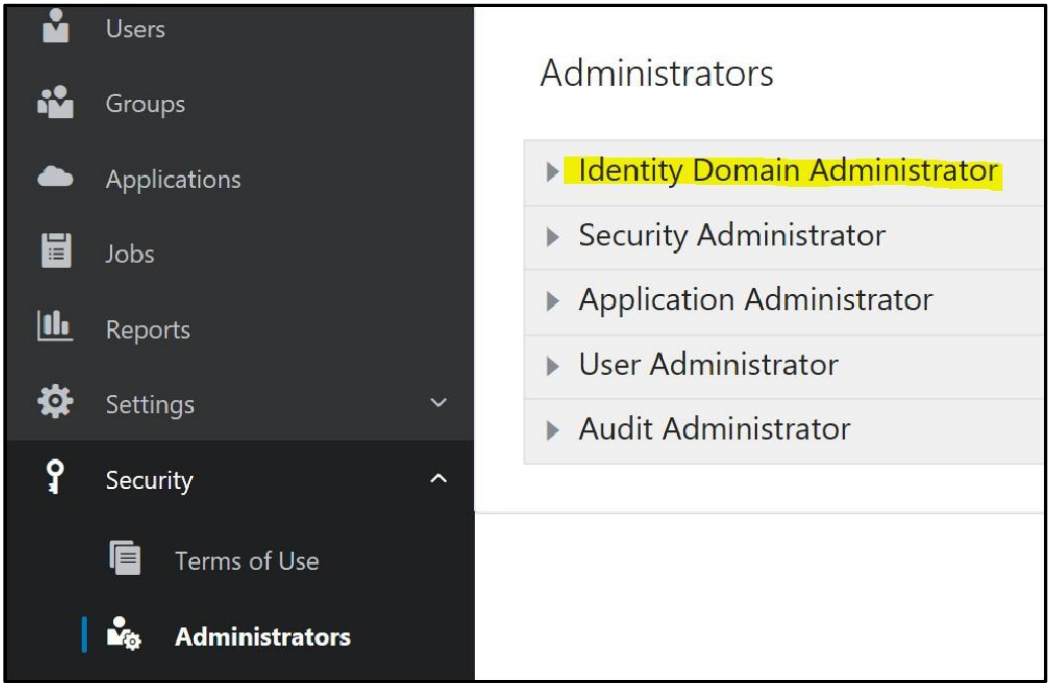

Figure 2: Administrators Section

On the page, click **Identity Domain Administrator** and verify that your name is on the list of Identity Domain Administrators.

1.3.4 Verifying Subscription Contents

Click **Oracle Cloud Services** (**Applications** in earlier versions) on the navigation pane. The main panel displays a list of available applications.

Each Application in represents an environment, for example Production or Test.

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.

The list of applications may also include an instance of Oracle Cloud Object Storage.

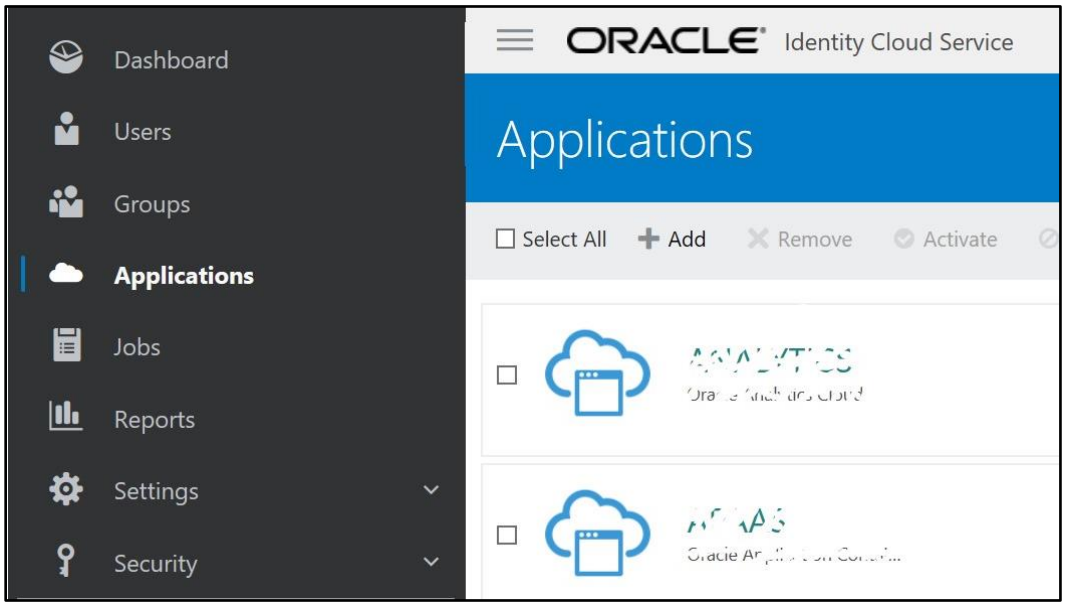

Figure 3: Applications

1.3.5 Exploring the Applications

Click on one of the applications on the list and display the single application. Most of the information is system-generated and read-only. Users and Groups should be assigned to Application Roles within the application to gain access to the environment.

Click the **Application Roles** tab and review available Application Roles. While the application represents a single environment, the different Application Roles represent different components within the environment. To authorize user's access to a certain component the user has to be assigned to a corresponding Application Role. Application Roles include:

- Online Application Access
- Web services REST/SOAP API
- Access to supporting Applications such as Analytics Publisher and SQL Developer Web

Application Roles also used to support coarse-grained authorization in the target component, for example the BI Content Author versus an ordinary BI Consumer.

1.3.6 Verifying Access to Object Storage

See the Object Storage Setup section for more information about object storage.

1.3.7 Verifying Security Administrator Access to Service

As part of the service activation notifications, the security administrator is provided with URLs for all components within Production and Non-Production environments.

Perform the following steps to verify the access:

- Assign the security administrator user to online-related Application Roles in all environments (Application Role description indicates whether the access is given for online or for the REST/SOAP API)
- Try to access the URLs for the online applications

1.4 User Management Procedures

This section describes general procedures related to managing users and groups. It contains the following topics:

- User Onboarding - My Services Portal
- Advanced User and Access Management - Identity Cloud Service Admin Console

1.4.1 User Onboarding - My Services Portal

The basic user access management operations can be performed directly on the **My Services** portal on the **Oracle Cloud Account Portal**. The link to the **User Management** portal is located on the upper navigation bar.

Note: My Services portal might not be applicable for all the scenarios, in most of the cases user access management operations needs be performed in Oracle Identity and Access Management, see the User Onboarding section for the same.

1.4.1.1 Setting Up a New User

Click **Add** on the **Users** tab of the **User Management** portal to set up a new user.

Add User Details

Enter the minimum required information:

- Last Name
- First Name
- Email address

Note: By default, the email address is used as the user name. Uncheck **Use Email as User Name** to enter the User Name manually.

- User Name

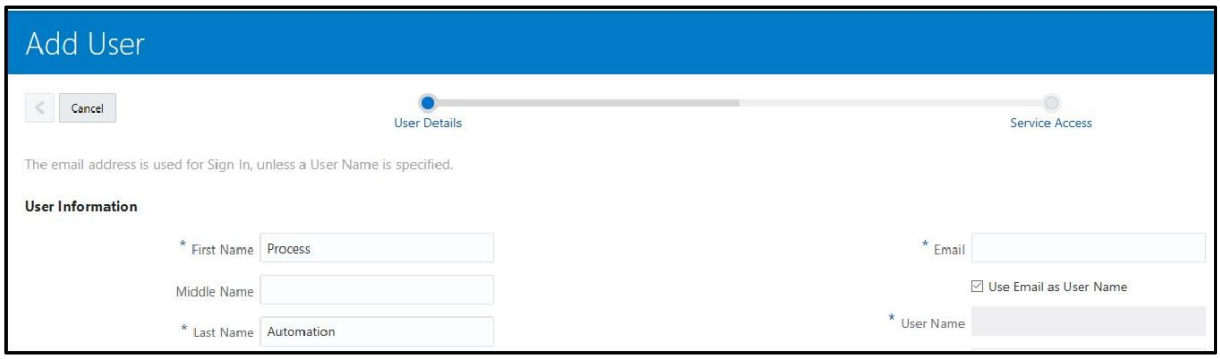

Figure 4: Add User

Click **Next** to set up the user's Service Access.

Define Access to Service

The **Service Access** page displays a list of environments and services. Locate the environment in the list or use Search to filter out a specific environment. To add one or more roles for an environment, click on the field beneath the environment's name.

Figure 5: Service Access

To add all available roles at once click **Add User Roles**. Click **Finish** button to complete the setup. The new user appears on the **User Management** portal.

Note: Additional product-specific setup may be required in order to provide user authorization and Just In Time provisioning. For more information, see User Provisioning for Oracle Revenue Management and Billing Cloud Services.

1.4.1.2 Setting Up a New Security Administrator

The new security administrator is configured as follows:

- Add new user record as shown above
- Grant administrative role(s) to the new user.

Cloud Account Administrator

The Cloud Account administrator can manage every aspect of the subscription including but not limited by Identity Cloud Service administration. The Security Administrator is assigned this role. To grant the same privileges to the new user:

- Filter the services list Cloud Account service on the list
- Select the Cloud Account Administrator role.

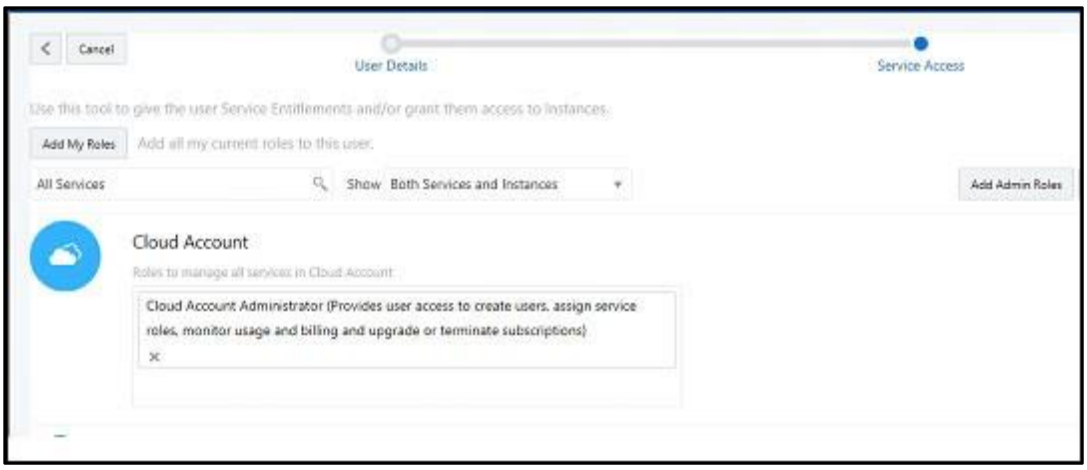

Figure 6: Cloud Account Administrator

Identity Administrator

Identity administration roles authorize users to manage configurations and administer Identity Cloud Service. There are various level of access:

- User Administrators are allowed to create and manage users and groups.
- The Application Administrator role is limited to the Application configuration and lifecycle.
- Audit and Security Administrator roles provide access to basic security settings and Identity-related reports.
- The Identity Domain Administrator role includes all the above.

To grant user the administrative role in Identity Cloud Service:

- Filter the services list and locate an Identity Cloud service.
- Select one or more roles from the list or click **Add Admin Roles** to add all available roles at once.

1.4.1.3 Updating or Removing a User

User records are displayed on the **User Management** portal.

Update User Details

To update details for a user, double-click the user or click on the action menu icon to open the user record and update the user information as appropriate.

Note: First and Last names are editable. The email address is editable only if not used as user name (login).

Update Access to Service

To update the access a user has to services, modify the existing user's access to services by adding or removing roles.

Remove User

To remove a user, click **Remove** from the menu.

Note: Removing a user is irreversible.

1.4.1.4 Defining User Group Membership

Select one or more user records and the multi-record actions became available:

- **Add to Group**: Adds selected users to an existing group
- **Create New Group**: Creates a new Group and adds the selected users to it
- **Clear Selections**: Deselects selected users

Figure 7: User Management

1.4.1.5 Managing Groups

Click the **Groups** tab on the **User Management** portal. The portal displays a list of all available group.

Add New Group

To add a new group click **Add**. Enter the **Group Name** and **Description** and save the new group.

Add Users

To add users to a group, click on the group name on the list or use the Edit menu action. The portal displays the selected group record.

Click the **Users** tab, then click **Add Users** to add one or multiple users to the group.

Group Access to Service

Click the **Roles** tab. The access setup steps are like setting up an individual user's access.

The portal displays a list of available environments and services. Filter the list and assign group to one or more roles.

To setup a group with administrator privileges, locate Identity Cloud on the list and add one or more administrative roles to the group.

1.4.2 Advanced User and Access Management - Identity Cloud Service Admin Console

Use the **Identity Cloud Service** admin console to manage applications, perform user management and administer general and security settings also view basic reports.

1.4.2.1 Managing Users

Users can be added and maintained via **Identity Cloud Service** admin console. Access the **Users** portal from the **Identity Cloud Service** admin console dashboard or from the navigation bar. To add a new User, click the **+Add** button and populate the required user details. On the next screen you can also immediately add user to one or more Groups. In addition to add and remove, the following multi-record actions are available on the **User** page:

- Resend Invitation
- Reset Password
- Activate/Deactivate User
- Update User information and preferences (on individual User record)
- Unlock User (on individual User record)

Resend Invitation to Service

The initial email invitation to access the service is sent to the user immediately upon user record creation. This invitation is expired after certain period.

Reset Password

Resets a single, multiple, or all passwords. Users will receive a password reset email notification immediately.

Activate/Deactivate User

User can be temporarily activated or deactivated. The email notification is sent to the user immediately. If the deactivation lasts longer than the password rotation period, the activation will cause password reset.

Update User Information and Preferences

Updates details for individual users. In addition to the minimum required information provided during user creation the following details can be updated:

- Title
- Time Zone and Address including Country
- Preferred language
- Alternative email and contact information

Unlock User

Unlocks a locked user account. The user's account may be locked for various reasons for example after too many unsuccessful login attempts.

Select **Unlock User** from the **More** menu to unlock the locked account.

1.4.2.2 Managing Groups

Users and groups can be added and maintained using the Identity Cloud Service admin console. Access the **Groups** portal from the Identity Cloud Service admin console dashboard or from the navigation bar. Select one or more entries from the list. In addition to add and remove, the following actions are available:

- Import Groups
- Export Groups

1.4.2.3 Managing Applications

The applications that represent the provisioned services are pre-created during the service order processing. The Application Roles are also pre-configured.

The administrator is authorized to activate or deactivate certain applications, assign users to Application Roles, and perform import and export of application role's members.

1.4.2.4 Bulk Upload and Download

IDCS supports import and export of users, groups, and application roles membership. The bulk identity data operations may be required for the fast user onboarding or as part of the federated single sign on setup. The **Import** and **Export** actions are available on multiple Admin Console pages:

- **Users** page:
  - Import all or a selected set of users
  - Export information for one or more users
- **Groups** page:
  - Import all or a selected set of groups and their member users
  - Export one or more groups and their member users
- **Application** > **Application Roles** page:
  - Import all or a selected set of application role's membership (users and groups)
  - Export one or more application role's membership (users and groups)

Importing

1. Navigate to the **Users**, **Groups**, or **Applications** (**Application Roles** tab) page as appropriate.
2. Click **Import** on the top actions bar.
3. Download the sample file.
4. Review the sample file. Note that you can provide different type of information:
   - Users
   - Groups
   - Application Roles Membership
5. Populate the file with user's data and save.
6. Import the file into Identity Cloud Service.

Exporting

1. Navigate to the **Users**, **Groups**, or **Applications** (**Application Roles** tab) page as appropriate.
2. Select entries for the export.
3. Click **Export** on the top actions bar. A notification email is sent as soon as the export job is completed, and the file is available for the download.

1.4.2.5 Updating Settings

Use the navigation bar to expand the **Settings** topic. The following settings can be modified:

- **Default Settings**: Used to manage default time zone, language, and audit setup.
- **Session Settings**: Used to manage session expiration.
- **Password Policy**: Used to amend the default password policy according to your requirements.
- **Notifications**: Used to modify the default email notification templates provided with Identity Cloud Service.

Notification Update Example: Welcome Email

The email notification templates are provided for multiple identity management-related events. The default content of these notifications can be amended to reflect customer's business requirements.

For example, there are two approaches to user account creation: using email address as a user name as opposed to using a manually defined user name. The former means the user knows what to specify on the login screen (email address). The later means the user name that is created manually by the security administrator has to be communicated to the user. In order to communicate the **user name** in the **Welcome** email perform the following steps:

- Select **Notification** on the left-side navigation bar.
- Click on the **Email Templates** tab.
- Expand the **Welcome** template:
  - In the email body, the greeting line reads: `Hello ${user.displayName}`
- Modify the greeting to include the user name (login) as follows:

```
Hello ${user.displayName} (${user.userName})
```

Note that other substitution variables are also available for use in the notifications. To explore the variables available to a specific template, click the **Email Variables** link above the email body editor.

1.4.2.6 Updating Security Privileges

Use side navigation panel to expand the **Security** topic. Use **Administrators** link to add or remove administrative privileges from the users.

1.4.2.7 Sign-On Policies for Online Access

IDCS supports the ability to restrict web-browser-based access to the applications based on set of conditions including the user's client IP addresses. Both IP "blocklist" and "allowlist" approaches are supported:

- A blocklist defines a set of IP addresses that are blocked from the access. This approach should be used when the "bad" IPs are well-known and permanent, and the list is not expected to change very often.
- An allowlist defines the set of IP addresses that are permitted to access the application while everybody else is denied access.

In addition to IP addresses the following can be allowed or blocked:

- Specific users
- Groups
- User's administrative role in IDCS
- User being authenticated by a specific external identity provider(s)

Note: Sign-On Policies are applied ONLY when user attempts to authenticate to IDCS using a web browser. They are not applicable for requests submitted via REST/SOAP API.

Setup a Network Perimeter

A Network Perimeter represents a set of IP addresses, and can be defined as:

- A list of one or more IP addresses
- A range of IP addresses
- One or more IP addresses in IPv4 CIDR notation, which encompass all IP addresses belonging to a subnet. You can also use the IPv4 CIDR notation to see the entire internet: 0.0.0.0/0.

Create Network Perimeters:

- Use side navigation panel to expand the Security Topic
- Locate Network Perimeters
- Add one or more Network Perimeters that define "blocklist" and/or "allowlist" IP addresses

Setup Sign-On Policies

Sign-on policies define the set of rules used for granting the access to the applications. The out-of-box default policy contains a single default rule that grants the access to every authenticated user. You can either modify the default policy or create a new one(s).

Sign-on policy rule definition includes multiple optional conditions to filter the users and an action to **allow** or **deny** the access:

- By authenticating the Identity Provider: Denying/allowing access for users authenticated by specific external IP in case of a federated SSO
- By group membership: Denying/allowing access for specific set of groups
- By being or not being an IDCS administrator
- By being one of the explicit lists of users
- By the user client's IP address being in one or more of the Network Perimeters

The rules on the policy are evaluated top-to-bottom. The first result halts the evaluation. Meaning if the user satisfies the rule's condition, the rule's action (**allow** or **deny** access) is applied and evaluation ends.

Note: The default rule on the default policy cannot be deleted, therefore it must be modified first.

Example:

Let's assume that the requirement is to:

- Allow access from IP addresses on the company's intranet
- In addition, allow certain administrators to connect from their personal home computers

- Block anyone else

To configure this example:

- Create two new Network Perimeters:
  - **NP1-Company** to represent the intranet: specify an entire subnet using CIDR notation, like, for example, 10.10.0.1/24, which means all addresses in 10.10.0 subnet
  - **NP2-Admins**: specify one or more IP addresses, comma-separated
- Configure Default Sign-On Policy:
  - Modify Default Rule:
    - Set the rule's "and the user's client IP address is" condition to "in one or more of these network perimeters" and specify **NP1-Company**
    - Set the rule's action to "**Allowed**"
  - Add new Rule:
    - Set the rule's "*And is an administrator*" condition to "true"
    - Set the rule's "*and the user's client IP address is*" condition to "*in one or more of these network perimeters*" and specify **NP2-Admins**
    - Set the rule's action to "**Allowed**"
  - Add new Rule:
    - Set the rule's "and the user's client IP address is" condition to "Anywhere"
    - Set the rule's action to "**Denied**"

Sample Sign-in Scenarios:

Scenario 1:

An employee is trying to login from the office computer that is connected to the intranet.

- The first rule (the default rule) is evaluated first. The user's IP satisfies the condition by being on the NP1-Company perimeter. The rule's action ("*Allowed*") is applied, and the user is allowed to sign in.

Scenario 2:

The administrator is trying to login with admin's user name from a personal computer whose IP is listed in NP2-Admins perimeter.

- The first rule (the default rule) is evaluated first. The user's IP does not satisfy the condition by being on the NP1-Company perimeter.
- The second rule is evaluated. The user's IP does satisfy both conditions: being and administrator and being on the Np2-Admins perimeter.
- The rule's action ("*Allowed*") is applied, and the user is allowed to sign in.

Scenario 3:

The employee is trying to connect from the home computer.

- The first rule (the default rule) is evaluated first. The user's IP does not satisfy the condition by being on the NP1-Company perimeter.

- The second rule is evaluated. The user's IP does not satisfy any of the conditions: being neither an administrator nor being on the Np2-Admins perimeter.
- The third rule is evaluated. The user's IP satisfies the "Anywhere" condition.
- The rule's action ("*Denied*") is applied and the sign in is blocked. The IDCS login error message: "Sign-on policy denies access." is displayed.

See *IDCS Documentation* for the detailed instructions regarding Sign-On Policy and Network Perimeter setup.

1.4.2.8 Available Reports

The following **Identity Cloud Service** reports are available for review and download:

- Successful Login Attempts
- Unsuccessful Login Attempts
- Application Access
- Granted and Revoked Application Roles

1.5 User Provisioning for Oracle Revenue Management and Billing Cloud Services

This section describes user provisioning for Oracle Revenue Management and Billing cloud services. It contains the following topics:

1.5.1 Overview

Each Oracle Revenue Management and Billing Cloud Service environment included in the subscription contains multiple components:

- Business Applications that run on the Oracle Utilities Application Framework, (OUAF) supports fine-grained authorization to access various features within the Business Application. It stores users and user groups.

  For each user authorized to access Oracle Utilities Application Framework the corresponding application user is created in the Oracle Utilities Application Framework.

  For the online application access, Oracle Utilities Application Framework users are created through Just in Time Provisioning flow.

Note: Identity Cloud Service user names (login id) are **case-sensitive**. This information should be communicated to users to avoid authorization and authentication issues.

- Supplemental components such as Analytics Publisher that don't maintain their own user records and support role-based authentication and authorization.

1.5.2 Pre-Defined Application Roles

The following roles are pre-defined in the Applications that represent Oracle Revenue Management and Billing Cloud Service environments. Each role represents an entitlement within the environment and grants user an access to a certain component:

Application Role	Authorized Access
Online Application User	The user assigned to this role may access online application.
Web Services Access	The user assigned to this role is authorized to access the REST/SOAP APIs.
BI Consumer	The user assigned to this role may access the Analytics Publisher within the environment and view and execute predefined reports.
BI Content Author	The user assigned to this role may access the Analytics Publisher within the environment and author new and view/execute existing reports.
SQL Developer Web Online User	The user assigned to this role may access the SQL Developer Web online and query the database to retrieve the information from both production and conversion schema.
REST Enabled SQL	The user assigned to this role may use cURL utility to invoke REST services and query the database to retrieve the information from both production and conversion schemas.

Note: Additional pre-defined roles for Data Visualization may be provided with specific cloud services. Examples include *CustomerContentCreator*. *CustomerContentConsumer* among others.

1.5.3 Configuring Just in Time Provisioning

Just In Time provisioning is a process that creates application user record in the OUAF-based business applications upon first successful login. The new user is created in the business application based on a pre-defined OUAF Template User. The Template User is determined from the mapping between Groups and OUAF Template Users defined in **Integration Configuration**.

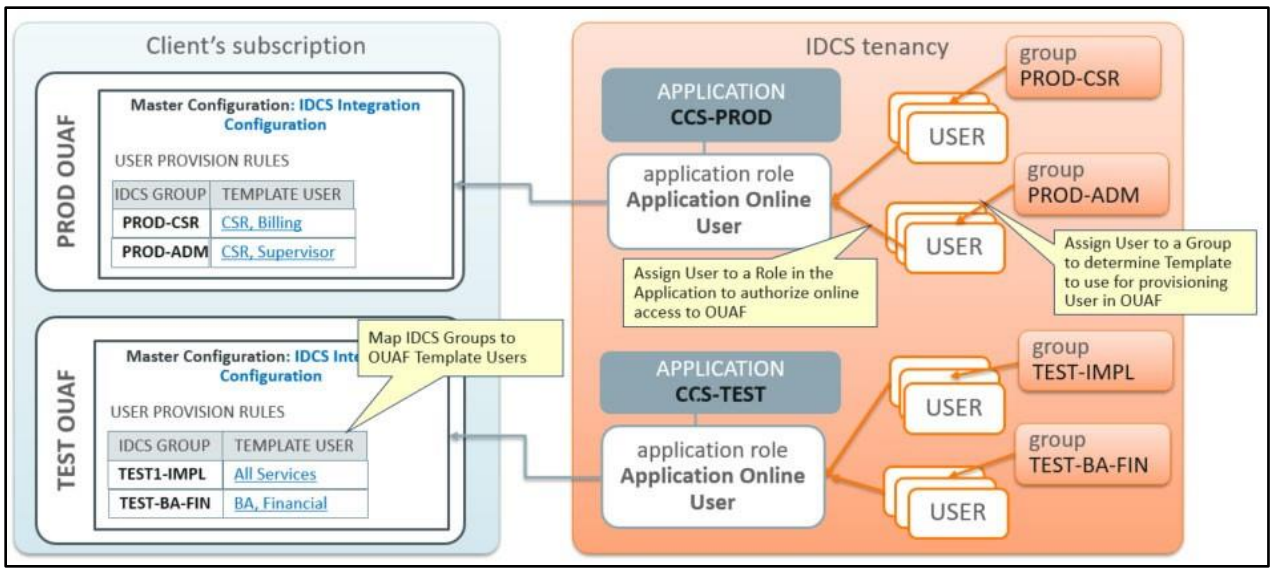

Figure 8: Provisioning Groups

Steps to configure Just In Time provisioning:

- Assign Security Administrator user to a Online Application Role in the environment (this is required to access the OUAF with access administrator privileges)
- Setting Up Groups for Provisioning - Identity Cloud Service
- Configuring User Provisioning Rules - OUAF

1.5.3.1 Setting Up Groups for Provisioning - Identity Cloud Service

Create Groups in Identity Cloud Service that represent broad functional areas and/or authorization level in the service. For example:

- For Non-Production (Development and Testing) environments:
  - Implementers
  - Business Analysts
  - QA Team
  - Security Testing
  - Functional Testing
- For Production environments:
  - Call Center
  - Call Center Supervisor
  - Business Administrator
  - Accounting

1.5.3.2 Configuring User Provisioning Rules - OUAF

To configure Identity Cloud Service Integration in OUAF:

- Create Template Users that represent various level of access authorization.
- Review existing Template Users.

If your intention is to use a Template User to provision integration (non-human) users you might have to assign Default Access Group to the Template User.

- Map the Groups created above to the Template Users in OUAF in the IDCS Integration Master Configuration.

  If the IDCS Integration Master Configuration is not configured at the time the user record is created, the user will be provisioned with K1MINACS (default minimal access).

1.5.4 Creating and Provisioning Users

This section describes steps involved in creating users and providing access to the cloud service's various components.

1.5.4.1 Setting Up an OUAF Security and Access Administrator

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Assign this user to the User Administrator role. See Setting Up a New Security Administrator for more details.
3. After first login to OUAF this user will be provisioned with Template User K1SCRADM (security administrator).

1.5.4.2 Setting Up an Online Application User

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Assign the user to the group that represents the appropriate level of authorization for the environment.
3. Locate the application that is corresponding to the environment.
4. Assign the user to the Online Application User role in the environment.

1.5.4.3 Setting Up an Integration User for REST/SOAP Web Services

REST/SOAP API doesn't perform Just-In-Time provisioning. Users for web services must be created manually in both and OUAF applications.

An email address must be provided as part of user creation:

- It is recommended that this email address is used for non-human user setup only.
- All email notifications concerning user account are sent to this email address.
- Security administrator must have access to this email account.

Perform the following steps:

1. Create a new user or search for and select existing user:
   - Specify the email address allocated for the integration/non-human users.
   - When the activation email is received, reset the user's password, and communicate the email address and password to the integration team.
2. Assign the User to the REST/SOAP Web Services role in the Application that represents the environment.

3. Login to OUAF and create a new User with Login ID = User Name. Assign the user to user groups that provide access to all or selected application services, according to the business requirements.

1.5.4.4 Setting Up an Integration OAuth Client for REST/SOAP Web Services

External systems may access Oracle Revenue Management and Billing Cloud Service REST APIs using OAuth client credentials. OAuth clients are created by the Oracle Revenue Management and Billing Cloud Operations team. To request creation of a new OAuth Client, create a Cloud Operations service request and provide the following information:

- **Environment**(s) where the OAuth client is needed. For example, PROD, TEST01, DEV.
- **Client name suffix**: Use a distinct name that may suggest the functional purpose of the integration, for example METERDATA or whatever is applicable for the integration's business use. If not provided, the default suffix is INTEG.
- **Client description**: Provide a meaningful description of the integration point.
- **Client type (trusted or confidential) and client certificate**: The integration requirements may call for trusted client and the external application may also supply its own certificate. Otherwise, Oracle Identity Cloud Service creates trusted client with its internal native certificate.
- **OAuth flow for your intended integration**: Currently supported are *client credentials*, *JWT assertion*, and *authorization* code flows. For the authorization code flow, you can also supply your own redirect URL.
- **Scope**: You can define OAuth clients with access to either REST or SOAP APIs or both REST and SOAP APIs.

The Oracle Revenue Management and Billing Cloud Operations team will create the OAuth Client using the input provided in the service request. Once the client has been created, locate the newly created OAuth Client on the Oracle Identity Cloud Service **Admin Console**, under **Oracle Cloud Services**. The name is composed as `<product>-<domain><tenant><suffix><sequential number>`.

For example:

`ORMBCS-PRODC12345CMETERDATA0 , ORMBCS-PRODC12345FIELDSERVICE1`

Where,

- The client ID and secret can be found in the **General** section of the **Configuration Tab**.
- The allowed scope can be found in the **OAuth Client** section on the **Configuration Tab**, under **Token Issuance Policy**.

The next step is to create an application user in the appropriate Oracle Revenue Management and Billing Cloud Service. Access the appropriate Oracle Revenue Management and Billing Cloud Service application and navigate to the **User** portal. Create a new user corresponding to the OAuth Client created above:

- Enter the OAuth client ID as the user's **Login ID**.
- Select "OAuth Client" from the **User Type** drop-down list.
- Assign **User Group**(s) that will provide the integration with access to the appropriate functionality.

The OAuth Client credentials are now ready to use. When issuing a webservice call, specify the client id, secret and allowed scope that you've determined from the Oracle Identity Cloud Service **Admin Console**.

Maintaining OAuth Clients Created for Integration

You can delete the OAuth client or regenerate the OAuth client secret by creating a service request with the Oracle Revenue Management and Billing Cloud Operations team. Provide the OAuth Client ID and the Oracle Identity Cloud Service tenancy URL. The Oracle Revenue Management and Billing Cloud Operations team will perform the requested action on your behalf.

1.5.4.5 Setting Up a User with Access to Analytics Publisher and Data Visualization

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to one of the Application Roles available in the environment:
    - **Analytics Publisher**: Choose one (or both) of the following application roles:
        - BI Consumer
        - BI Content Author
    - **Data Visualization**: Choose one or more product-specific application roles related to Data Visualization features, such as CustomerContentConsumer.

1.5.4.6 Setting Up a User Authorized to Execute Ad-hoc SQL Queries

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to one of the following roles:
    - **SQL Developer Web Online User**: Provides access to the online web-based interface that enables user to execute queries.
    - **Rest Enabled SQL**: Provides the ability to execute REST calls using `cURL` command.

1.5.5 Cloud Service Implementation User

The environment provisioning process creates an internal (non-human) user account named "K1IPROCESS" that is used by cloud service implementation tools and processes, including configuration migration between environments.

1.6 Using Federated Single Sign-On

This section describes tasks required when using an external identity management system to provide authentication for the application instances within your cloud subscription. It contains the following topics:

- Overview
- Setup External Identity Provider
- Service Access for Federated Users
- Just In Time Provisioning for Federated Users

1.6.1 Overview

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 should be available after the subscription is live.
- The Federated Single Sign-On only concerns online access; it is not applicable for the integration and other non-human accounts.
- The option to configure federation with existing Identity and Access Management is included with Identity Cloud Service subscriptions as part of Oracle Revenue Management and Billing Cloud Services.

1.6.2 Setup External Identity Provider

Configure a Security Assertion Markup Language (SAML) 2.0 external identity provider such as Active Directory Federation Services (AD FS) for federated SSO to Oracle Identity Cloud Service. Configuration steps include:

- Configure Microsoft Active Directory Bridge or implement user data synchronization via REST SCIM API or flat file import.
- Setup the Security Assertion Markup Language 2.0 Identity Provider.
- Verify Federated Single Sign-On.

To access detailed configuration instructions provided by Identity Cloud Service:

- Navigate to the Identity Cloud Service console dashboard and select Managing Security Settings to access online Identity Cloud Service tutorials.

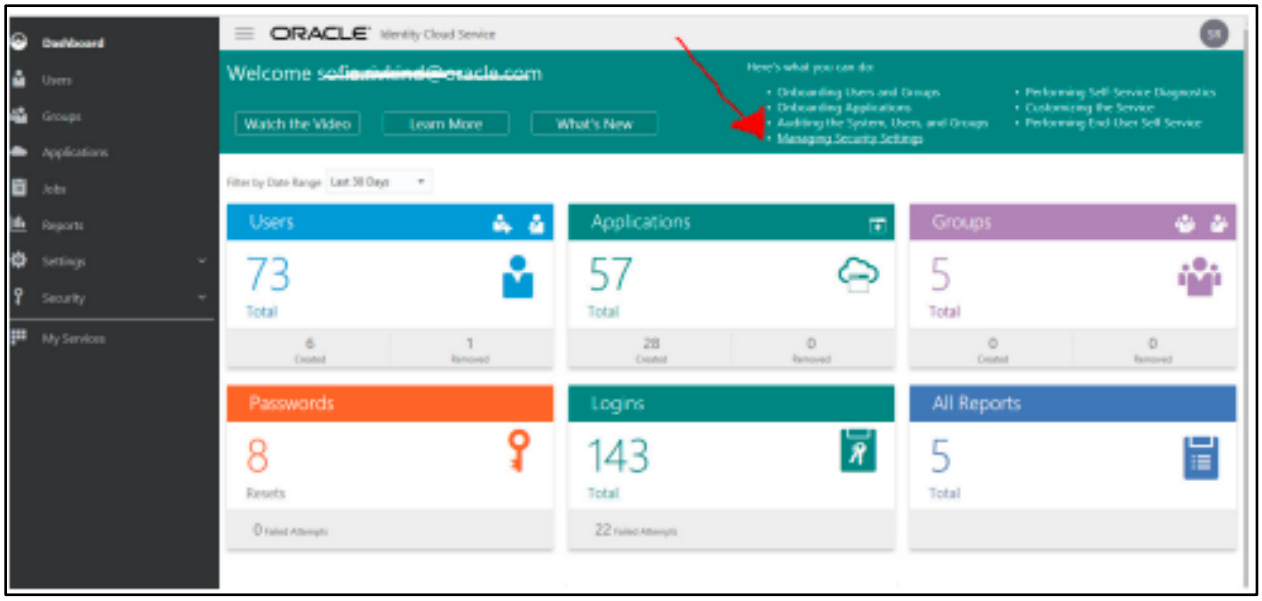

Figure 9: Identity Cloud Service Console Dashboard

- Follow the instructions under Configure External Provider.

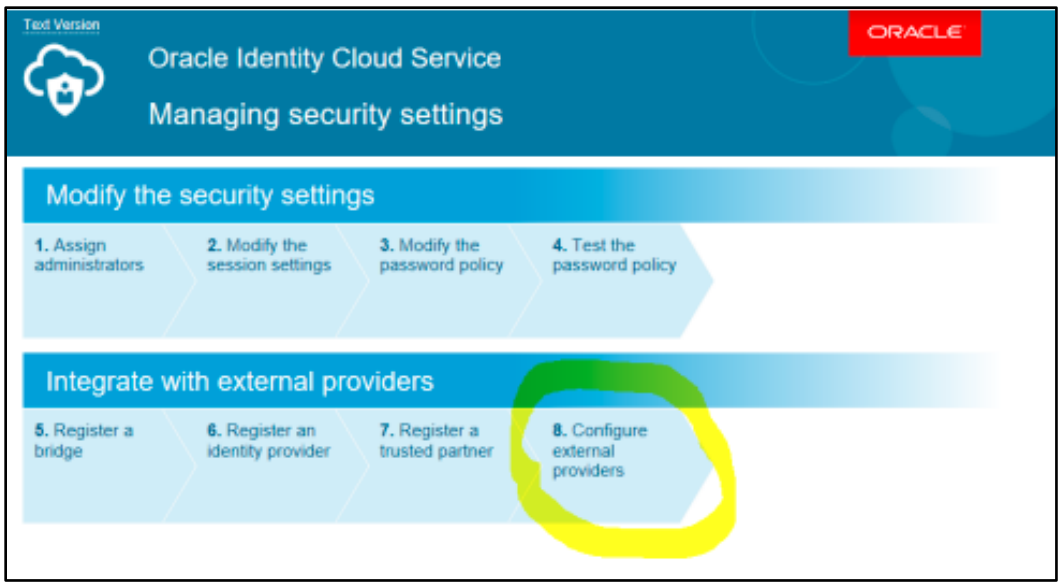

Figure 10: Managing Security Settings

Note: Federated authentication is enabled by default. This configuration means the user credentials will be validated against a configured Identity Provider.

When configuring Identity Bridge, define the federated authentication as follows:

- To continue validate credentials and maintain passwords and password rules in the external identity management system leave the Federated Authentication checkbox checked.
- To validate credentials and manage passwords in Identity Cloud Service uncheck the Federated Authentication checkbox. Identity Cloud Service will generate the password for the users and send the notification by email (the email attribute must be filled in Microsoft Active Directory and mapped to the Oracle Identity Cloud Service).

1.6.3 Service Access for Federated Users

Users created in Identity Cloud Service via federation should be granted access to the environments within the subscription the same way as the users created directly in Identity Cloud Service. See Update Access to Service and Setting Up an Online Application User for the instructions on how to assign user to the online access application roles.

Possible approaches:

- Process users one by one: locate user in Identity Cloud Service and assign to the application roles
- Process multiple users:
    - Export users from directly or from the group (see Exporting for more details).
    - Copy the information into Application Role import file and import users and/or groups to the Application Role (see Importing for more details).

1.6.4 Just In Time Provisioning for Federated Users

In the federated SSO scenario the Identity Cloud Service users and groups are imported from the external identity provider's data repository.

- Evaluate the groups created in Identity Cloud Service as a result of sync with external Identity Provider and determine whether to use them for Just In Time provisioning purpose.
- Login to the OUAF-based application and set up Template Users that represent authorization levels corresponding to the Identity Cloud Service groups synchronized from the external provider.
- Configure the Identity Cloud Service Group - Template User mapping in the Master Configuration.

See Configuring Just in Time Provisioning for more detailed configuration instructions.

2. Object Storage Setup

Oracle Cloud Object Storage is a part of Oracle Cloud Infrastructure Storage Services, and it is a required service for Oracle Revenue Management and Billing Cloud Services, including Oracle Revenue Management and Billing Cloud Services (ORMBCS). These cloud services use Oracle Cloud Object Storage as the vehicle to exchange data files with customers during an implementation and in production.

Oracle Infrastructure Services get provisioned separately from Oracle Revenue Management and Billing Cloud Services but are grouped together under the same customer Cloud Account. Access and administration of Oracle Cloud Infrastructure Services is done via the Oracle Cloud Infrastructure Console that can be accessed from the Oracle Cloud Account. This document describes the tasks that are required for connecting the system to Object Storage and the basic administration that is needed for implementation stages and beyond that.

For more information on Oracle Cloud Object Storage (including concepts, security best practices, and more), see Oracle documentation about Oracle Cloud Infrastructure Services at: https://cloud.oracle.com/iaas.

This section provides information about setup and configuration of object storage for use with Oracle Revenue Management and Billing Cloud Services. It contains the following topics:

- Object Storage Management
- Connecting to Oracle Cloud Object Storage
- Recommended Object Storage Structure for a New Implementation
- Initial Testing of Object Storage Connectivity
- Cross-Region Disaster Recovery Considerations

2.1 Object Storage Management

This section outlines the basic administration tasks of Oracle Cloud Infrastructure related to Object Storage. It contains the following topics:

- Object Storage Structure
- Security and Access Management
- Tenant Information
- API Access

2.1.1 Object Storage Structure

This section provides an overview how object storage is structured. It contains the following topics:

- Compartments
- Object Storage Buckets

2.1.1.1 Compartments

All cloud infrastructure resources are organized in Compartments. A tenancy can include several compartments. A compartment is a logical grouping of resource types. For object storage, compartments help manage the structure of objects that are stored in the cloud.

Compartments can have child-compartments which support multi-level hierarchy of resource grouping. Each compartment is identified by a unique Oracle Cloud ID (OCID). When connecting the system to object storage, the compartment identification is part of the required connection configuration information. There are no hard requirements as to the structure or number of compartments that should be created. A recommended setup is described later in this document and has reference to compartments as well.

Root Compartment

The Root Compartment is created for each account and is the top level of the compartment's hierarchy. The name of that compartment includes the string "(root)" in it.

2.1.1.2 Object Storage Buckets

Oracle Cloud Object Storage is organized in buckets. A bucket is like a folder or a directory that stores one or more objects. Objects can be any file and can includes documents, images, and so on. Each compartment can have one or more buckets. Buckets cannot include other buckets.

An example of Object Storage structure can be:

- Root Compartment
  - Compartment A
    - Child Compartment A1
      - Bucket A1-1
      - Bucket A1-2
      - Bucket A1-3
    - Bucket A1
  - Compartment B
    - Bucket B1
    - Bucket B2

Bucket names are unique within a tenancy which means that the same bucket name cannot be used in different compartments. Compartments have a unique identifier (OCID) so they are in fact unique within the tenancy. The system can be configured to connect to any compartment and bucket that you define. This configuration is described in the next section.

2.1.2 Security and Access Management

Oracle Revenue Management and Billing Cloud Services security is managed by an Oracle Identity Cloud Service (IDCS) instance that gets created when those services are provisioned. Oracle Cloud Infrastructure security is managed by Oracle Identification and Access Management (IAM).

These two-identity management system are linked together and synchronized to allow easy access and security administration tasks. This document includes only the information needed for the security administration of Oracle Cloud Infrastructure services.

2.1.2.1 Accessing the Cloud Infrastructure Console

Access to the console can be done by selecting **Open Service Console** from the small action menu on the lower right side of the **Compute** tile on Oracle Cloud Account. In addition, the URL for the console can be found on the **My Admin Accounts** tab when selecting the **Account Management** box in the **Oracle Cloud Account** page. The URL for the console will appear next to the **Compute (OCI) Users** account type.

Note: If you don't see a tile called **Compute**, click the **Customize Dashboard** tile on the dashboard and select to show the **Compute** service from the list under the **Infrastructure** category. If you cannot see that service or it is not available yet, please contact your Oracle support representative.

Authentication and Access Management: Federated and Non-Federated Users

When accessing Oracle Cloud Infrastructure, authentication can be Federated or Non-Federated:

- **Federated** users are defined in Oracle Identity Cloud Service (IDCS), they are synchronized with IAM and are authenticated by IDCS when logging into Oracle Cloud Infrastructure.
- **Non-Federated** users are defined only in IAM and are authenticated by IAM only.

The initial security administration user is created as BOTH a Federated and Non-Federated user. That means that this administration user can login into Oracle Cloud Infrastructure from the Cloud Account Portal without the need to provide their credentials again.

2.1.2.2 First Time Login

Since the security administrator has users' definitions that are both Federated and Non-Federated, they can login into Oracle Cloud Infrastructure for the first time in several ways:

- Login from their Oracle Cloud Account (using the Open Service Console option on the Compute tile): this automatically logs the user into Oracle Cloud Infrastructure without the need to provide any credentials.
- Login directly to Oracle Cloud Infrastructure (using the direct URL): when using this option, the user is presented with two authentication options:
    - Login using Single Sign On (SSO): this requires Federated user credentials. If the user is already logged into their Cloud Account, they will not need to provide their credentials.
    - Login directly into Oracle Cloud Infrastructure: this requires Non-Federated user credentials. In the case of a first login, the temporary password that was assigned to the federated user will be the same for the non-federated user.

2.1.2.3 Managing Users

There are two types of users that should have access to infrastructure services (Object Storage being one of these): UI Access users and API Access users. UI Access users should typically include administrator level personnel that use the Infrastructure Console to manage security and the various infrastructure services (such as Object Storage).

Note: UI Access users that should not have administrator access to Object Storage but are only involved in business operations (for example: uploading files to an Object Storage Bucket) should have Non-Federated users with non-administration security access setup.

API Access users are applications that use the API to access the various services but do not have access to the console user interface. These users can be Federated or Non-Federated. However, the instructions below see Non-Federated users only!

The recommended setup outlined later in the document includes details about both types of users.

Adding a New User:

1. To add a new user, use the upper left menu in the infrastructure console, select **Identity**, then **Users**. Click **Create User** to create a new user.
2. After saving the new user information (name and description are sufficient in this case) you should be able to see the new name in the list of users.

API Access users do not need a password since they are identified via API keys. API Key management is described later in the document.

Note: When looking at the users defined for Oracle Cloud Infrastructure you will be able to see Federated and Non-Federated users. Federated users will typically have a name in a format similar to "oracleidentitycloudservice/username…".

Creating or Resetting User Password

Note: Initial password setup is required for Non-Federated UI Access users.

1. From the **User** list in the console, select the user name to go to the user details page.
2. Click **Create/Reset Password** to create an initial password for the user. The new temporary password can be emailed to the customer for them to login. They will be required to change the password on their first login.

User Identification

A User is identified by an OCID key that is displayed underneath the user name. That key is used to identify users when connecting to Object Storage via API calls.

User API Keys

API Access users that use API calls to connect to object storage should generate an encryption key pair (private/public) in PEM format and register the public key for the appropriate user (that is used in the API call). To register a public key for a user:

1. From the **User** list in the console, select the **User** name to go to the **User** details page.
2. Select the **API Keys** option from the **Resource List** on the left for that User.
3. Click **App Public Key**.
4. Copy and paste the public key content into the page and click **Add**.

2.1.2.4 Managing Groups

Security management is done in Oracle Cloud Infrastructure by User Groups. Oracle Cloud Infrastructure includes an Administrator User Group that is predefined and contains the initial administrator user.

Adding a New User Group:

1. To add a new user group, use the upper left menu in the **Infrastructure Console**, select **Identity**, then **Groups**. Click **Create Group** to create a new group.

2. Provide a **Name** and a **Description** for the group. Tags are optional and are not covered in this document.

Adding Users to a User Group:

Users can be added to user groups in two ways:

1. When editing a user group record, you can add a user from the **Group Members** section by clicking **Add User to Group**.
2. When editing a user record, select the **Groups** option from the **Resource** list on the left for that user and click **Add User to Group** on the **Groups** section that is shown for that user.

2.1.2.5 Managing Policies

Policies can be used to enforce access rights for Users that are a part of a User Group. Policies are defined in IAM using the **Identity → Policies** menu.

Using policy definitions, you can define the access rights to your infrastructure services, for example, Object Storage. You can define what compartment or bucket user groups have access to, and the type of access (read, write, and so on). Policies can apply to specific compartments or the root compartment, in which case it will apply to all the compartments.

A policy is a collection of statements with specific syntax that describe access rights to resources. For example, in a policy, you can define that a certain user group has access to create and delete buckets and objects in a certain compartment. See *Oracle Cloud Infrastructure Documentation* for Identify and Access Management to find out more about policies.

2.1.3 Tenant Information

Information about the tenancy is displayed when selecting **Administration**, then **Tenancy Details** from the upper left menu in the **Infrastructure Console**. The information displayed is important for connecting the system to that Object Storage instance, and includes:

- **The OCID key of the tenancy:** This is the tenancy identification.
- **Home Region:** This is the main data region selected for this tenancy. Additional data regions added to this tenancy can be defined.
- **Object Storage Namespace:** This identification is pre-generated and is needed for the connection of the system to Object Storage.

2.1.3.1 Regions

When a cloud account is created, a Home Region is assigned to it. This is the main data region that is linked to that account. Additional data regions can be subscribed to for the tenancy if access to regions outside the home regions are required.

The list of all available regions is displayed under the **Regions** section of the **Tenancy Details** page. Clicking **Subscription** for a region will add that to the list of available regions for this tenancy. All administration tasks will be conducted at the home region but will be synced to the other regions automatically. Please note that when connecting the system to object storage the region must be identified as well.

2.1.4 API Access

Oracle Cloud Object Storage can be accessed via the **Infrastructure Console** or via three types of APIs:

- Command Line Interface (CLI)
- REST calls
- Java SDK

The system connects to Object Storage using REST calls to the Object Storage endpoints that are documented for each of the data regions to which your cloud service has access. For more information about Object Storage APIs, see *Oracle Cloud Infrastructure Object Storage Documentation* (go to: https://cloud.oracle.com/storage and select the **Documentation** tab).

2.2 Connecting to Oracle Cloud Object Storage

The system supports and manages connections to Object Storage via metadata configuration. The system can connect to any number of Object Storage locations and Tenancies.

REST API calls issued by the system, to interact with the Cloud Object Storage, require API key signature. The system is designed to have a unique private/public key pair for each environment that connects to Object Storage. This means that each system environment should have a unique user defined in IAM with a registered unique API Key.

Currently the system supports accessing files on Object Storage via batch processing. Referencing a file location as Object Storage is done using a special notation.

This section contains the following topics:

- Object Storage Connection Configuration
- API Key Management
- Referencing Files on Object Storage

For additional information, see **External File Storage** help topic in the Oracle Revenue Management and Billing Cloud Service Online Help.

2.2.1 Object Storage Connection Configuration

Each connection configuration is represented in the system via the File Storage Configuration extendable lookup (F1-FileStorage). Each value for that extendable lookup should contain the information described below. To configure a new connection, go to the Extendable Lookup portal by selecting **Admin**, then **General**, then **Extendable Lookup**, then **Search**, and search for "File Storage Configuration". After selecting it, click **Add** to add a new value. When adding a new value, select the Oracle Cloud Object Storage file adapter and provide the following information:

- **User**: The User Identification (OCID Key) that is used for that connection. A unique user ID should be defined for each system environment (for example Dev, Test, Prod) that is connecting to that object storage tenancy. It is strongly recommended that this user ID is not used for other purposes. If one system environment is required to connect to multiple object storage tenancies, there should be a different user ID for each of these tenancies.
- **Tenancy**: The tenancy ID (OCID Key) of the object storage tenancy.

- **Compartment**: The compartment ID (OCID Key) of the compartment for that connection. Each compartment needs a separate connection configuration.
- **Namespace**: The Namespace of the object storage tenancy.
- **Key Ring**: The Key Ring name that was created in the system. See API Key Management for more information.
- **Region**: The region of the object storage tenancy for that connection. Reminder: object storage tenancies can have multiple regions if additional subscription was done.
- **Bucket Name Prefix**: a name prefix that will be added to the bucket name of file paths referencing object storage (see Referencing Files on Object Storage for more information).

2.2.2 API Key Management

Secured access to Object Storage is accomplished by using API Signature Key. Each configured connection to Object Storage includes a Key Ring.

A key ring is an object that hold a set of private/public encryption key pairs. Object Storage connections can share the same key ring and even the same key in the key ring for the same system environment. For example, key ring A can be defined and used in all the system environments: Dev, Test, and Prod.

However, the key pairs inside the ring must be different in each of the environments. The connections defined for Object Storage can all use the same key ring A in all the environments since the actual key pair that is used in each environment, is different.

To create a new key ring, select **Admin**, then **Security**, then **Add Key Ring**. Make sure to generate a key pair in that ring after creating it.

2.2.2.1 Registering the API Key

Once a key ring has been created with an active key pair, click **View** for the Public Key of that key pair to copy the public key content. That content should be pasted into the User API Key in IAM (see the User API Keys section in Security and Access Management of Object Storage Management).

2.2.3 Referencing Files on Object Storage

Reference to Object Storage can be used anywhere that a file location reference is allowed in the system.

The format is `file-storage://<File Location>/<Bucket>/<Filename.ext>`, where:

- **<File-Location>**: The File Storage Configuration extendable lookup value defined for that file. This will include the compartment identification.
- **<Bucket>**: The object storage bucket in the compartment that is defined as part of the File Storage Configuration extendable lookup value.
- **<Filename.ext>**: The name of the file.

For example, the "`payment_info.dat`" file in the "Payment-Upload" bucket in a compartment that is referenced in the "AB-Payments" File Storage Configuration extendable lookup value can be referenced as "`file-storage://AB-Payments/ Payment-Upload/payment_info.dat`".

2.2.3.1 Using the Bucket Name Prefix

If you set the Bucket Name Prefix in the File Storage configuration, any file path referencing this configuration will be automatically revised at runtime, adding the name prefix to the bucket name. This allows you to define different name prefix for buckets for each environment (or for production vs non-production environments) and keep your file paths for your batch jobs the same in each environment.

For example:

- You can create all your non-production buckets with a "NP-" name prefix, and all your production buckets without a name prefix.
- You can then define a File Storage configuration named "OS-APP" in each of your environments and set the **Bucket Name Prefix** to:
    - "NP-" in all the non-production environments
    - Blank in the production environment
- When you will use a file path reference on your batch jobs, for example "`filestorage://OS-APP/AB-Payments`" then:
    - When the job related to that file runs in a non-production environment it will reference the payment files in the "NP-AB-Payments" bucket
- When the job runs in the production environment, it will reference the "AB-Payments" bucket.

2.3 Recommended Object Storage Structure for a New Implementation

This section describes a recommended configuration and structure for your Object Storage tenancy for your service implementation. Using the recommended setup can simply the initial implementation and testing activities of your new service but they are not mandatory. Furthermore, you can start with the recommended setup and adjust it per your implementation needs.

See the following topics in the Oracle Revenue Management and Billing Cloud Service Online Help:

- Object Storage
- Process Automation Tool
- Data Conversion

2.3.1 Security Considerations

The system connection to Oracle Cloud Object Storage is governed by a combination of User, User Group (optional) and Access Policies that are defined in IAM (see the Managing Object Storage section for more information). As a reminder, the User ID details are provided as part of the File Storage Extendable Lookup value in the system.

2.3.1.1 Compartments

It is recommended to divide your resources amongst several compartments:

- **Production Compartment**: This compartment includes all the production resources (such as object storage buckets and objects that store production data).

- **Non-Production Compartment**: This compartment includes all the nonproduction resources used during the implementation and testing phases.
- **Shared Compartment**: This compartment is used to hold resources that are used by special activities or processes and can be accesses by production and non-production users. A good example of that can be configuration data (that can be exported from a testing environment and moved to the production environment when ready, using the Configuration Migration Assistant) or conversion data that can be used in both production and non-production environments (during the implementation phases).

2.3.1.2 Users

It recommended that each system environment uses a unique user ID in IAM so that access rights to production vs non-production files or objects can be enforced for that tenancy. Each user will have its own API Key registered and should be a part of a user group, which will simplify the security access definitions.

2.3.1.3 User Groups

It is recommended to assign the users to several groups, for example:

- **Application Access User Group for Production**: This group includes the user assigned to the production system environment and other users that will need access to object storage production information via API calls.
- **User Access User Group for Production**: This group includes all the users that will need access to object storage production information via the **Infrastructure Console**.
- **Application Access User Group for Non-Production**: This group includes the users assigned to the non-production system environments and other users that will need access to object storage non-production information via API calls.
- **User Access User Group for Non-Production**: This group includes all the users that will need access to object storage non-production information via the **Infrastructure Console**.

These groups can be referenced when defining the security policies for production and non-production access.

2.3.1.4 Policies

It is recommended to create Policies to control access to resources based on:

- **Production vs Non-Production**: For example, it is recommended to restrict access to production resources only to production users.
- **System vs Human Users**: For example, it is recommended to restrict certain operations from system users (such as ability to delete objects or buckets).

2.3.2 Recommended Setup for a Single Cloud Service

If you are using a single Oracle Revenue Management and Billing Cloud Service, consider the following recommended setup.

2.3.2.1 Oracle Cloud Infrastructure - IAM and Object Storage

Compartments and Buckets

- Root Compartment
  - ORMBCS-Prod (Compartment)
  - ORMBCS-Non-Prod (Compartment)
  - ORMBCS-Shared (Compartment)
    - CMA-Files (Bucket)

      [for the system Configuration Migration Assistant]
    - CONV-Upload (Bucket)

      [for Data Conversion]
    - CONV-Output (Bucket)

      [for Data Conversion]

Application Users and User Groups for Object Storage Access

- ORMBCSDEV (for the Development environment)

  [part of User Group ORMBCSObjectStorageAppNonProdAccess]
- ORMBCSTEST (for the Testing environment)

  [part of User Group ORMBCSObjectStorageAppNonProdAccess]
- ORMBCSPROD (for the production environment)

  [part of User Group ORMBCSObjectStorageAppProdAccess]

Additional environments will each have their own unique User with the "ORMBCS" prefix and will be a part of the ORMBCSObjectStorageAppNonProdAccess User Group.

Policies for Object Storage

- Policy for application access to object storage in the Production Compartment:
  - Defined under the root compartment.
  - Open only to production user groups.
  - Allows read, create, and modify access to buckets and objects in the Production Compartment and the Shared Compartment.
- Policy for application access to object storage in the Non-Production Compartment:
  - Defined under the root compartment.
  - Open only to non-production user groups.
  - Allows read, create, and modify access to buckets and objects in the Non-Production Compartment and the Shared Compartment.

2.3.2.2 Example: Oracle Revenue Management and Billing Cloud Service

The following example references the setup in the Oracle Revenue Management and Billing Cloud Service application outlined above.

File Storage Configuration

The following File Storage Configuration extendable lookup values should be defined to correspond to the cloud infrastructure setup above:

- OS-SHARED: This value will point to the Shared Compartment:
  - The user ID will be different in each environment (ORMBCSDEV, ORMBCSTEST, ORMBCSPROD).
  - The key ring can be the same in all environments, but each environment key ring will have different key pairs (generated separately in each environment).
- Additional values can be defined based on the file location your specific processes will need to access, for example:
  - OS-Payment: for Payment upload interface
  - OS-MR-Up: for Meter Reads upload interface
  - OS-MR-Dl: for Meter Reads download interface
  - The Extendable Lookup values (the name) will be the same in each environment but some of the information that is defined for them will be different in each environment:
    - User ID, compartment (Prod vs Non-Prod) and keys

2.3.3 Recommended Setup for Multiple Cloud Services

If you are using multiple Oracle Revenue Management and Billing Cloud Services and you are still using a single Oracle Cloud Infrastructure tenancy (and therefore single Object Storage tenancy), then:

- Duplicate the Cloud Infrastructure setup (compartments, buckets, users, groups, policies, etc.), one set with the ORMBCS1 name prefixed and one set with the ORMBCS2 name prefix.
- The setup in the Oracle Revenue Management and Billing Cloud Service (ORMBCS1 or ORMBCS2) would be identical for both. The differences will be in the references to the various Cloud Infrastructure resources prefixed with ORMBCS1 or ORMBCS2, for example:
  - OS-SHARED in ORMBCS1 will point to ORMBCS1-Shared Compartment with User ORMBCS1DEV/TEST/PROD.
  - OS-SHARED in ORMBCS2 will point to ORMBCS2-Shared Compartment with User ORMBCS2DEV /TEST/PROD.

2.4 Initial Testing of Object Storage Connectivity

This section contains step by step instructions for initial testing of your connection between your cloud service and your object storage. The instructions represent a simple setup for testing the connection to object storage.

These instructions do not represent the complete recommended setup that was described in previous section.

1. Log into Oracle Cloud Infrastructure Console using credentials provided to you by your security administrator:
    a. In the **Identity** menu, select **Users**:
        i. Create a new user named "INIT-TEST" (Take note of the user OCID). (This will be a Non-Federated user.)
        ii. Add that user to the Administrator user group.
    b. In the **Identity** menu, select **Compartments**:
        i. Create a new compartment named "INIT-TEST" (take note of the compartment OCID).
    c. In the **Object Storage** menu, select **Object Storage**:
        i. Select the INIT-TEST compartment in the **Compartment** field under the **List Scope** section.
        ii. Create the following buckets under the INIT-TEST compartment: CMA-Files
    d. In the **Administration** menu, select **Tenancy Details**:
        i. Take note of the tenancy OCID (under **Tenancy Information**)
        ii. Take note of the namespace (**Name** field under **Tenancy Information**)
        iii. Take note of the home region
2. Log into the Utility Cloud Service development environment (DEV), using credentials provided to you by your security administrator:
    a. Go to the **Key Ring** portal (use the Menu Search option):
        i. Add a new Key Ring named "INIT-TEST"
        ii. After creating the new Key Ring, click **Generate Key**.
        iii. In the **Key Pair** section, choose the **Activate** action for the new generated Key Pair.
        iv. Click **View** to get the public key portion of the key pair.
        v. Copy the full content of the public key displayed in a popup window, save it in a text document. You will use this later.
    b. Go to the File Storage Configuration extendable lookup and search for a value of OS-SHARED.
    c. Edit that value and enter the following information:
        i. **User**: The user OCID of INIT-TEST User from step #1.
        ii. **Tenancy**: The tenancy OCID from step #1.
        iii. **Compartment**: The compartment OCID of INIT-TEST Compartment from step #1.
        iv. **Namespace**: The namespace noted in step #1.
        v. **Key Ring**: Search for the INIT-TEST key ring created above and select it.
        vi. **Region**: The home region noted in step #1.

vii. Click **Save**.

d. Go to the **Master Configuration** portal (use the Menu Search option):

i. Look for the **Migration Assistant Configuration** master configuration.

ii. Make sure that the **Import** and **Export** directories have the following value:

"file-storage://OS-SHARED/CMA-Files"

3. Log back into Oracle Cloud Infrastructure Console using credentials provided to you by your security administrator:

a. From the **Identity** menu, select Users:

i. Select the INIT-TEST user created earlier.

ii. In the **API Keys** section, click **Add Public Key**.

iii. In the popup window paste the public key value saved in previous step (the public key portion of the key pair generated in the Oracle Revenue Management and Billing Cloud Service application) and click **Add**.

4. You are ready to test the object storage connectivity. Log back into the Utility Cloud Service development environment (DEV), using credentials provided to you by your security administrator:

a. Go to the **Migration Request** portal (use the Menu Search option).

b. Search for a Migration Request named Users (F1-Users).

c. Click **Export** for that request (Users).

i. In the popup window enter the file name "init_test" (for example)

ii. Click **Save**. You will be directed to the **Migration Data Set Export** page.

d. Go to the **Batch Job Submission** portal and submit a job with the F1-MGDPR batch code. When the job ends, go back to the **Migration Data Set Export** portal, and check the status:

i. If the status changed to Exported, log into the Oracle Cloud Infrastructure Console, navigate to the CMA-Files object storage Bucket under the INITTEST Compartment and check that there is a file called init_test.cma there.

ii. If the file exists, the test is successful!

5. If the connectivity test was successful, proceed with the overall setup of the Object Storage and your Cloud Service application per the recommended setup above.

2.5 Cross-Region Disaster Recovery Considerations

This section outlines the considerations for Object Storage connection and configuration in case the cross-regional disaster recovery option has been enabled for your system. This section contains the following topics:

2.5.1 Home and Disaster Recovery (DR) Regions

Your system has a Home Region, which is the data region that it was initially provisioned at. This will be referred to as the System Home Region. When cross regional disaster recovery is enabled for your system, it will have a designated disaster recovery (DR) region. The disaster recovery region is the data region that your system will be switched to in case your home region is no longer available. This will be referred to as the System Disaster Recovery Region.

Your Oracle Cloud Infrastructure (where your Object Storage resides) has also a home region, that will be referred to as the Object Storage Home Region. If your system has a designed disaster recovery region, it will make sense for your object storage to have a designated disaster recovery region as well, which will be referred to as the Object Storage Disaster Recovery Region.

In most cases the System Home Region will be the same as the Object Storage Home Region but it could be different if it was chosen to be different. The same is true for the System Disaster Recovery Region and the Object Storage Disaster Recovery Region. Selecting an Object Storage Disaster Recovery Region will be covered in the next section.

Note: If the Object Storage Home Region is different that the System Home Region, you can skip this section since the cross-region disaster recovery procedures will not affect your object storage and will not affect your system connection to object storage.

2.5.2 Preparing your Disaster Recovery Region

If cross-region disaster recovery was enabled for your system, it will be automatically set up to be ready for a disaster event in terms of availability of resources on your System Disaster Recovery Region, according to your service level agreements. It is your responsibility to make sure that your object storage is ready as well.

Since Object Storage is a regional service, there is no automatic disaster recovery for that. Assuming your Object Storage Home Region is identical to your System Home Region, you need to plan for the eventuality that this region might become unavailable and so you will need to have your object storage available on another region.

The first thing you will need to do is to subscribe to an additional data region to be your Object Storage Disaster Recovery Region. To subscribe to an additional region, you should do the following:

1. In the Oracle Cloud Infrastructure Console, select **Administration**, then **Manage Regions** and look at the list of additional available data regions. Select the data region to designate as the Object Storage Disaster Recovery Region (is it recommended to have it identical to your System Disaster Recovery Region, if possible).
2. Your request for subscription to a new data region will be processed and when it is completed, you will see your new region in the list of available regions.

3. You will also be able to switch to this data region in your Oracle Cloud Infrastructure Console via the **Region** drop-down list.

2.5.2.1 Copying Your Object Storage Bucket Structure

Your Oracle Identification and Access Management (IAM) definitions (i.e., users, groups, policies and compartments) are all maintained in your Object Storage Home Region and these definitions are replicated automatically to all the other regions to which you are subscribed. Object Storage Buckets are region dependent which means that each data region can have its own set of buckets.

For your system to continue to work properly once it is switched to your System Disaster Recovery Region (for functions that require access to object storage), your object storage bucket structure should exist in your Object Storage Disaster Recovery Region.

Therefore, we recommend that you synchronize your bucket structure periodically between your Object Storage Home Region and Object Storage Disaster Recovery Region. This means, at a minimum, that buckets created in your Object Storage Home Region should be also added to your Object Storage Disaster Recovery Region.

2.5.2.2 Copying Your Object Storage Data

You may also choose to periodically copy the objects inside your buckets from your Object Storage Home Region to your Object Storage Disaster Recovery region. Please note that copying data from one region to another will result in the use of additional object storage space, which in turn can lead to additional cost per billing period.

See Using Replication in the **Object Storage** section of the *Oracle Cloud Infrastructure Documentation* for more information about configuring data replication policies to copy data between buckets in different regions. If you can re-create lost data when a disaster occurs, then you might not need to copy your data across regions in advance, for example:

- Most files generated by your system via batch jobs can be regenerated if necessary
- 3rd party applications that load files into object storage may also be able to reproduce these files upon request

2.5.3 Recovering from a Disaster

A disaster is defined as an event that will cause your System Home Region to become unavailable. When a disaster occurs, your system will automatically be switched to your System Disaster Recovery Region, based on your service level agreements. When that happens you are responsible to tell the system what object storage region to connect to instead of the current one that is was linked to when the disaster happened (if that region has also became unavailable). This section covers what you should do during a disaster and after it is resolved.

2.5.3.1 Switching to Your Disaster Recovery Region

Once your system has been switched to its System Disaster Recovery region, you will need to point it to a different data region for object storage access:

1. Log into each of the system environments.
2. In each environment look at all your current File Storage Configurations.

3. Edit each File Storage Configuration and change the region field to your Object Storage Disaster Recovery Region.
4. Save your changes.

2.5.3.2 Switching Back to Your Home Region

When your home region has been recovered and data was restored, the system will be switched back to your System Home Region. At this point you will need to point it back to your Object Storage Home Region for object storage access:

1. Log into each of the system environments.
2. In each environment look at all your current File Storage Configurations.
3. Edit each File Storage Configuration and change the region field to your Object Storage Home Region.
4. Save your changes.

2.5.3.3 Copying Back Your Object Storage Data

When you are switched back to your Object Storage Home Region, you may need to copy back some of the data that was created in your Object Storage Disaster Recovery Region. This may also include changes in bucket structure that you may have done while working in your disaster recovery regions.

- Changes in object storage bucket structure can be repeated in your home region manually after that region has been recovered.
- If you need to copy data back to your home region, see Using Replication in the **Object Storage** section of the *Oracle Cloud Infrastructure Documentation* for guidance.

3. Identity and Access Management with Identity Domains

This section provides instructions for Security Administrators regarding how to set up user accounts for Oracle Revenue Management and Billing Cloud Services, manage the user identity lifecycle, and govern authentication in multiple business applications. Identity and access management tasks include creation of users and groups, granting access to business applications, and configuring various settings. This section contains the following topics:

3.1 Identity and Access Management Overview

This section introduces working with Oracle Cloud Infrastructure Identity and Access Management (IAM) and Identity Domains.

Oracle Cloud Infrastructure tenancy is provisioned to customers with subscriptions to Oracle Revenue Management and Billing Cloud Services. Identity and Access Management (IAM) is a built-in part of the Oracle Cloud Infrastructure, and it governs the access to Oracle Cloud Infrastructure resources and Oracle Cloud Services.

Identity Domains are part of IAM and is where users and access to Oracle Cloud Services are configured and managed. Each cloud service subscription includes at least one Identity Domain. The Identity Domains are managed exclusively by the customer (see Identity Domains for more information). This section contains the following topic:

3.1.1 Identity Domains

The Oracle Revenue Management and Billing Cloud Service configurations are defined and maintained in an Identity Domain. Initial provision of the service results in all environments being connected to a single Identity Domain (usually a Default domain).

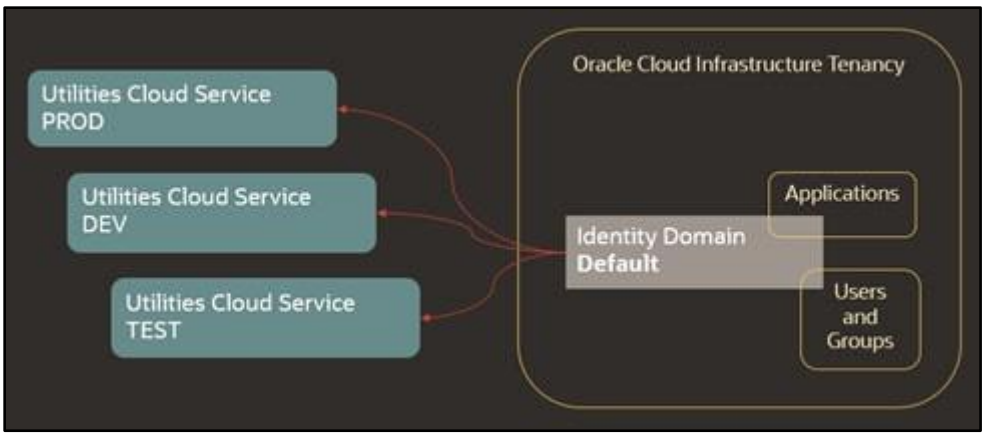

Figure 11: Identity Domain (Default)

This topology may be modified in the future. For example, you may create an additional Identity Domain that is dedicated for production environment. In this scenario, you should submit a request for the reconnection to the Oracle support team.

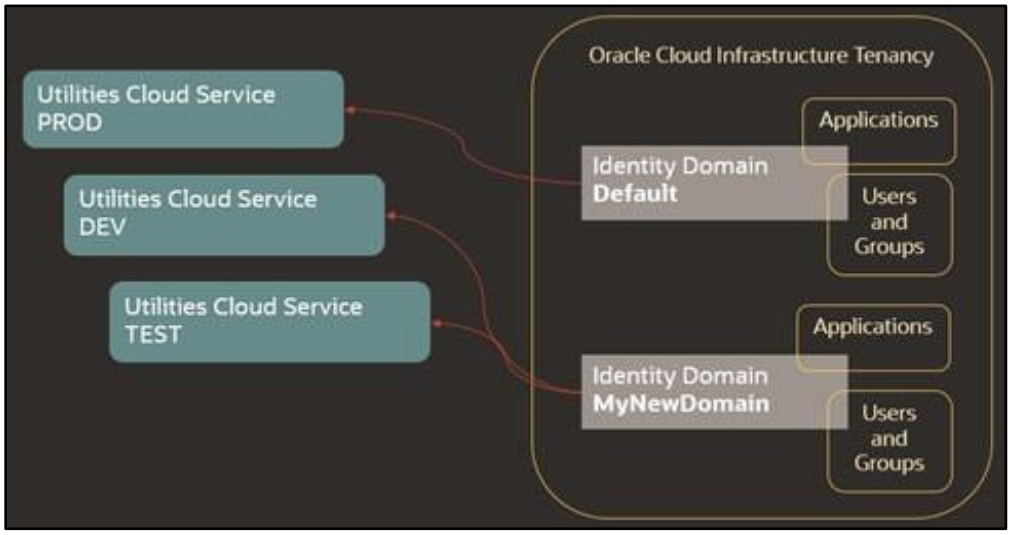

Figure 12: Identity Domain (MyNewDomain)

The following configurations are necessary to perform the identity and access management for the Oracle Revenue Management and Billing Cloud Services:

- **Application:** For Oracle Revenue Management and Billing Cloud Services the application represents a single environment, Production, or non-Production. Applications are created by the service provisioning process.
- **Application Role:** The Application Role represents an entitlement to access one of the components within the environment. By assigning user or groups to an Application Role the security administrator is authorizing access to the corresponding component(s). Application Roles are created by the service provisioning process.
- **User:** Users represent a human or non-human entity that is accessing the environment. User records are created and managed by the Security Administrator.
- **Group**: Groups comprise of one or more users. Groups are created and managed by the Security Administrator.

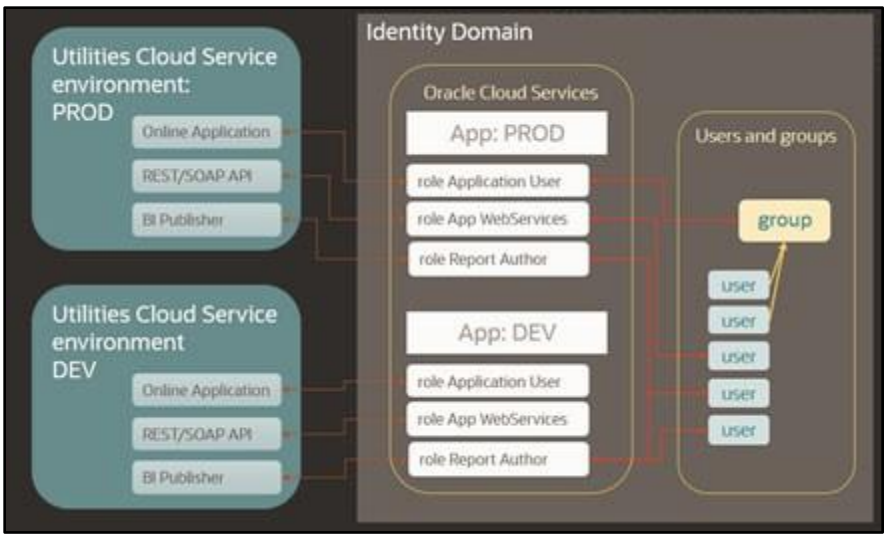

Figure 13: Configurations

3.2 Quick Start Guide

This section provides an overview of the initial set up of your cloud server user community. It contains the following topics:

- Activate Security Administrator Account
- Adjust the Default Oracle Identity Cloud Service Settings
- Prepare User Community
- Setup Process Summary

3.2.1 Activate Security Administrator Account

Access the Oracle Cloud Infrastructure console and perform the verification of the provisioned environments. Follow the steps described in the Security Administrator Account section.

3.2.2 Adjust the Default Oracle Identity Cloud Service Settings

Locate the Settings menu and review and/or modify Identity Domain settings. Below are suggestions regarding some settings:

- **Domain settings**: Review the default settings; specify whether the primary email address will be also used as a user name (login).
- **Notifications**: You may want to include user names in communication emails. Update notification(s) accordingly (see Notification Update Example: Welcome Email for an example of updating notifications).

  Update the notifications further to include additional details, for example the contact information of the technical support team.
- **Password Policy**: Evaluate the default Password Policy and amend according to your organization's requirements. You may return and modify it later and create multiple policies for different groups of users.
- **Branding**: customize the look of the login page with your company's branding elements (optional).

For more information, see Updating Settings.

3.2.3 Prepare User Community

Explore the Users list. Beside the Security Administrator account you may find a Process Automation group and user. This account is created as part of the service provisioning and is usually linked to the Security Administrator's email address. Process Automation is an internal user for inter-domain communications.

Take advantage of the user import feature to quickly establish user access to the provisioned environments, using the following steps:

- Compose initial lists of users who'll be accessing the environment(s), including:
  - Key members of the implementation team who are likely to have access to the non-production environments
  - Preliminary list of production environment users
- Define Group(s) for Just-In-Time Provisioning (if required). See Setting Up Groups for Provisioning - Identity Domain for more information).
- Browse the Oracle Cloud Services, locate the Application for each environment, and determine the Application Roles that users will be assigned to.
- Download the bulk upload template files and create import files for:
  - Users
  - Groups
  - Application Roles

  See Bulk Upload and Download for more detailed information about uploading and downloading template files.

3.2.4 Setup Process Summary

Note that the following assumes the Security Administrator account has been activated.

- If you wish to delegate the just-in-time provisioning and access/authorization setup, assign administrator role to at least one user per environment (see Updating Security Privileges).
- Access the environment and configure Just-In-Time provisioning according to the product's specifications (see Configuring User Provisioning Rules - OUAF).
  - Setup the Identity Management Integration Master Configuration for Oracle Revenue Management and Billing Cloud Services. Make sure the IAM Groups are the same Groups that were used for the User/Group import files.
- Perform import of Users, Groups and Application Roles using the import files prepared above (see Bulk Upload and Download).
- Setup at least one integration (non-human) user per environment of each Oracle Revenue Management and Billing Cloud Service and communicate the credentials to the implementation team (see Setting Up an Integration User for REST/SOAP Web Services).
- Setup access to production environment for those users who are responsible for legacy data migration.

3.3 Security Administrator Account

This section explains how to set up a security administrator account for user provisioning. It contains the following topics:

3.3.1 Setting Up the Security Administrator Account

The account for the Security Administrator is created during provisioning. The customer provides the name and the email address of the intended security administrator as part of the service order. Once the order is completed the Security Administrator receives a cloud account activation email.

The activation email contains:

- Activation URL
- The user name and the temporary one-time password

Security administrators should use the following procedure the first time they log in:

1. Press the activation link or copy the link into the internet browser's address. You will be redirected to the login page.
2. Enter the user name and the temporary password.
3. Follow the prompts to create a new permanent password.

   Finally, you will be redirected to your Oracle Cloud Infrastructure tenancy services dashboard.

3.3.2 Navigating to the Identity Domain

The Identity Domain can be accessed via the Oracle Cloud Infrastructure portal.

3.3.2.1 Accessing via Oracle Cloud Infrastructure Portal

On the Oracle Cloud Infrastructure Portal dashboard, click the hamburger menu right corner of the screen. Find and expand the **Identity and Security** link. Click the **Domains** option under **Identity**. You'll be redirected to **Domains** portal.

When logging in for the first time, the **Domains** list will be empty. You should select a compartment from the **Compartments** list on the left navigation pane. Pick the root compartment and the **Domains** list will be reloaded. If there is only one domain (named Default) on the list, select it. If you observe multiple domains, select the Oracle Cloud Services domain. The Domain Overview screen opens. It contains a general information such as the domain’s name and description, domain type, and home region.

Note the Domain URL field. To retrieve detailed information about Identity Domain, compose discovery URL by concatenate the domain URL (without port) with `/.well-known/idcs-configuration?region=true` and access it in your browser.

3.3.3 Verifying Security Administrator Identity Cloud Service Access

Expand the **Security** topic on the navigation pane and click **Administrators**.

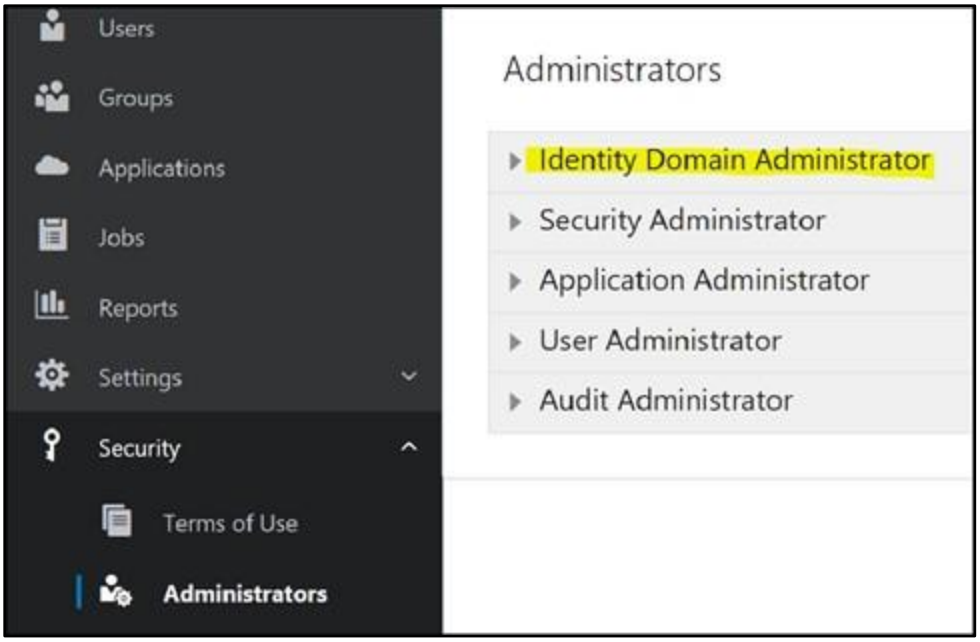

Figure 14: Administrators

On the page, expand the **Identity Domain Administrator** section and verify that your name is on the list of Identity Domain Administrators.

3.3.4 Verifying Subscription Contents

Click **Oracle Cloud Services** on the navigation pane. The main panel displays a list of available applications.

The list contains Applications representing each environment in the subscription, for example Production or Test. The Application name comprise of service acronym, environment "type" and tenant identifier, for example ORMBCS-PROD (C123456).

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.

The list of applications may also include an instance of Oracle Cloud Object Storage.

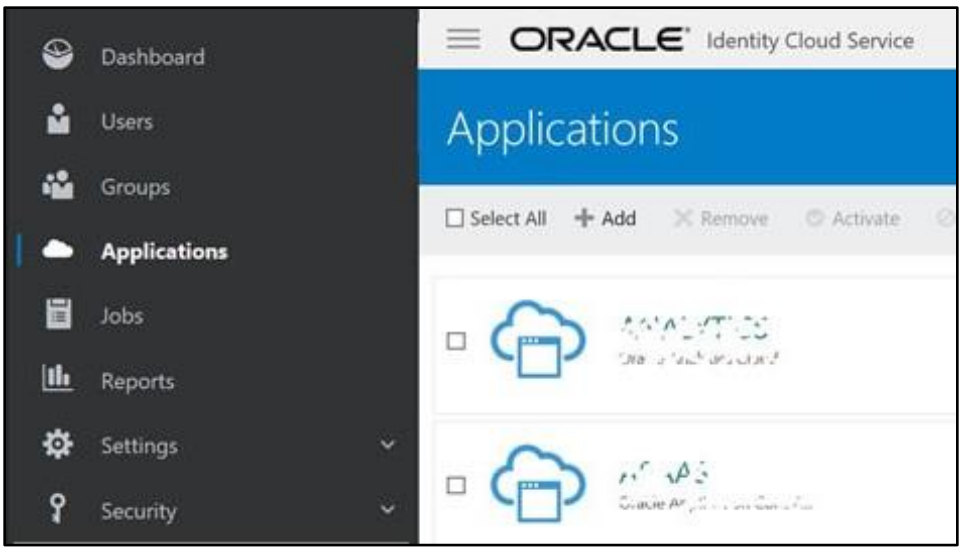

Figure 15: Applications

3.3.5 Exploring the Applications

Click on one of the applications on the list and display the single application. Most of the information is system-generated and read-only. Users and Groups should be assigned to Application Roles within the application to gain access to the environment.

Click the **Application Roles** tab and review available Application Roles.

While the application represents a single environment, the different Application Roles represent different components within the environment. To authorize user's access to a certain component the user has to be assigned to a corresponding Application Role. Application Roles include:

- Online Application Access
- Web services REST/SOAP API
- Access to supporting Applications such as BI Publisher and SQL Developer

Web Application Roles also used to support coarse-grained authorization in the target component, for example the BI Content Author versus an ordinary BI Consumer.

3.3.6 Verifying Access to Object Storage

See Object Storage Setup with Identity Domains for more information about object storage.

3.3.7 Verifying Security Administrator Access to Service

As part of the service activation notifications, the security administrator is provided with URLs for all components within Production and Non-Production environments. Perform the following steps to verify the access:

- Assign the security administrator user to both online-related and web services Application Roles in each environment (Application Role description indicates whether the access is given for online or for the REST/SOAP API).

- Access each environment via the URL for the online application; this action will provision your user into the Oracle Revenue Management and Billing Cloud Service application. Modify your user: add default data Access Role and Group and default To Do Role.

3.4 User Management Procedures

This section describes general procedures related to managing users and groups. It contains the following topics:

- User Onboarding
- Advanced User and Access Management
- Updating Settings

3.4.1 User Onboarding

Users and groups are managed separately for each Identity Domain and not replicated automatically across domains. The user for the Cloud Account Security Administrator is always created by the provisioning process in the Default domain.

To onboard new users, navigate to the Identity Domain and find **Users** and **Groups** navigation links located on the left side navigation pane.

3.4.1.1 Setting Up a New User

Click **Create New User** above the **Users** list.

Add User Details

Enter the minimum required information:

- Last Name
- First Name
- Email address

Note: By default, the email address is used as the user name. Uncheck **Use Email as User Name** to enter the User Name manually.

- User Name

Optionally, you can also add User to the existing Groups Click **Create** button to complete the setup. The new user appears on the list.

Note: Additional product-specific setup may be required in order to provide user authorization and Just In Time provisioning. For more information, see User Provisioning for Oracle Revenue Management and Billing Cloud Services.

3.4.1.2 Setting Up a New Security Administrator

There are multiple levels of administrative privileges that can be assigned to a new security administrator:

- Users assigned to the Cloud Account Administrator administrative role are authorized to perform all identity and not identity-related administrative functions within Oracle Cloud Infrastructure tenancy including manage all Identity Domains.
    - Create a user for the new Cloud Account Administrator in the Default Identity Domain and add this user to the Administrators Group.
- Users assigned to the Domain Administrator administrative role are authorized to perform administrative functions within a specific Identity Domain.
    - Create a user for the new Domain Administrator in the Identity Domain (except Default) and add this user to the Domain Administrators Group.
- Users assigned to the Identity Domain administrative role(s) are authorized to perform specific administrative functions defined by these roles within a specific Identity Domain.
    - Create a user in the Identity Domain. Navigate to **Security**, **Administrators** and assign the user to one or more administrative roles.

3.4.1.3 Managing Groups

Click the **Groups** link on the left navigation panel to display a list of available groups.

Add New Group

To add a new group click **Create Group**.

Enter the **Group Name** and **Description** and save the new group.

Add Users

To add users to a group, click on the group name on the list or use the Edit menu action. The portal displays the selected group record.

Click the **Users** tab to add one or multiple users to the group.

3.4.2 Advanced User and Access Management

You manage applications, perform user management, and administer general and security settings also view basic reports with Identity Domains.

3.4.2.1 Managing Users

In addition to add and remove, the following single and multi-record actions are available on the **User** page:

- Resend Invitation
- Reset Password
- Activate/Deactivate User
- Update User information and preferences (on individual User record)
- Unlock User (on individual User record)

In addition, the following actions are available:

- Import Users
- Export Users

Resend Invitation to Service

The initial email invitation to access the service is sent to the user immediately upon user record creation. This invitation is expired after certain period.

Reset Password

Resets a single, multiple, or all passwords. Users will receive a password reset email notification immediately.

Activate/Deactivate User

User can be temporarily activated or deactivated. The email notification is sent to the user immediately. If the deactivation lasts longer than the password rotation period the activation will cause password reset.

Update User Information and Preferences

Updates details for individual users. In addition to the minimum required information provided during user creation the following details can be updated:

- Title
- Time Zone and Address including Country
- Preferred language
- Alternative email and contact information

Unlock User

Unlocks a locked user account. The user's account may be locked for various reasons for example after too many unsuccessful login attempts. Select **Unlock User** from the **More** menu to unlock the locked account.

3.4.2.2 Managing Groups

Access the **Groups** portal from navigation pane. Select one or more entries from the list. In addition to add and remove, the following actions are available:

- Import Groups
- Export Groups

3.4.2.3 Managing Applications

The applications that represent the provisioned services are pre-created during the service order processing. The Application Roles are also pre-configured.

The administrator is authorized to activate or deactivate certain applications, assign users to Application Roles, and perform import and export of application role's members.

3.4.2.4 Bulk Upload and Download

Identity and Access Management supports import and export of users, groups, and application roles membership. The bulk identity data operations may be required for the fast user onboarding or as part of the federated single sign on setup.

The **Import** and **Export** actions are available on multiple pages:

- **Users** page:
  - Import all or a selected set of users
  - Export information for one or more users
- **Groups** page:
  - Import all or a selected set of groups and their member users
  - Export one or more groups and their member users
- **Application → Application Roles** page**:**
  - Import all or a selected set of application role's membership (users and groups)
  - Export one or more application role's membership (users and groups)

Importing

1. Navigate to the **Users**, **Groups**, or **Applications** (**Application Roles** tab) page as appropriate.
2. Click **Import** on the top actions bar.
3. Download the sample file.
4. Review the sample file. Note that you can provide different type of information:
   - Users
   - Groups
   - Application Roles Membership
5. Populate the file with user's data and save.
6. Import the file into **Identity Domain**.

Exporting

1. Navigate to the **Users**, **Groups**, or **Applications** (**Application Roles** tab) page as appropriate.
2. Select entries for the export.
3. Click **Export** on the top actions bar. A notification email is sent as soon as the export job is completed, and the file is available for the download.

3.4.3 Updating Settings

Use the navigation bar to expand the **Settings** topic. The following settings can be modified:

- **Default Settings**: Used to manage default time zone, language, and audit setup.
- **Session Settings**: Used to manage session expiration.
- **Password Policy**: Used to amend the default password policy according to your requirements.

- **Notifications**: Used to modify the default email notification templates provided with IAM and also enable or disable one or more notifications.

Notification Update Example: Welcome Email

The email notification templates are provided for multiple identity management-related events. The default content of these notifications can be amended to reflect customer's business requirements.

For example, there are two approaches to user account creation: using email address as a user name as opposed to using a manually defined user name. The former means the user knows what to specify on the login screen (email address). The later means the user name that is created manually by the security administrator has to be communicated to the user. In order to communicate the **user name** in the **Welcome** email perform the following steps:

1. Select **Notification** on the left-side navigation pane.
2. Click on the **Email Templates** tab.
3. Expand the **Welcome** template:

   In the email body the greeting line reads: Hello ${user.displayName}

4. Modify the greeting to include the user name (login) as follows:

   ```
   Hello ${user.displayName} (${user.userName})
   ```

Note that other substitution variables are also available for use in the notifications. To explore the variables available to a specific template, click the **Email Variables** link above the email body editor.

3.4.3.1 Updating Security Privileges

Use side navigation panel to expand the **Security** topic. Use **Administrators** link to add or remove administrative privileges from the users.

3.4.3.2 Sign-On Policies for Online Access

Identity and Access Management supports the ability to restrict web-browser-based access to the applications based on set of conditions including the user's client IP addresses. Both IP "blocklist" and "allowlist" approaches are supported.

- A blocklist defines a set of IP addresses that are blocked from the access. This approach should be used when the "bad" IPs are well-known and permanent, and the list is not expected to change very often.
- An allowlist defines the set of IP addresses that are permitted to access the application while everybody else is denied access.

In addition to IP addresses, the following can be allowed or blocked:

- Specific users
- Groups
- User's administrative role in IAM
- User being authenticated by a specific external identity provider(s)

Note: Sign-On Policies are applied ONLY when user attempts to authenticate to IAM using a web browser. They are not applicable for requests submitted via REST/SOAP API.

Setup a Network Perimeter

A Network Perimeter represents a set of IP addresses, and can be defined as:

- A list of one or more IP addresses
- A range of IP addresses
- One or more IP addresses in IPv4 CIDR notation, which encompass all IP addresses belonging to a subnet. You can also use the IPv4 CIDR notation to see the entire internet: 0.0.0.0/0.

Create Network Perimeters:

- Use side navigation panel to expand the Security Topic
- Locate Network Perimeters
- Add one or more Network Perimeters that define "blocklist" and/or "allowlist" IP addresses

Setup Sign-On Policies

Sign-on policies define the set of rules used for granting the access to the applications. The out-of-box default policy contains a single default rule that grants the access to every authenticated user. You can either modify the default policy or create a new one(s).

Sign-on policy rule definition includes multiple optional conditions to filter the users and an action to **allow** or **deny** the access:

- By authenticating the Identity Provider: Denying/allowing access for users authenticated by specific external IP in case of a federated SSO
- By group membership: Denying/allowing access for specific set of groups
- By being or not being an Identity Domain administrator
- By being one of the explicit list of users
- By the user client's IP address being in one or more of the Network Perimeters

The rules on the policy are evaluated top-to-bottom. The first result halts the evaluation. Meaning if the user satisfies the rule's condition, the rule's action (**allow** or **deny** access) is applied and evaluation ends.

Note: The default rule on the default policy cannot be deleted, therefore it must be modified first.

Example:

Let's assume that the requirement is to:

- Allow access from IP addresses on the company's intranet
- In addition, allow certain administrators to connect from their personal home computers
- Block anyone else

To configure this example:

- Create two new Network Perimeters:
    - **NP1-Company** to represent the intranet: specify an entire subnet using CIDR notation, like, for example, 10.10.0.1/24, which means all addresses in 10.10.0 subnet
    - **NP2-Admins**: specify one or more IP addresses, comma-separated

- Configure Default Sign-On Policy:
    - Modify Default Rule:
        - Set the rule's "and the user's client IP address is" condition to "in one or more of these network perimeters" and specify **NP1-Company**
        - Set the rule's action to "**Allowed**"
    - Add new Rule:
        - Set the rule's "*And is an administrator*" condition to "true"
        - Set the rule's "*and the user's client IP address is*" condition to "*in one or more of these network perimeters*" and specify **NP2-Admins**
        - Set the rule's action to "**Allowed**"
    - Add new Rule
        - Set the rule's "and the user's client IP address is" condition to "Anywhere"
        - Set the rule's action to "**Denied**"

Sample Sign-in Scenarios:

Scenario 1:

An employee is trying to login from the office computer that is connected to the intranet.

- The first rule (the default rule) is evaluated first. The user's IP satisfies the condition by being on the NP1-Company perimeter. The rule's action ("*Allowed*") is applied, and the user is allowed to sign in.

Scenario 2:

The administrator is trying to login with admin's user name from a personal computer whose IP is listed in NP2-Admins perimeter.

- The first rule (the default rule) is evaluated first. The user's IP does not satisfy the condition by being on the NP1-Company perimeter.
- The second rule is evaluated. The user's IP does satisfy both conditions: being and administrator and being on the Np2-Admins perimeter.
- The rule's action ("*Allowed*") is applied, and the user is allowed to sign in.

Scenario 3:

The employee is trying to connect from the home computer.

- The first rule (the default rule) is evaluated first. The user's IP does not satisfy the condition by being on the NP1-Company perimeter.
- The second rule is evaluated. The user's IP does not satisfy any of the conditions: being neither an administrator nor being on the Np2-Admins perimeter.
- The third rule is evaluated. The user's IP satisfies the "Anywhere" condition.
- The rule's action ("*Denied*") is applied and the sign in is blocked. The IAM login error message: "Sign-on policy denies access." is displayed.

See *IAM Documentation* for the detailed instructions regarding Sign-On Policy and Network Perimeter setup.

3.4.3.3 Available Reports

The following reports are available for review and download:

- Successful Login Attempts
- Unsuccessful Login Attempts
- Application Access
- Granted and Revoked Application Roles
- Diagnostics

3.5 User Provisioning for Oracle Revenue Management and Billing Cloud Services

This section describes user provisioning for Oracle Revenue Management and Billing Cloud Services. It contains the following topics:

3.5.1 Overview

Each Oracle Revenue Management and Billing Cloud Services environment included in the subscription contains multiple components:

- Business Applications that run on the Oracle Utilities Application Framework, (OUAF) supports fine-grained authorization to access various features within the Business Application. It stores users and user groups.

  For each user authorized to access Oracle Utilities Application Framework the corresponding application user is created in the Oracle Utilities Application Framework.

  For the online application access, Oracle Utilities Application Framework users are created through Just in Time Provisioning flow.

3.5.2 Pre-Defined Application Roles

The roles listed below are pre-defined in the Applications that represent Oracle Revenue Management and Billing Cloud Service environments. Each role represents an entitlement within the environment and grants user an access to a certain component. New roles may be added with future releases as the Oracle Revenue Management and Billing Cloud Services are expanded into new functional areas.

Application Role	Authorized Access
Online Application User	The user assigned to this role may access online application.

Application Role	Authorized Access
Web Services Access	The user assigned to this role is authorized to access the REST/SOAP APIs.
BI Consumer	The user assigned to this role may access the Analytics Publisher within the environment and view and execute predefined reports.
BI Content Author	The user assigned to this role may access the Analytics Publisher within the environment and author new and view/execute existing reports.
SQL Developer Web Online User	The user assigned to this role may access the SQL Developer Web online and query the database to retrieve the information from both production and conversion schema.
REST Enabled SQL	The user assigned to this role may use cURL utility to invoke REST services and query the database to retrieve the information from both production and conversion schemas.

Note: Additional pre-defined roles for Data Visualization may be provided with specific cloud services. Examples include *CustomerContentCreator*. *CustomerContentConsumer* among others.

3.5.3 Configuring Just in Time Provisioning

Just In Time provisioning is a process that creates application user record in the OUAF-based business applications upon first successful login. The new user is created in the business application based on a pre-defined OUAF Template User. The Template User is determined from the mapping between Groups and OUAF Template Users defined in **Identity Management Integration Configuration**.

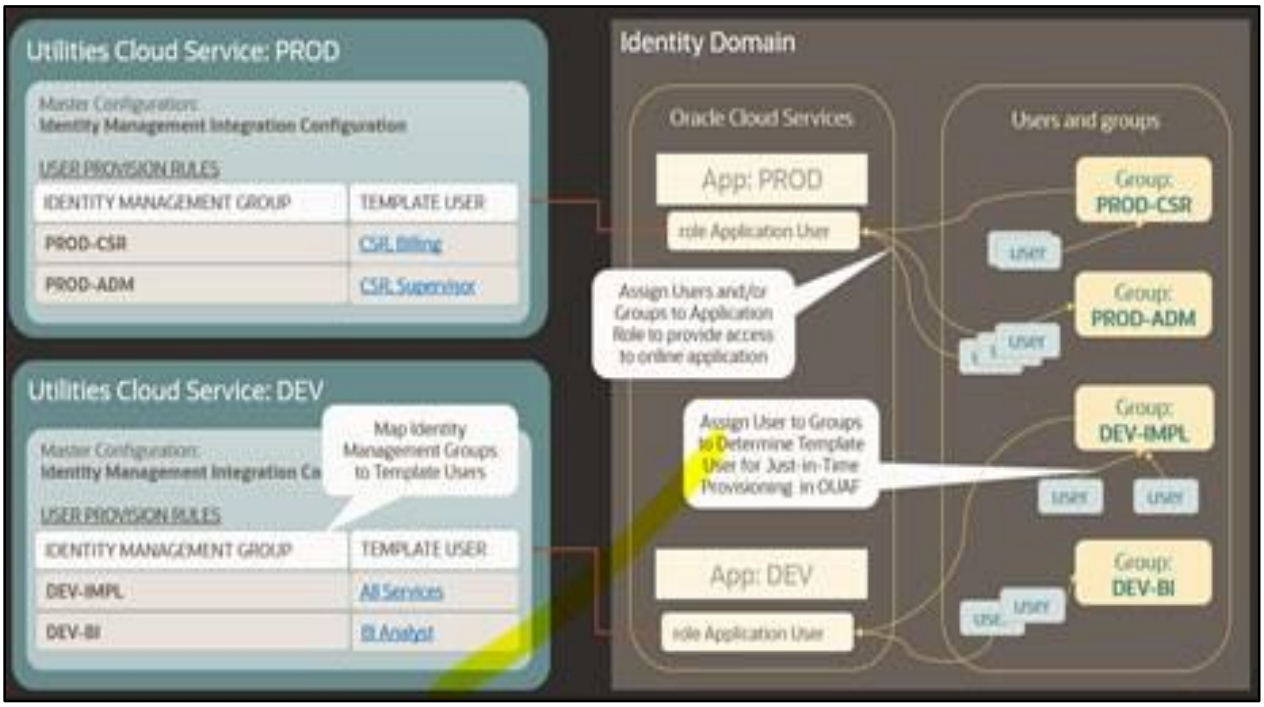

Figure 16: Just In Time Provisioning

Steps to configure Just In Time provisioning:

- Setting Up Groups for Provisioning - Identity Domain
- Configuring User Provisioning Rules - Oracle Utilities Application Framework

3.5.3.1 Setting Up Groups for Provisioning - Identity Domain

The following is a suggested approach to Just-In-Time provisioning.

Create Groups in the Identity Domain that represent broad functional areas and/or authorization level in the service. For example:

- For Non-Production (Development and Testing) environments:
  - Implementers
  - Business Analysts
  - QA Team
  - Security Testing
  - Functional Testing
- For Production environments:
  - Call Center
  - Call Center Supervisor
  - Business Administrator
  - Accounting

3.5.3.2 Configuring User Provisioning Rules - Oracle Utilities Application Framework

To configure Identity Management Integration in the Oracle Utilities Application Framework (OUAF):

- Create Template Users that represent various level of access authorization.
- Review existing Template Users.

  If your intention is to use a Template User to provision integration (non-human) users, you might have to assign Default Access Group to the Template User.
- Map the Groups created above to the Template Users in OUAF in the Identity Management Integration Master Configuration.

  If the Identity Management Integration Master Configuration is not configured at the time the user record is created, the user will be provisioned with K1MINACS (default minimal access).

3.5.4 Creating and Provisioning Users

This section describes steps involved in creating users and providing access to the cloud service's various components.

3.5.4.1 Setting Up an OUAF Security and Access Administrator

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Assign this user to the User Administrator role. See Setting Up a New Security Administrator for more details.
3. After first login to OUAF this user will be provisioned with Template User K1SCRADM (security administrator).

3.5.4.2 Setting Up an Online Application User

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Assign the user to the group that represents the appropriate level of authorization for the environment.
3. Locate the application that is corresponding to the environment.
4. Assign the user to the Online Application User role in the environment.

3.5.4.3 Setting Up an Integration User for REST/SOAP Web Services

REST/SOAP API doesn't perform Just-In-Time provisioning. Users for web services must be created manually in both and OUAF applications.

An email address must be provided as part of user creation:

- It is recommended that this email address is used for non-human user setup only.
- All email notifications concerning user account are sent to this email address.
- Security administrator must have access to this email account.

Perform the following steps:

1. Create a new user or search for and select existing user:
    - Specify the email address allocated for the integration/non-human users.
    - When the activation email is received, reset the user's password, and communicate the email address and password to the integration team.
2. Assign the User to the REST/SOAP Web Services role in the Application that represents the environment.
3. Login to OUAF and create a new User with Login ID = User Name. Assign the user to user groups that provide access to all or selected application services, according to the business requirements.

Notes on integration user accounts management:

- Expiring passwords may cause integration flows to stop working. Reset passwords regularly to avoid eventual outages.
- You may choose to maintain two user accounts for each integration - a "main" account and an "alternate" account - to allow a graceful switch to a new password. When required, first reset password for the "alternate" user while the "main" user is still valid and working; then reconfigure the integration to use "alternate" user credentials and only then reset the "main" account password.
- Oracle recommends that you setup a dedicated integration user account for each production and non-production environment.

3.5.4.4 Setting Up an Integration OAuth Client for REST/SOAP Web Services

External systems may access Oracle Revenue Management and Billing Cloud Service REST APIs using OAuth client. OAuth clients are created by the Oracle Revenue Management and Billing Cloud Operations team (see the *Oracle Revenue Management and Billing Cloud Services Operations Guide* for more information).

To request creation of a new OAuth Client, create a Cloud Operations service request and provide the following information:

- **Environment**(s) where the OAuth client is needed. For example, PROD, TEST01, DEV.
- **Client name suffix**: Use a distinct name that may suggest the functional purpose of the integration, for example METERDATA or whatever is applicable for the integration's business use. If not provided, the default suffix is INTEG.
- **Client description**: Provide a meaningful description of the integration point.
- **Grant Type**: Client Credentials and/or JWT Assertion or both, depending on your integration requirements.
- **Client type (trusted or confidential) and client certificate**: The integration requirements may call for trusted client and the external application may also supply its own certificate.
- **OAuth flow for your intended integration**: Currently supported are *client credentials*, *JWT assertion*, and *authorization* code flows. For the authorization code flow you can also supply your own redirect URL.
- **Scope**: You can define OAuth clients with access to either REST or SOAP APIs or both REST and SOAP APIs.

The Oracle Revenue Management and Billing Cloud Operations team will create the OAuth Client using the input provided in the service request.

Once the client has been created, locate the newly created OAuth Client in the Identity Domian under **Oracle Cloud Services**. The name is composed as `<product><domain><tenant><suffix><sequential number>`.

For example:

```
ORMBCS-PRODC12345CMETERDATA0 , ORMBCS-PRODC12345FIELDSERVICE1
```

Where,

- The client ID and secret can be found in the **General Information** section of the **OAuth Configuration** section.
- The allowed scope can be found in the **OAuth Client** section on the **Configuration** section, under **Token Issuance Policy**.

If your integration implements Client Credentials OAuth flows, the next step is to create an application user in the appropriate Oracle Revenue Management and Billing Cloud Service. Access the appropriate Oracle Revenue Management and Billing Cloud Service application and navigate to the **User** portal.

Create a new user corresponding to the OAuth Client created above:

- Enter the OAuth client ID as the user's **Login ID**.
- Assign **User Group**(s) that will provide the integration with access to the appropriate functionality.

The OAuth Client credentials are now ready to use. When issuing a webservice call, specify the client id, secret and allowed scope that you've determined from the Identity Domain.

Maintaining OAuth Clients Created for Integration

You can delete the OAuth client or regenerate the OAuth client secret by creating a service request with the Oracle Revenue Management and Billing Cloud Operations team. Provide the OAuth Client ID and the Identity Domain URL. The Oracle Revenue Management and Billing Cloud Operations team will perform the requested action on your behalf. See the *Oracle Revenue Management and Billing Cloud Services Operations Guide* for more information about working with the Oracle Revenue Management and Billing Cloud Operations team.

3.5.4.5 Setting Up a User with Access to Analytics Publisher and Data Visualization

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to one of the Application Roles available in the environment:
    - **Analytics Publisher**: Choose one (or both) of the following application roles:
        - BI Consumer
        - BI Content Author
    - **Data Visualization:** Choose one or more product-specific application roles related to Data Visualization features, such as CustomerContentConsumer.

3.5.4.6 Setting Up a User Authorized to Execute Ad-hoc SQL Queries

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to one of the following roles:

- **SQL Developer Web Online User**: Provides access to the online web-based interface that enables user to execute queries.
- **Rest Enabled SQL**: Provides the ability to execute REST calls using `cURL` command.

3.5.5 Cloud Service Implementation User

The environment provisioning process creates an internal (non-human) user account named "K1IPROCESS" that is used by cloud service implementation tools and processes, including configuration migration between environments.

3.6 Using Federated Single Sign-On

This section describes tasks required when using an external identity management system to provide authentication for the application instances within your cloud subscription. It contains the following topics:

3.6.1 Overview

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 should be available after the subscription is live.
- The Federated Single Sign-On only concerns online access; it is not applicable for the integration and other non-human accounts.
- The option to configure federation with existing Identity and Access Management is included with Identity Cloud Service subscriptions as part of Oracle Revenue Management and Billing Cloud Services.

3.6.2 Setup External Identity Provider

Configure a SAML 2.0 external identity provider such as Active Directory Federation Services (AD FS) for federated SSO with the IAM Identity Domain. Configuration steps include:

- Setup the SAML 2.0 Identity Provider.
- Verify Federated Single Sign-On.
- Establish user synchronization between the Identity Domain and the SAML Identity Provider. It is necessary to copy users into Identity Domain because the access to the service is granted by assigning users to the Application Roles in Oracle Cloud Services.
    - Configure Microsoft Active Directory Bridge or implement user data synchronization via REST SCIM API, flat file import, or using one of the pre-defined provisioning Applications from the IAM catalog. See the IAM documentation for more details.

To access detailed configuration instructions provided by IAM:

- Return to the Oracle Cloud Infrastructure console, expand hamburger menu on the top left corner and select **Identity**. Click the **Identity** link and load the **Overview** page. Use one of the quick links to access documentation and tutorials on SAML SSO configuration.

Note on Identity Bridge setup only: Federated authentication is enabled by default. This configuration means the user credentials will be validated against a configured Identity Provider.

When configuring Identity Bridge define the federated authentication as follows:

- To continue validate credentials and maintain passwords and password rules in the external identity management system leave the Federated Authentication checkbox checked.
- To validate credentials and manage passwords in IAM uncheck the Federated Authentication checkbox. IAM will generate the password for the users and send the notification by email (the email attribute must be filled in Microsoft Active Directory and mapped to the Identity Domain).

3.6.3 Service Access for Federated Users

Federated users should be granted access to the environments the same way as the users created directly in the Identity Domain.

See Setting Up an Online Application User for the instructions on how to assign user to the online access application roles.

Possible approaches:

- Process users one by one: locate user in Identity Cloud Service and assign to the application roles.
- Process multiple users:
    - Export users from directly or from the group (see Exporting for more details).
    - Copy the information into Application Role import file and import users and/or groups to the Application Role (see Importing for more details).

3.6.4 Just In Time Provisioning for Federated Users

In the federated SSO scenario the Identity Cloud Service users and groups are imported from the external identity provider's data repository.

- Evaluate the groups created in the Identity Domain as a result of sync with external Identity Provider and determine whether to use them for Just In Time provisioning purpose.
- Login to the OUAF-based application and set up Template Users that represent authorization levels corresponding to the IAM groups synchronized from the external provider.
- Configure the **Group - Template User** mapping in the Identity Management Integration Master Configuration.

See Configuring Just in Time Provisioning for more detailed configuration instructions.

4. Object Storage Setup with Identity Domains

Oracle Cloud Object Storage is a part of Oracle Cloud Infrastructure Storage Services, and it is a required service for Oracle Revenue Management and Billing Cloud Service.

These cloud services uses Oracle Cloud Object Storage as the vehicle to exchange data files with customers during an implementation and in production.

Oracle Infrastructure Services get provisioned separately from Oracle Revenue Management and Billing Cloud Services but are grouped together under the same customer Cloud Account.

Access and administration of Oracle Cloud Infrastructure Services is done via the Oracle Cloud Infrastructure Console. This document describes the tasks that are required for connecting the system to Object Storage and the basic administration that is needed for implementation stages and beyond that.

For more information on Oracle Cloud Object Storage (including concepts, security best practices, and more), see Oracle documentation about Oracle Cloud Infrastructure Services at: https://cloud.oracle.com/iaas.

This section provides information about setup and configuration of object storage for use with Oracle Revenue Management and Billing Cloud Services. It contains the following topics:

4.1 Object Storage Management

This section outlines the basic administration tasks of Oracle Cloud Infrastructure related to Object Storage. It contains the following topics:

4.1.1 Object Storage Structure

This section provides an overview how object storage is structured. It contains the following topics:

4.1.1.1 Compartments

All cloud infrastructure resources are organized in Compartments. A tenancy can include several compartments. A compartment is a logical grouping of resource types. For object storage, compartments help manage the structure of objects that are stored in the cloud. Compartments can have child-compartments which support multi-level hierarchy of resource grouping.

Each compartment is identified by a unique Oracle Cloud ID (OCID). When connecting the system to object storage, the compartment identification is part of the required connection configuration information.

There are no hard requirements as to the structure or number of compartments that should be created. A recommended setup is described later in this document and has reference to compartments as well.

Root Compartment

The Root Compartment is created for each account and is the top level of the compartment hierarchy. The name of that compartment includes the string "(root)" in it.

4.1.1.2 Object Storage Buckets

Oracle Cloud Object Storage is organized in buckets. A bucket is like a folder or a directory that stores one or more objects. Objects can be any file and can includes documents, images, and so on. Each compartment can have one or more buckets. Buckets cannot include other buckets.

An example of Object Storage structure can be:

- Root Compartment
  - Compartment A
    - Child Compartment A1
      - Bucket A1-1
      - Bucket A1-2
      - Bucket A1-3
    - Bucket A1
  - Compartment B
    - Bucket B1
    - Bucket B2

Bucket names are unique within a tenancy which means that the same bucket name cannot be used in different compartments. Compartments have a unique identifier (OCID) so they are in fact unique within the tenancy. The system can be configured to connect to any compartment and bucket that you define. This configuration is described in the next section.

Virtual Folders

While the structure of buckets is flat across the tenancy, you can simulate a hierarchy within a bucket by using the "/" notation in the object name. For example, you can have the following objects "A/file1.dat" and "B/file1.dat" inside a bucket named "ABC". While bucket "ABC" will physically have 2 objects in it, it can also be represented as also having "A" and "B" virtual folders, both containing a file named "file1.dat".

4.1.2 Security and Access Management

Oracle Revenue Management and Billing Cloud Services security is managed by Oracle Identity Domains. Each Cloud Account has a default Identity Domain but can have multiple domains.

When a new Cloud Account is created, the Default Identity Domain is where you would typically define your security settings for managing your infrastructure services (including Object Storage). While additional Identity Domains can be created, this section will focus on activities and settings in your default domain. Identity Domain management is done via the Oracle Cloud Infrastructure Console (OCI Console).

4.1.2.1 Accessing the Oracle Cloud Infrastructure Console

Once your cloud service has been provisioned, you should receive an email with the link to your Cloud Account. That link will take you to your Oracle Cloud Infrastructure (OCI) Console. In your OCI Console you will have access to manage your infrastructure resources as well as your users and their access to the various resources.

4.1.2.2 Managing Users

There are two types of users that should have access to infrastructure services (Object Storage being one of these): Human users and System Account users.

Human users should typically include two types of users:

- Administrator level personnel that use the OCI Console to manage security and the various infrastructure services (such as Object Storage).
- Business users that need access to various resources as part of the normal operations of the business. For example, such users may need access to create, modify and delete Objects in Object Storage but will not have access to administrative functions beyond that.

System Account users are applications that use an API to access the various services but do not have access to the OCI Console.

Human users will typically require email information as part of their registration while System Account users might not.

Note: Please see your Identity Domain settings to set whether an email is always required for new users. If an email is required, you will need to assign a special email address to the System Accounts that will be required for your cloud service connection to Object Storage.

Both Human users and System Account users should be assigned to User Groups that together with Policies define their access rights to various resources provided as part of your cloud service.

The process of creating a new user is described in previous sections. This section focuses on users' unique attributes, groups and policies that will govern user access for both, Human and System Account users.

User Identification

A User is identified by an OCID key that is displayed underneath the user name. This is especially important for System Account users when configuring the connection from your cloud service to Object Storage. The OCID is the unique identifier of the user when making API calls to various infrastructure services, including Object Storage.

User API Keys

While any user can have registered API keys, they are required for System Account users that will be used for API access. The API key registered for a user is the public portion of an encryption key pair (private/public) in PEM format.

To register a public key for a User:

1. From the **User** list in your OCI Console, under your default **Identity Domain**, select the **User** name to go to the **User** details page.
2. Select the **API Keys** option from the **Resource List** on the left for that User.
3. Click **App Public Key**.
4. Select the **Paste Key** option to paste the public key content into the page and click **Add**.

   There are other options to import a public key, including the actual generation of a key pair in OCI. The API keys that will be registered for Object Storage access from your cloud service will require the **Paste Key** option.

4.1.2.3 Managing Groups

Security management is done in Oracle Cloud Infrastructure by User Groups. Oracle Cloud Infrastructure includes an Administrator User Group that is predefined and contains the initial administrator user.

Adding a New User Group:

1. To add a new user group, use the upper left menu in the **Infrastructure Console**, select **Identity & Security**, then **Domains** (under the **Identity** section). Make sure you select the root compartment and from the domain list select your default domain.
2. Under the **Identity Domain** section select **Groups** and click **Create Group** to create a new group.
3. Provide a **Name** and a **Description** for the group. Tags are optional and are not covered in this document.

Adding Users to a User Group:

Users can be added to user groups in two ways:

1. When editing a user group record, you can add a user from the **Users** section by selecting **Users** from the resource list and clicking **Add Users to Group**.
2. When editing a user record, select the **Groups** option from the **Resource** list and click **Assign Users to Group**.

4.1.2.4 Managing Policies

Policies can be used to enforce access rights for Users that are a part of a User Group. Similarly, to Compartments, Policies are managed at your tenancy level and not at the Identity Domain level (e.g. for Users and Groups).

Policies are defined using the **Identity**, **Policies** menu.

Using policy definitions, you can define the access rights to your infrastructure services, for example, Object Storage. You can define what compartment or bucket user groups have access to, and the type of access (read, write, and so on).

Policies can apply to specific compartments or the root compartment, in which case it will apply to all the compartments. A policy is a collection of statements with specific syntax that describe access rights to resources. For example, in a policy, you can define that a certain user group has access to create and delete buckets and objects in a certain compartment.

See *Oracle Cloud Infrastructure Documentation* for Identify and Access Management to find out more about policies.

4.1.3 Tenant Information

Information about the tenancy is displayed when selecting **Governance & Administration** from the left side menu in your OCI Console and then selecting **Tenancy Details** under the **Account Management** section.

The information displayed is important for connecting the system to Object Storage, and includes:

- **The OCID key of the tenancy:** This is the tenancy identification.
- **Home Region:** This is the main data region selected for this tenancy. Additional data regions added to this tenancy can be defined.
- **Object Storage Namespace:** This identifier is pre-generated and is needed for the connection of the system to Object Storage.

4.1.3.1 Regions

When a cloud account is created, a Home Region is assigned to it. This will be the Home Region you selected when you activated your order and created the account. The Home Region is the main data region that is linked to that account. Additional data regions can be subscribed to for the tenancy if access to regions outside the home regions are required.

The list of all available regions is displayed by selecting **Region Management** under the **Account Management** section of the **Governance & Administration** page. Clicking **Subscription** for a region will add that to the list of available regions for this tenancy. All administration tasks will be conducted at the home region but will be synced to the other regions automatically. Please note that when connecting the system to object storage the region must be identified as well.

4.1.4 API Access

Oracle Cloud Object Storage can be accessed via the **Infrastructure Console** or via three types of APIs:

- Command Line Interface (CLI)
- REST calls
- Java SDK

The system connects to Object Storage using REST calls to the Object Storage endpoints that are documented for each of the data regions to which your cloud service has access. For more information about Object Storage APIs, see *Oracle Cloud Infrastructure Object Storage Documentation* (go to: https://cloud.oracle.com/storage and select the **Documentation** tab).

4.2 Connecting to Oracle Cloud Object Storage

The system supports and manages connections to Object Storage via metadata configuration. The system can connect to any number of Object Storage locations and Tenancies.

REST API calls issued by the system, to interact with the Cloud Object Storage, require an API key signature. The system is designed to have a unique private/public key pair for each environment that connects to Object Storage. This means that each system environment should have a unique System Account user defined in your default Identity Domain with a registered unique API Key.

Currently the system supports accessing files on Object Storage via batch processing. Referencing a file location as Object Storage is done using a special notation.

This section contains the following topics:

For additional information, see **External File Storage** help topic in the Oracle Revenue Management and Billing Cloud Service Online Help.

4.2.1 Object Storage Connection Configuration

Each connection configuration is represented in the system via the File Storage Configuration extendable lookup (F1-FileStorage). Each value for that extendable lookup should contain the information described below.

To configure a new connection, go to the Extendable Lookup portal by selecting **Admin**, then **General**, then **Extendable Lookup**, then **Search**, and search for "File Storage Configuration". After selecting it, click **Add** to add a new value.

When adding a new value, select the Oracle Cloud Object Storage file adapter and provide the following information:

- **User**: The System Account user identification (OCID Key) that is used for that connection.

  A unique System Account user ID should be defined for each system environment (for example Dev, Test, Prod) that is connecting to that object storage tenancy. This System Account user should not be used for other purposes.

  If one system environment is required to connect to multiple object storage tenancies, there should be a different System Account user ID for each of these tenancies.

- **Tenancy**: The tenancy ID (OCID Key) of the object storage tenancy.
- **Compartment**: The compartment ID (OCID Key) of the compartment for that connection.

  Each compartment can have a separate connection configuration, but this is not mandatory. In fact, the compartment ID is optional for many Object Storage operations.

However, it is recommended that you provide a compartment ID value in that field for future supported operations that might require a reference compartment, and as a good self-documenting configuration practice.

You can provide the value of a parent compartment for a connection to Object Storage buckets within that compartment or all its sub-compartments. For example: if you have a compartment "A" with 2 sub-compartments. "AB" and "AC" and you have the same security access requirements for buckets in compartment "A", "AB" and "AC" you can specify the OCID of compartment "A" in your connection configuration details instead of creating separate connection configurations for "AB" and "AC".

- **Namespace**: The Namespace of the object storage tenancy.
- **Key Ring**: The Key Ring name that was created in the system. See API Key Management for more information.
- **Region**: The region of the object storage tenancy for that connection. Reminder: object storage tenancies can have multiple regions if additional subscription was done.
- **Bucket Name Prefix**: A name prefix that will be added to the bucket name of file paths referencing object storage (see Referencing Files on Object Storage for more information).

4.2.2 API Key Management

Secured access to Object Storage is accomplished by using API Signature Key. Each configured connection to Object Storage includes a Key Ring. A key ring is an object that hold a set of private/public encryption key pairs. Object Storage connections can share the same key ring and even the same key in the key ring for the same system environment.

For example, key ring A can be defined and used in all the system environments: Dev, Test, and Prod. However, the key pairs inside the ring must be different in each of the environments. The connections defined for Object Storage can all use the same key ring A in all the environments since the actual key pair that is used in each environment, is different. To create a new key ring, select **Admin**, then **Security**, then **Add Key Ring**. Make sure to generate a key pair in that ring after creating it.

4.2.2.1 Registering the API Key

Once a key ring has been created with an active key pair, click **View** for the Public Key of that key pair to copy the public key content. That content should be pasted into the System Account user API Key in your default Identity Domain (see the User API Keys section in Security and Access Management of Object Storage Management).

4.2.3 Referencing Files on Object Storage

Reference to Object Storage can be used anywhere that a file location reference is allowed in the system.

The format is `file-storage://<File Location>/<Bucket>/<Filename.ext>`, where:

- `<File-Location>`: The File Storage Configuration extendable lookup value defined for that file. This will include the compartment identification.
- `<Bucket>`: The object storage bucket in the compartment that is defined as part of the File Storage Configuration extendable lookup value.
- `<Filename.ext>`: The name of the file.

For example, the "`payment_info.dat`" file in the "Payment-Upload" bucket in a compartment that is referenced in the "AB-Payments" File Storage Configuration extendable lookup value can be referenced as "`file-storage://AB-Payments/ Payment-Upload/payment_info.dat`".

4.2.3.1 Using the Bucket Name Prefix

If you set the Bucket Name Prefix in the File Storage configuration, any file path referencing this configuration will be automatically revised at runtime, adding the name prefix to the bucket name. This allows you to define different name prefix for buckets for each environment (or for production vs non-production environments) and keep your file paths for your batch jobs the same in each environment. For example:

- You can create all your non-production buckets with a "NP-" name prefix, and all your production buckets without a name prefix.
- You can then define a File Storage configuration named "OS-APP" in each of your environments and set the **Bucket Name Prefix** to:
  - "NP-" in all the non-production environments
  - Blank in the production environment
- When you will use a file path reference on your batch jobs, for example "`filestorage://OS-APP/AB-Payments`" then:
  - When the job related to that file runs in a non-production environment it will reference the payment files in the "NP-AB-Payments" bucket
  - When the job runs in the production environment it will reference the "AB-Payments" bucket

4.3 Recommended Object Storage Structure for a New Implementation

This section describes a recommended configuration and structure for your Object Storage tenancy for your service implementation. Using the recommended setup can simply the initial implementation and testing activities of your new service but they are not mandatory. Furthermore, you can start with the recommended setup and adjust it per your implementation needs. See the following topics in the Oracle Revenue Management and Billing Cloud Service Online Help:

- Object Storage
- Process Automation Tool
- Data Conversion

4.3.1 Security Considerations

The system connection to Oracle Cloud Object Storage is governed by a combination of User, User Group (optional) and Access Policies that are defined in your default Identity Domain (see the Object Storage Management section for more information). As a reminder, the User ID details are provided as part of the File Storage Extendable Lookup value in the system.

4.3.1.1 Compartments

It is recommended to divide your resources amongst several compartments:

- **Production Compartment**: This compartment includes all the production resources (such as object storage buckets and objects that store production data).
- **Non-Production Compartment**: This compartment includes all the nonproduction resources used during the implementation and testing phases.
- **Shared Compartment**: This compartment is used to hold resources that are used by special activities or processes and can be accesses by production and non-production users. A good example of that can be configuration data (that can be exported from a testing environment and moved to the production environment when ready, using the Configuration Migration Assistant) or conversion data that can be used in both production and non-production environments (during the implementation phases).

4.3.1.2 Users

It recommended that each system environment uses a unique System Account user ID so that access rights to production vs non-production files or objects can be enforced for that tenancy. Each System Account user will have its own API Key registered. Human users should be created if needed to manage the tenancy resource and to perform the daily operations needed for the system (such as uploading files into Object Storage). All users should be assigned to a user group, which will simplify the security access definitions.

4.3.1.3 User Groups

It is recommended to assign the users to several groups, for example:

- **Application Access User Group for Production**: This group includes the System Account users assigned to the production system environment. These users will access object storage via API calls.
- **User Access User Group for Production**: This group includes all the Human users that will need access to object storage production information. These users will typically access object storage via the OCI Console.
- **Application Access User Group for Non-Production**: This group includes the System Account users assigned to the non-production system environments. These users will access object storage via API calls.
- **User Access User Group for Non-Production**: This group includes all the Human users that will need access to object storage non-production information. These users will typically access object storage via the OCI Console.

These groups can be referenced when defining the security policies for production and non-production access.

4.3.1.4 Policies

It is recommended to create Policies to control access to resources based on:

- **Production vs Non-Production**: For example, it is recommended to restrict access to production resources only to production users.
- **System Account vs Human users**: For example, it is recommended to restrict certain operations from System Account users (such as the ability to delete buckets).

4.3.2 Recommended Setup for a Single Cloud Service

If you are using a single Oracle Revenue Management and Billing Cloud Service, consider the following recommended setup.

4.3.2.1 Oracle Cloud Infrastructure - IAM and Object Storage

Compartments and Buckets

- Root Compartment
  - ORMBCS-Prod (Compartment)
  - ORMBCS-Non-Prod (Compartment)
  - ORMBCS-Shared (Compartment)
    - CMA-Files (Bucket)

      [for the system Configuration Migration Assistant]
    - CONV-Upload (Bucket)

      [for Data Conversion]
    - CONV-Output (Bucket)

      [for Data Conversion]

System Account Users and User Groups for Object Storage Access

- ORMBCS-DEV (for the Development environment)

  [part of User Group ORMBCS-OSNonProdApp]
- ORMBCS-TEST (for the Testing environment)

  [part of User Group ORMBCS-OSNonProdApp]
- ORMBCS-PROD (for the production environment)

  [part of User Group ORMBCS-OSProdApp]

Additional environments will each have their own unique User with the "ORMBCS" prefix and will be a part of the ORMBCS-OSNonProdApp User Group.

Policies for Object Storage

- Policy for System Account users access to object storage in the Production Compartment:
  - Typically defined under the root compartment.
  - Open only to production user groups.
  - Allows read access to buckets and read, create, modify, and delete access to objects in the Production Compartment and the Shared Compartment.
- Policy for System Account users access to object storage in the Non-Production Compartment:
  - Defined under the root compartment.
  - Open only to non-production user groups.
  - Policy details can resemble the production policy or be less restrictive in terms of access allowed for buckets.
- Policies for Human users can be like the policies for System Account users but can allow more access for managing compartments and buckets as needed. These policies will be typically separated into production vs non-production resource access.

4.3.2.2 Example: Oracle Revenue Management and Billing Cloud Service

The following example references the setup in the Oracle Revenue Management and Billing Cloud Service application outlined above.

File Storage Configuration

The following File Storage Configuration extendable lookup values should be defined to correspond to the cloud infrastructure setup above:

- OS-SHARED: This value will point to the Shared Compartment:
  - The user ID will be different in each environment (ORMBCSDEV, ORMBCSTEST, ORMBCSPRODCCS-DEV, ORMBCS-TEST, ORMBCS-PROD)
  - The key ring can be the same in all environment, but each environment key ring will have different key pairs (generated separately in each environment).
- Additional values can be defined based on the file location your specific processes will need to access, for example:
  - OS-Payment: for Payment upload interface
  - OS-MR-Up: for Meter Reads upload interface
  - OS-MR-Dl: for Meter Reads download interface
  - The Extendable Lookup values (the name) will be the same in each environment but some of the information that is defined for them will be different in each environment:
    - User ID, compartment (Prod vs Non-Prod) and keys

4.3.3 Recommended Setup for Multiple Cloud Services

If you are using multiple Oracle Revenue Management and Billing Cloud Services and you are still using a single Oracle Cloud Infrastructure tenancy (and therefor single Object Storage tenancy), then:

- Duplicate the Cloud Infrastructure setup (compartments, buckets, users, groups, policies, etc.), one set with the ORMBCS1 name prefixed and one set with the ORMBCS2 name prefix.
- The setup in the Oracle Revenue Management and Billing Cloud Service (ORMBCS1 or ORMBCS2) would be identical for both. The differences will be in the references to the various Cloud Infrastructure resources prefixed with ORMBCS1 or ORMBCS2, for example:
    - OS-SHARED in ORMBCS1 will point to ORMBCS1-Shared Compartment with User ORMBCS1DEVCCS-DEV/TEST/PROD.
    - OS-SHARED in ORMBCS2 will point to ORMBCS2-Shared Compartment with User ORMBCS2DEVCCS -DEV/TEST/PROD.

4.4 Initial Testing of Object Storage Connectivity

This section contains step by step instructions for initial testing of your connection between your cloud service and your object storage. The instructions represent a simple setup for testing the connection to object storage. These instructions do not represent the complete recommended setup that was described in previous section.

1. Log into your OCI Console using credentials provided to you by your security administrator:
    a. In the **Identity & Security** menu section, select **Domains** and then select your default domain and from the **Identity Domain** menu, select **Users**:
        i. Create a new user named "INIT-TEST" (Take note of the user OCID).
        ii. Add that user to the Administrator user group.
    b. In the **Identity & Security** menu section, select **Compartments**:
        i. Create a new compartment named "INIT-TEST" (take note of the compartment OCID).
    c. In the **Storage** menu section, select **Buckets**:
        i. Select the INIT-TEST compartment in the **Compartment** field under the **List Scope** section.
        ii. Create the following buckets under the INIT-TEST compartment: CMA-Files
    d. In the **Governance & Administration** menu section, select **Tenancy Details** (under Account Management):
        i. Take note of the tenancy OCID (under **Tenancy Information**)
        ii. Take note of the namespace (**Name** field under **Tenancy Information**)
        iii. Take note of the home region

2. Log into the Utility Cloud Service development environment (DEV), using credentials provided to you by your security administrator:
    a. Go to the **Key Ring** portal (use the Menu Search option):
        i. Add a new Key Ring named "INIT-TEST"
        ii. After creating the new Key Ring, click **Generate Key**.
        iii. In the **Key Pair** section, choose the **Activate** action for the new generated Key Pair.
        iv. Click **View** to get the public key portion of the key pair.
        v. Copy the full content of the public key displayed in a popup window, save it in a text document. You will use this later.
    b. Go to the File Storage Configuration extendable lookup and search for a value of OS-SHARED.
    c. Edit that value and enter the following information:
        i. **User**: The user OCID of INIT-TEST User from step #1.
        ii. **Tenancy**: The tenancy OCID from step #1.
        iii. **Compartment**: The compartment OCID of INIT-TEST Compartment from step #1.
        iv. **Namespace**: The namespace noted in step #1.
        v. **Key Ring**: Search for the INIT-TEST key ring created above and select it.
        vi. **Region**: The home region noted in step #1.
        vii. Click **Save**.
    d. Go to the **Master Configuration** portal (use the Menu Search option):
        i. Look for the **Migration Assistant Configuration** master configuration.
        ii. Make sure that the **Import** and **Export** directories have the following value: "`file-storage://OS-SHARED/CMA-Files`"
3. Log back into your OCI Console using credentials provided to you by your security administrator:
    a. In the **Identity & Security** menu section, select **Users**:
        i. Select the INIT-TEST user created earlier.
        ii. In the **API Keys** section, click **Add Public Key**.
        iii. In the popup window, select the **Paste Key** option and paste the public key value saved in previous step (the public key portion of the key pair generated in the Oracle Revenue Management and Billing Cloud Service application), and click **Add**.

4. You are ready to test the object storage connectivity. Log back into the Utility Cloud Service development environment (DEV), using credentials provided to you by your security administrator:
    a. Go to the **Migration Request** portal (use the Menu Search option).
    b. Search for a Migration Request named Users (F1-Users).
    c. Click **Export** for that request (Users).
        i. In the popup window enter the file name "`init_test`" (for example)
        ii. Click **Save**. You will be directed to the **Migration Data Set Export** page.
    d. Go to the **Batch Job Submission** portal and submit a job with the F1-MGDPR batch code. When the job ends, go back to the **Migration Data Set Export** portal, and check the status:
        i. If the status changed to Exported, log into the Oracle Cloud Infrastructure Console, navigate to the CMA-Files object storage Bucket under the INITTEST Compartment and check that there is a file called `init_test.cma` there.
        ii. If the file exists, the test is successful!
5. If the connectivity test was successful, proceed with the overall setup of the Object Storage and your Cloud Service application per the recommended setup above.

4.5 Cross-Region Disaster Recovery Considerations

This section outlines the considerations for Object Storage connection and configuration in case the cross-regional disaster recovery option has been enabled for your system. This section contains the following topics:

4.5.1 Home and Disaster Recovery (DR) Regions

Your system has a Home Region, which is the data region that it was initially provisioned at. This will be referred to as the System Home Region. When cross regional disaster recovery is enabled for your system, it will have a designated disaster recovery (DR) region. The disaster recovery region is the data region that your system will be switched to in case your home region is no longer available. This will be referred to as the System Disaster Recovery Region.

Your Oracle Cloud Infrastructure (where your Object Storage resides) also has a home region, which will be referred to as the OCI Home Region. In addition to that, your Object Storage might reside in a different region than your OCI Home Region (Object Storage is a regional service and any cloud account can subscribe to more than one region) the region where your Object Storage will reside and be used for your system will be referred to as Object Storage Home Region.

Home regions examples:

- #1 Typical new account:
    - System Home Region: US-Ashburn
    - OCI Home Region: US-Ashburn
    - Object Storge Home Region: US-Ashburn
- #2 New service to an existing Oracle Cloud Infrastructure account:
    - System Home Region: US-Ashburn
    - OCI Home Region: CA-Toronto
    - Object Storage Home Region: US-Ashburn

If your system has a designed disaster recovery region, it will make sense for your object storage to have a designated disaster recovery region as well, which will be referred to as the Object Storage Disaster Recovery Region. In most cases the System Home Region will be the same as the Object Storage Home Region, but it could be different if it was chosen to be different. The same is true for the System Disaster Recovery Region and the Object Storage Disaster Recovery Region. Selecting an Object Storage Disaster Recovery Region will be covered in the next section.

Note: If the Object Storage Home Region is different that the System Home Region, you can skip this section since the cross-region disaster recovery procedures will not affect your object storage and will not affect your system connection to object storage.

4.5.2 Preparing your Disaster Recovery Region

If cross-region disaster recovery was enabled for your system, it will be automatically set up to be ready for a disaster event in terms of availability of resources on your System Disaster Recovery Region, according to your service level agreements.

It is your responsibility to make sure that your object storage is ready as well.

Since Object Storage is a regional service, there is no automatic disaster recovery for that. Assuming your Object Storage Home Region is identical to your System Home Region, you need to plan for the eventuality that this region might become unavailable and so you will need to have your object storage available on another region.

The first thing you will need to do is to subscribe to an additional data region to be your Object Storage Disaster Recovery Region.

To subscribe to an additional region, you should do the following:

1. In your OCI Console, in the **Governance & Administration** menu section, select **Region Management** (under Account Management) and look at the list of additional available data regions. Select the data region to designate as the Object Storage Disaster Recovery Region (is it recommended to have it identical to your System Disaster Recovery Region, if possible).
2. Your request for subscription to a new data region will be processed and when it is completed, you will see your new region in the list of available regions.
3. You will also be able to switch to this data region in your OCI Console via the **Region** drop-down list.

4.5.2.1 Copying Your Object Storage Bucket Structure

Your cloud security definitions (i.e., users, groups, policies, and compartments) are all maintained in your OCI Home Region and your Identity Domains. These definitions are replicated automatically to all the other regions (which you subscribed to) or have their own automatic disaster recovery procedures.

Object Storage Buckets are region dependent which means that each data region can have its own set of buckets.

For your system to continue to work properly once it is switched to your System Disaster Recovery Region (for functions that require access to object storage), your object storage bucket structure should exist in your Object Storage Disaster Recovery Region.

Therefore, we recommend that you synchronize your bucket structure periodically between your Object Storage Home Region and Object Storage Disaster Recovery Region. This means, at a minimum, that buckets created in your Object Storage Home Region should be also added to your Object Storage Disaster Recovery Region.

4.5.2.2 Copying Your Object Storage Data

You may also choose to periodically copy the objects inside your buckets from your Object Storage Home Region to your Object Storage Disaster Recovery region.

Please note that copying data from one region to another will result in the use of additional object storage space, which in turn can lead to additional cost per billing period. See Using Replication in the **Object Storage** section of the *Oracle Cloud Infrastructure Documentation* for more information about configuring data replication policies to copy data between buckets in different regions.

If you can re-create lost data when a disaster occurs, then you might not need to copy your data across regions in advance, for example:

- Most files generated by your system via batch jobs can be regenerated if necessary
- 3rd party applications that load files into object storage may also be able to reproduce these files upon request

4.5.3 Recovering from a Disaster

A disaster is defined as an event that will cause your System Home Region to become unavailable. When a disaster occurs, your system will automatically be switched to your System Disaster Recovery Region, based on your service level agreements. When that happens you are responsible to tell the system what object storage region to connect to instead of the current one that is was linked to when the disaster happened (if that region has also became unavailable).

This section covers what you should do during a disaster and after it is resolved.

4.5.3.1 Switching to Your Disaster Recovery Region

Once your system has been switched to its System Disaster Recovery region, you will need to point it to a different data region for object storage access:

1. Log into each of the system environments.
2. In each environment look at all your current File Storage Configurations.
3. Edit each File Storage Configuration and change the region field to your Object Storage Disaster Recovery Region.
4. Save your changes.

4.5.3.2 Switching Back to Your Home Region

When your home region has been recovered and data was restored, the system will be switched back to your System Home Region. At this point you will need to point it back to your Object Storage Home Region for object storage access:

1. Log into each of the system environments.
2. In each environment look at all your current File Storage Configurations.
3. Edit each File Storage Configuration and change the region field to your Object Storage Home Region.
4. Save your changes.

4.5.3.3 Copying Back Your Object Storage Data

When you are switched back to your Object Storage Home Region, you may need to copy back some of the data that was created in your Object Storage Disaster Recovery Region. This may also include changes in bucket structure that you may have done while working in your disaster recovery regions.

- Changes in object storage bucket structure can be repeated in your home region manually after that region has been recovered.
- If you need to copy data back to your home region, see Using Replication in the **Object Storage** section of the *Oracle Cloud Infrastructure Documentation* for guidance.

5. Cloud Monitoring

This section describes how to use Cloud Monitoring with Oracle Revenue Management and Billing Cloud Services. It contains the following topic:

5.1 Status Page

The Status Page shows the current operational status of the environments in your tenancy and informs you of any unplanned and planned maintenance events. An environment's operational status is based on the health checks most recently run on that environment. Health checks are run every few minutes to provide near-real time status updates. The Status Page is unique per tenancy and is only accessible with your Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) credentials. No specific role is required to access the Status Page.

5.2 Accessing the Status Page

Contact your Customer Success Manager to gain access to the Status Page for your tenancy. You will receive an email containing the Status Page's URL once the Status Page for your tenancy has been set up.

5.3 Subscribing to Status Page Updates

You can subscribe to receive email updates by completing these steps:

1. Select **Subscribe to updates** from Status Page.
2. On the **Subscribe** page, enter your email address, and select **Subscribe to updates**. You will receive an email containing a link that enables you to confirm your subscription.
3. On the **Status Page Notifications** page, select the environments in the Tenancy to which you will subscribe.

You can select **Manage Your Subscription** from an email alert in the Status Page to cancel or manage your subscriptions.

5.4 Events

The Status Page provides information about planned maintenance events. A maintenance event's status is commonly *Scheduled* on a specific date and time, which informs customers of an outage or performance impact ahead of time.

The Status Page also provides information about unplanned outage events. Unplanned outage events inform you of the following:

- **Major Outage** - Main services are down such as Oracle Revenue Management and Billing Cloud Service.

- **Partial Outage** - Supporting services are down such as Customer Cloud Oracle REST Data Services (ORDS).

An unplanned outage event typically transitions through the following statuses:

- **Investigating:** Oracle teams are actively investigating but the reason for the outage is still undetermined.
- **Identified:** Oracle teams have determined the cause of the outage and the resolution.
- **Maintenance**: Oracle teams are performing scheduled maintenance.
- **Monitoring:** Oracle teams applied the resolution and are monitoring the system's operation.
- **Resolved:** The service is back online and operating normally. Oracle teams continue to investigate the cause of the outage, assign corrective actions, and make efforts to prevent the cause of the outage from occurring in the future.

