Oracle Utilities Cloud Services

End User Provisioning Guide

Release 19A

F14069-03

February 2019
(Revised April 2019)

ORACLE

Oracle Utilities Cloud Services Release 19A End User Provisioning Guide

Contents

Chapter 1

Overview 1-1

About This Book 1-2

Identity Cloud Service Tenancy 1-3

Chapter 2

Quick Start Guide 2-1

Activate Security Administrator Account 2-2

Evaluate Federated Single Sign-On Requirements 2-2

Modify Oracle Identity Cloud Service Settings 2-2

Prepare User Community 2-2

Setup Process Summary 2-3

Chapter 3

Security Administrator Account 3-1

Setting Up the Security Administrator Account 3-2

Navigating to the Identity Cloud Service Admin Console 3-3

Accessing via Cloud Account Portal 3-3

Accessing Identity Cloud Services Admin Console Directly 3-3

Verifying Security Administrator Identity Cloud Service Access 3-4

Verifying Subscription Contents 3-5

Exploring the Applications 3-5

Verifying Access to Object Storage 3-6

Verifying Security Administrator Access to Service 3-6

Chapter 4

User Management Procedures 4-1

User Onboarding - My Services Portal 4-2

Setting Up a New User 4-2

Setting Up a New Security Administrator 4-3

Updating or Removing a User 4-4

Defining User Group Membership 4-4

Managing Groups 4-4

Advanced User and Access Management - Identity Cloud Service Admin Console 4-5

Managing Users 4-5

Managing Groups 4-6

Managing Applications 4-6

Bulk Upload and Download 4-7

Updating Settings 4-8

Updating Security Privileges 4-8

Sign-On Policies for Online Access 4-8

Available Reports 4-11

Chapter 5

User Provisioning for Oracle Utilities Customer Cloud Service 5-1

Overview 5-2
Pre-Defined Application Roles 5-3
Configuring Just in Time Provisioning 5-3
Setting Up Groups for Provisioning - Identity Cloud Service 5-4
Configuring User Provisioning Rules - OUAF 5-4
Creating and Provisioning Users 5-5
Setting Up an OUAF Security and Access Administrator 5-5
Setting Up an Online Application User 5-5
Setting Up an Integration User for REST/SOAP Web Services 5-5
Setting Up a User with Access to BI Publisher 5-6
Setting Up the Cloud Service Foundation User 5-6

Chapter 6

User Provisioning for Oracle Utilities Analytic Insights 6-1
Overview 6-2
Pre-Defined Application Roles 6-2
Setting Up Application Users 6-2

Chapter 7

User Management for Oracle Utilities Analytic Insights 7-1
Locating Provisioned Users in Oracle Utility Analytics Insights 7-2
Assigning Groups and Roles in Oracle Utility Analytic Insights 7-2
Assigning and Removing User Group Permissions 7-3
Assigning User Group Permissions 7-3
Removing User Group Permissions 7-3
Assigning User Role Permissions 7-3
Removing User Role Permissions 7-4

Chapter 8

Using Federated Single Sign-On 8-1
Overview 8-2
Setup External Identity Provider 8-3
Service Access for Federated Users 8-4
Just In Time Provisioning for Federated Users 8-4

Chapter 1

Overview

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

This guide provides instructions for Security Administrators to set up user accounts for Oracle Utilities 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 guide also provides an introduction to working with Oracle Identity Cloud Service (). Identity Cloud Service is provisioned to customers with subscriptions to Oracle Utilities 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** on page 1-3 for more information).

This chapter includes the following:

- About This Book
- Identity Cloud Service Tenancy

About This Book

This guide contains the following:

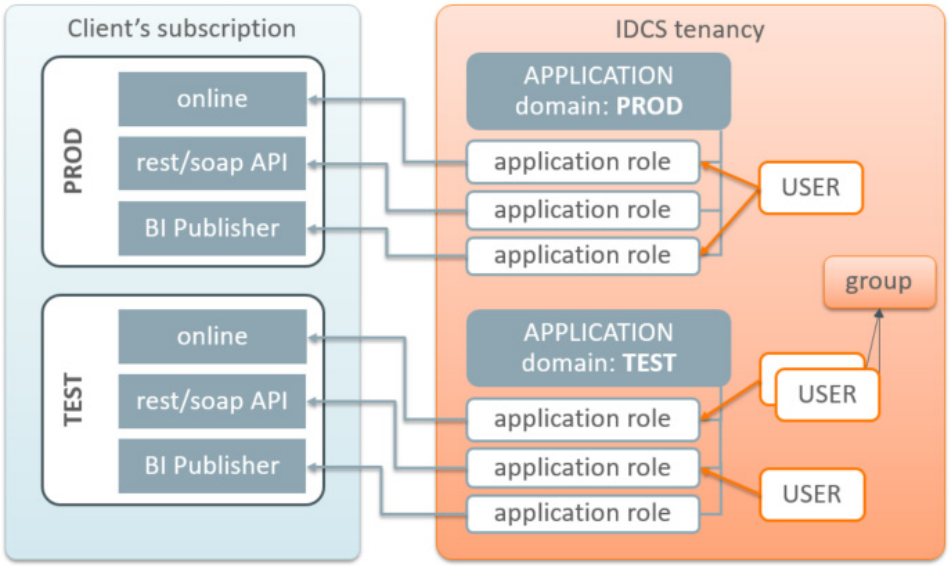
- Chapter 1: Overview (this chapter)
- Chapter 2: Quick Start Guide provides an overview of the end user provisioning process, with references to additional information in the following chapters.
- Chapter 3: Security Administrator Account describes how to set up a security administrator account for user provisioning.
- Chapter 4: User Management Procedures describes general procedures related to managing users and groups.
- Chapter 5: User Provisioning for Oracle Utilities Customer Cloud Service describes specific tasks related to user provisioning for Oracle Utilities Customer Cloud Service.
- Chapter 6: User Provisioning for Oracle Utilities Analytic Insights describes specific tasks related to user provisioning for Oracle Utilities Analytic Insights.
- Chapter 7: User Management for Oracle Utilities Analytic Insights describes specific tasks related to user management for Oracle Utilities Analytic Insights.
- Chapter 8: Using Federated Single Sign-On describes tasks required when using an external identity management system to provide authentication for the application instances within your cloud subscription.

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 Utilities cloud services the application represents a single environment, Production or non-Production. Applications are created by the subscription provisioning process.
- **Application Role**: In Oracle Utilities 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.



Chapter 2

Quick Start Guide

This chapter provides an overview of the initial set up of your cloud server user community including:

- Activate Security Administrator Account
- Evaluate Federated Single Sign-On Requirements
- Modify Oracle Identity Cloud Service Settings
- Prepare User Community
- Setup Process Summary

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 Chapter 3: Security Administrator Account.

Evaluate Federated Single Sign-On Requirements

If you are using IDCS as your only identity management system, proceed with adjusting the IDCS cloud settings followed by the user community setup. Otherwise if the user identities are managed by an existing enterprise identify management system then evaluate any Federated Single Sign On (SSO) requirements. If federation is required for all user accounts (including implementation team and the actual production users) proceed with the federated SSO setup as described in Chapter 8: Using Federated Single Sign-On.

Modify Oracle Identity Cloud Service Settings

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

- Define your user naming conventions: decide whether the email address will be used as user name. If not, you may want to include user name in the communication emails. Update notification(s) accordingly (see **Notification Update Example: Welcome Email** on page 4-8 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).

See **Updating Settings** on page 4-8 for more information about updating settings.

Prepare User Community

- 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** on page 5-4 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** on page 4-7 for more information about uploading and downloading template files.

Setup Process Summary

Note: 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** on page 4-8).
- Access the environment and configure Just-In-Time provisioning according to the product's specifications (see **Configuring User Provisioning Rules - OUAF** on page 5-4).
  - For example setup the IDCS Integration Master Configuration for CCS. Make sure the IDCS Groups are the same Groups that were used for the User/Group import files.
- Create Cloud Service Foundation accounts per environment (applicable for CCS)
- Perform import of Users, Groups and Application Roles using the import files prepared above (see **Bulk Upload and Download** on page 4-7).
- Setup at least one integration (non-human) user per environment of CCS and communicate the credentials to the implementation team (see **Setting Up an Integration User for REST/SOAP Web Services** on page 5-5)
- Setup access to production environment for those users who are responsible for legacy data migration

Chapter 3

Security Administrator Account

This chapter how to set up a security administrator account for user provisioning, including:

- Setting Up the Security Administrator Account
- Navigating to the Identity Cloud Service Admin Console
- Verifying Security Administrator Identity Cloud Service Access
- Verifying Subscription Contents
- Exploring the Applications
- Verifying Access to Object Storage
- Verifying Security Administrator Access to Service

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.

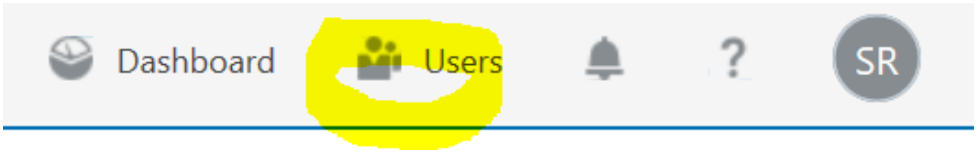
   Finally, you will be redirected to the **Oracle Cloud Account Portal** dashboard.

Navigating to the Identity Cloud Service Admin Console

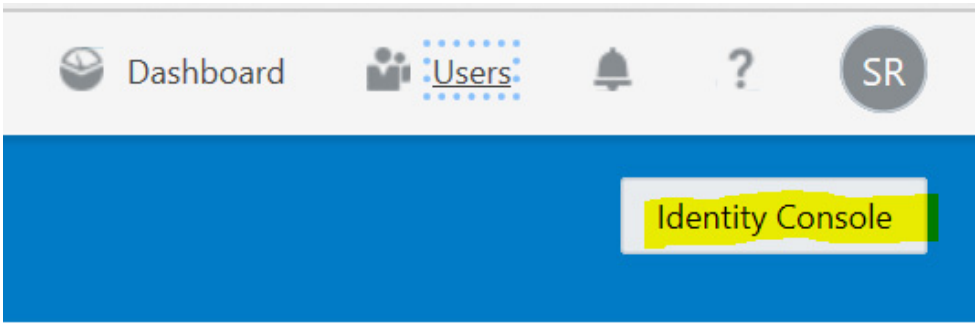
The Identity Cloud Service Admin Console can be accessed either directly or via Cloud Account Portal.

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.



Press the menu icon at the left top corner to expand the left-side navigation pane

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:

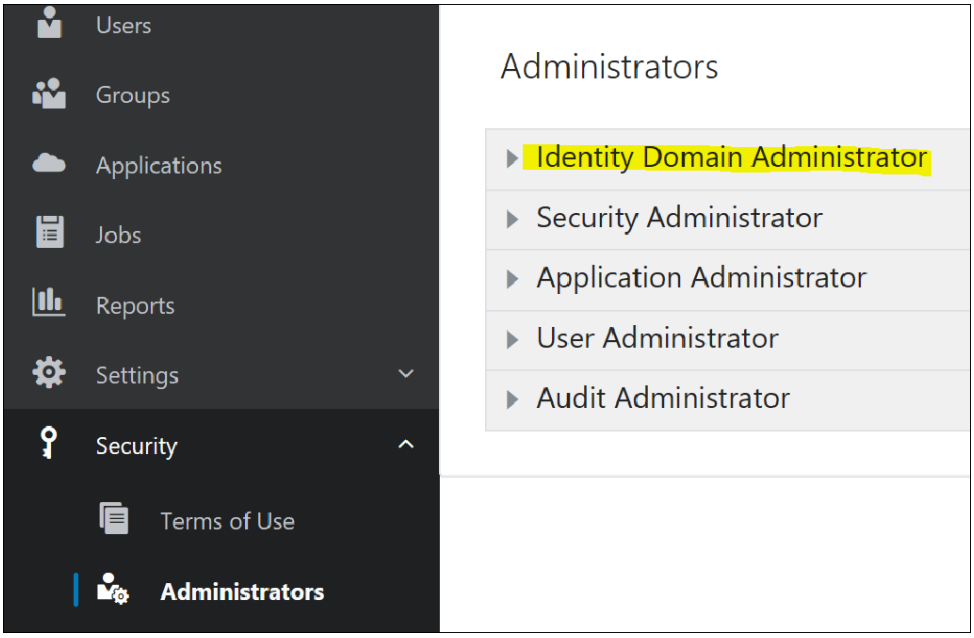
```
https://< tenancy>/ui/v1/adminconsole
```

where < tenancy> represents the instance of the 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.

Verifying Security Administrator Identity Cloud Service Access

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



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

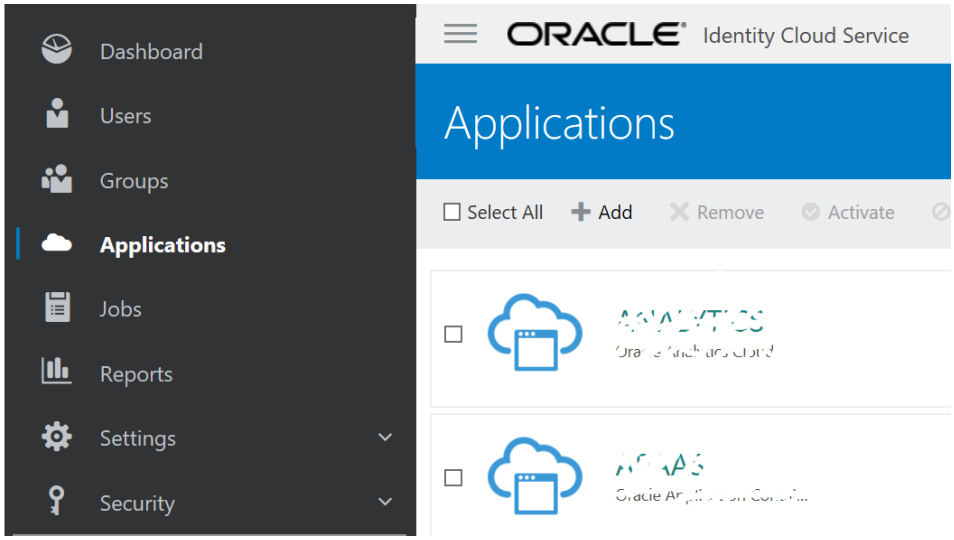
Verifying Subscription Contents

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

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

Typical Oracle Utilities Cloud Service subscription contains at least one production and one or more non-production environments.

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



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 can be assigned to Application Roles within the application.

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. In order to authorize user's access to a certain component the user has to be assigned to a corresponding Application Role. Separate Application Roles include:

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

Application Roles also used to support coarse-grained authorization in the target component, for example the Online Application Administrator versus an ordinary Online Application User

> **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

Verifying Access to Object Storage

Refer to the *Oracle Utilities Cloud Services Object Storage Setup Guide* in your service's documentation library for more information about object storage.

Verifying Security Administrator Access to Service

As part of the service activation notifications, the security administrator is provided with URL-s 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 URL-s for the online applications

See Oracle Utilities Integration documentation for more details on how to verify API access.

Chapter 4

User Management Procedures

This chapter general procedures related to managing users and groups, including:

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

User Onboarding - My Services Portal

The major 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.

Setting Up a New User

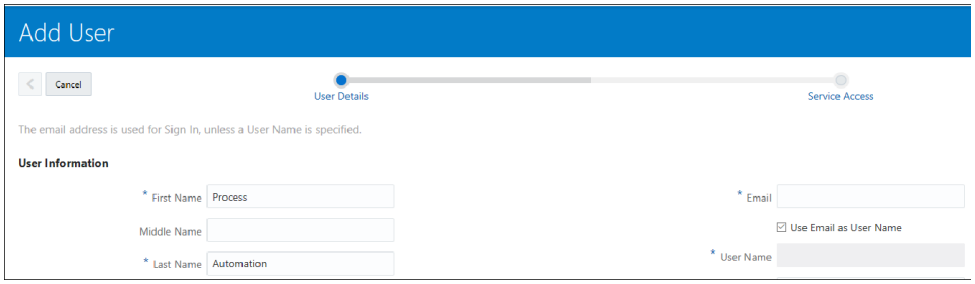
Click **Add** on the **Users** tab of the **User Management** portal to set up a new user.

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



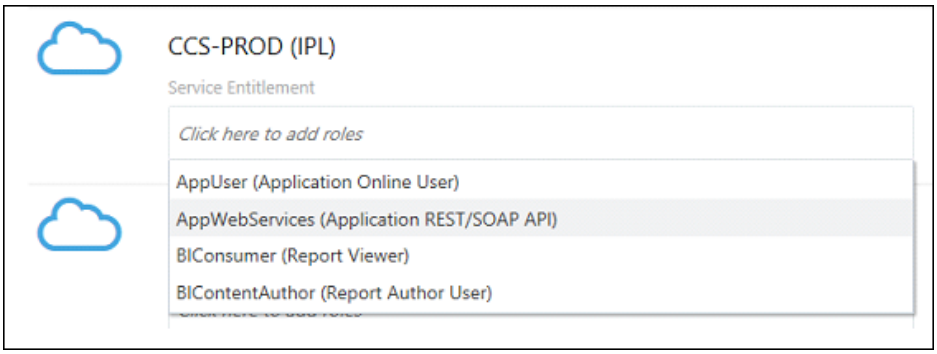
Click **Next** to set up the user's Service Access

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.



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. See Chapter 5: User Provisioning for Oracle Utilities Customer Cloud Service and Chapter 6: User Provisioning for Oracle Utilities Analytic Insights for more information.

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.

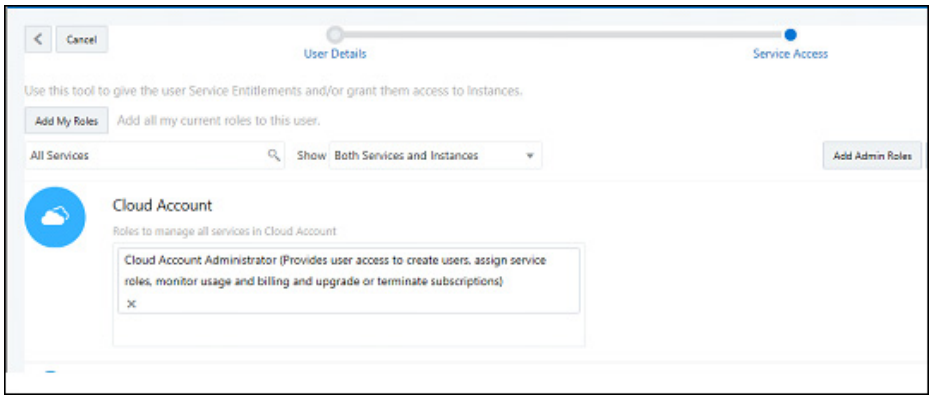
Cloud Account Administrator

The Cloud Account administrator's is able to 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.



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 of the above.

In order 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.

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

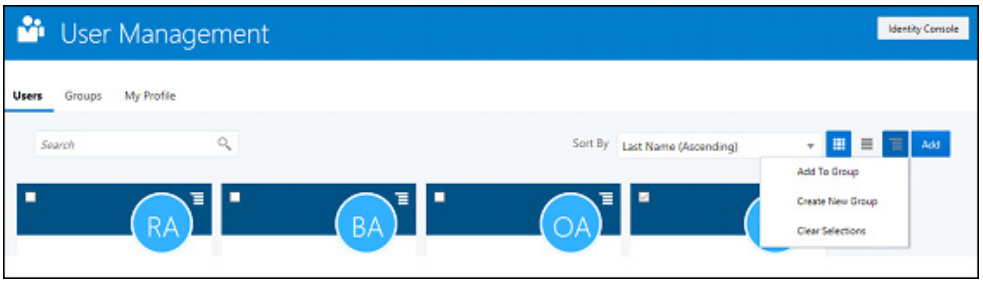
To remove a user, click **Remove** from the menu.

> **Note**: Removing a user is irreversible.

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



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 similar to 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.

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

Advanced User and Access Management - Identity Cloud Service Admin Console

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

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.

Select one or more users from the list, and select the appropriate action.

In addition to add and remove, the following actions are available:

- 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 of time.

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 wil 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.

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

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 also perform import and export of application role's members.

Bulk Upload and Download

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 competed and the file is available for the download.

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.

Updating Security Privileges

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

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 "blacklisting" and "whitelisting" approaches are supported.

- The blacklist defines a set of IP addresses that are blocked from the access. This approach should be used when the "bad" IP-s are well-known and permanent and the list is not expected to change very often.

- The whitelist 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 whitelisted or blacklisted:

- 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 refer to 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 "blacklisted" and/or "whitelisted" 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 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 has to 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 the 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 satisfies 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.

Refer to IDCS documentation for the detailed instructions regarding Sign-On Policy and Network Perimeter setup.

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

Chapter 5

User Provisioning for Oracle Utilities Customer Cloud Service

This chapter describes user provisioning for Oracle Utilities Customer Cloud Service, and includes the following:

- Overview
- Pre-Defined Application Roles
- Configuring Just in Time Provisioning
- Creating and Provisioning Users
- Setting Up the Cloud Service Foundation User

Overview

Each Oracle Utilities Customer Cloud Service environment included in the subscription contains multiple components:

- Business Applications that run on the Oracle Utilities Application Framework, (OUAF)

  Oracle Utilities Application Framework 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.

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

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

Pre-Defined Application Roles

The following roles are pre-defined in the Applications that represent Oracle Utilities service environments. Each role represents an entitlement within the environment and grants user an access to a certain component (OUAF-based products):

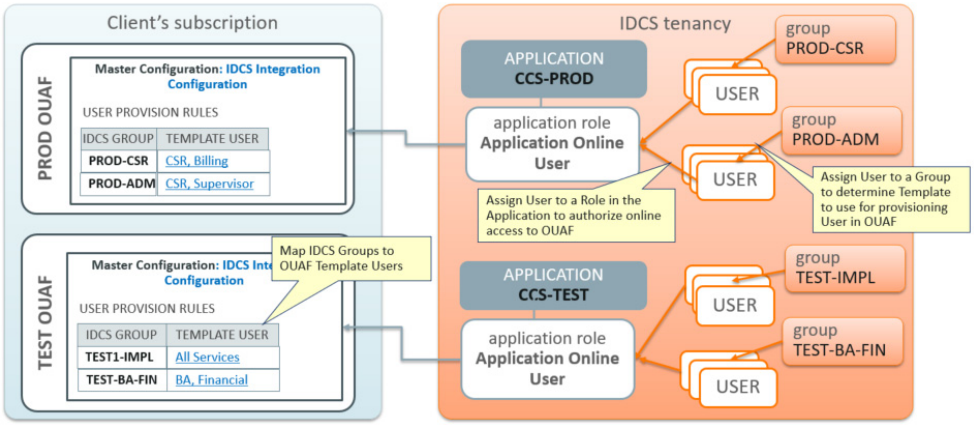
Application Role	Authorized Access
Online Application User	The user assigned to this role may access online application
Web Services Access	The user assigned to this role is authorized to access the REST/SOAP API-s
BI Consumer	The user assigned to this role may access the BI Publisher within the environment and view and execute pre-defined reports
BI Content Author	The user assigned to this role may access the BI Publisher within the environment and author new and view/execute existing reports

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**.



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

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

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.
- On the Integration Master Configuration. map Groups created above to the Template Users in OUAF
- If Integration Master Configuration is not configured at the time the user record is created in , the user will be provisioned with K1MINACS (default minimal access)

Creating and Provisioning Users

This section describes steps involved in creating and provisioning users.

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** on page 4-3 for more details.
3. After first login to OUAF this user will be provisioned with Template User K1SCRADM (security administrator)

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. Assign the User to the Online Application User role in the environment.

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 an 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 new User with Login ID = User Name in . Assign the user to user groups that provide access to all or selected application services, according to the business requirements.

Setting Up a User with Access to BI Publisher

Perform the following steps:

1. Create a new user or search for and select an existing User in .
2. Locate the application that is corresponding to the environment. Assign the User to one of the BI Publisher Application Roles available in the environment:
   - BI Consumer
   - BI Content Author

Setting Up the Cloud Service Foundation User

Your Oracle Utilities cloud services include a set of implementation tools. In order to enable these tools you need to create at least one Cloud Service Foundation Integration Account (non-human).

The credentials of this account are used by the outbound messages sent by the instances of the target application.

Perform the following steps:

1. Create a new user or search for and select an existing User.
   - Specify the email address allocated for the integration/non-human users. Authorized security administrators must be provided with access to this email account.
   - When the activation email is received and reset the user's password.
2. Assign the User to the REST/SOAP Web Services role in the Application that represents the environment.
3. Login to OUAF and retrieve User K1PAUSER. Duplicate this user; specify User's user name as a Login ID.

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

Chapter 6

User Provisioning for Oracle Utilities Analytic Insights

This chapter describes user provisioning for Oracle Utilities Analytic Insights, and includes the following:

- Overview
- Pre-Defined Application Roles
- Setting Up Application Users

Overview

Oracle Utilities Analytic Insights features internal user access management that grants users the access to various features within the application. It stores and maintains users.

For each user that authorized to access Oracle Utilities Analytic Insights the corresponding application user is created in OUAI.

The Oracle Utilities Analytic Insights user is created thru Just in Time Provisioning flow.

Pre-Defined Application Roles

The following roles are pre-defined in the Applications that represent Oracle Utilities Analytic Insights environments:

Application Role	Authorized Access
Online Application User	The user assigned to this role may access online application
Online Application Admin	The user assigned to this role may access the online application and also perform the administrative tasks in Oracle Utility Analytic Insights.
BI User	The user assigned to this role may access the Oracle Business Intelligence Enterprise Edition (OBIEE) component within the environment

Setting Up Application Users

Perform the following steps to provision new user:

1. Create a new user or search for and select an existing User in .
2. Locate the application that is corresponding to the Oracle Utilities Analytic Insights environment.
    1. Assign the user to one of the Online Application roles.
    2. Assign the user to the BI User role

Chapter 7

User Management for Oracle Utilities Analytic Insights

This chapter

Once an Identity Cloud Service user has been created and assigned to the application role(s), the user may access Oracle Utilities Analytic Insights online.

Upon first successful login, the user record is created in the Oracle Utilities Analytic Insights user list, and is ready to be configured and assigned to Oracle Utilities Analytic Insights groups and roles. Groups and roles determine the user features and functionality available to each user.

This chapter outlines specific steps that need to be performed to configured users in Oracle Utility Analytic Insights including:

- Locating Provisioned Users in Oracle Utility Analytics Insights
- Assigning Groups and Roles in Oracle Utility Analytic Insights
- Assigning and Removing User Group Permissions

Locating Provisioned Users in Oracle Utility Analytics Insights

Once a user has been created in Identity Cloud Service and logged into the application for the first time, it will appear in the Oracle Utility Analytic Insights user list. See Chapter 6: User Provisioning for Oracle Utilities Analytic Insights.

> **Note**: You need to have customer administration rights to complete this task. Verify that your user has been assigned to the Application Admin role in the application that is corresponding to the environment in Identity Cloud Service.

Use the following procedure to locate a user.

1. Log in to Oracle Utility Analytic Insights.
2. Select **Administer**, then **Security**, then **Users** to navigate to the **Administer Users** page.
3. Search for the user you created in Identity Cloud Service by completing one of the user information fields and then clicking **Get Users**.

   You may search for a user by any data entered when creating the user.

   The data table will return with the user information and links that allow you to assign their user environment. See the *Oracle Utilities Analytic Insights User Guide* (https:// docs.oracle.com/ cd/E72219_01/documentation.html) for additional information about the **Administer User** page.
4. Click **Edit** in the user row to open the **Manage Users** dialog box. The **Manage Users** dialog box allows you to modify group and role permissions.

Assigning Groups and Roles in Oracle Utility Analytic Insights

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

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

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

Module	Role
Meter to Bill	AMI Deployment Billing Meter Operations Safety

Revenue Protection	Revenue Protection
Distribution Planning and Operations	Distribution Planning
Demand Response and Energy Efficiency	Demand Response and Energy Efficiency

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

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

Assigning and Removing User Group Permissions

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

Assigning User Group Permissions

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

1. Locate the user in Oracle Utility Analytic Insight sand open the dialog box for the user. See **Locating Provisioned Users in Oracle Utility Analytics Insights** on page 7-2.
2. Click **Assign Additional Group**.
3. Select the appropriate group from the **Add Group** drop-down list, and click **Save**. The **Manage Users** dialog box will update the **Group** field with the assigned group.
4. If a user needs permissions for multiple groups, repeat the previous steps for each additional group.
5. Click **Cancel** or any area outside of the dialog box to close the dialog box.

Removing User Group Permissions

Use the following procedure to remove group assignments:

1. Open the **Manage User** dialog box for the user. See **Locating Provisioned Users in Oracle Utility Analytics Insights** on page 7-2.
2. Click **Remove** next to the group name you want to remove.

Assigning User Role Permissions

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

Use the following procedure to assign user role permissions:

1. Open the **Manage User** dialog box for the user. See **Locating Provisioned Users in Oracle Utility Analytics Insights** on page 7-2.
2. Click **Assign Additional Role**. The dialog will update with a drop-down list of the available roles based on the modules licensed to the customer.
3. Select the appropriate role from the list and click **Save**. The **Manage Users** dialog box will update the **Role** field with the newly assigned role.
4. If the user needs permissions for multiple roles, repeat the steps for each additional role.
5. Click **Cancel** or any area outside of the dialog box to close the dialog box.

Removing User Role Permissions

Use the following procedure to remove user role permissions:

1. Open the **Manage User** dialog box for the user. See **Locating Provisioned Users in Oracle Utility Analytics Insights** on page 7-2.
2. Click **Remove** next to the role.

Chapter 8

Using Federated Single Sign-On

This chapter describes tasks required when using an external identity management system to provide authentication for the application instances within your cloud subscription, including:

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

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 Utilities cloud services.

Setup External Identity Provider

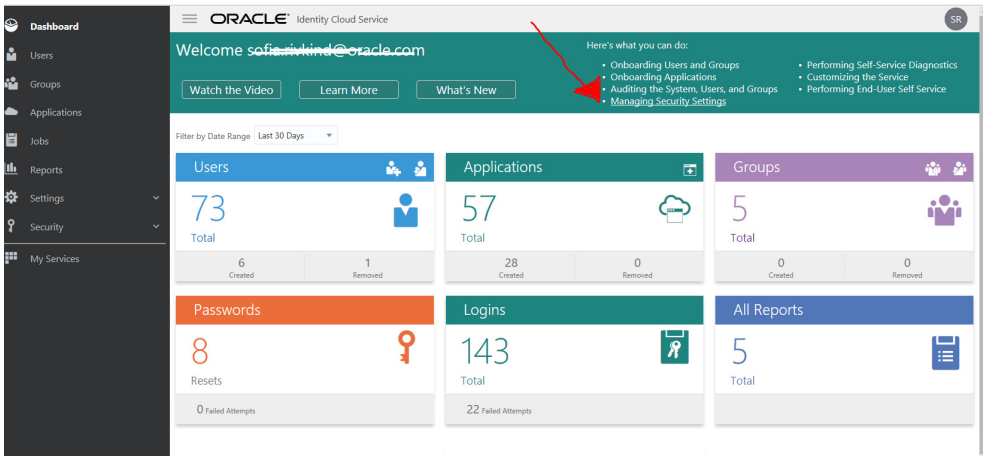
Configure a Security Assertion Markup Language (SAML) 2.0 external identity provider such as Active Directory Federation Services (AD FS) for federated SSO to Oracle Identity Cloud Service.

Configuration steps include:

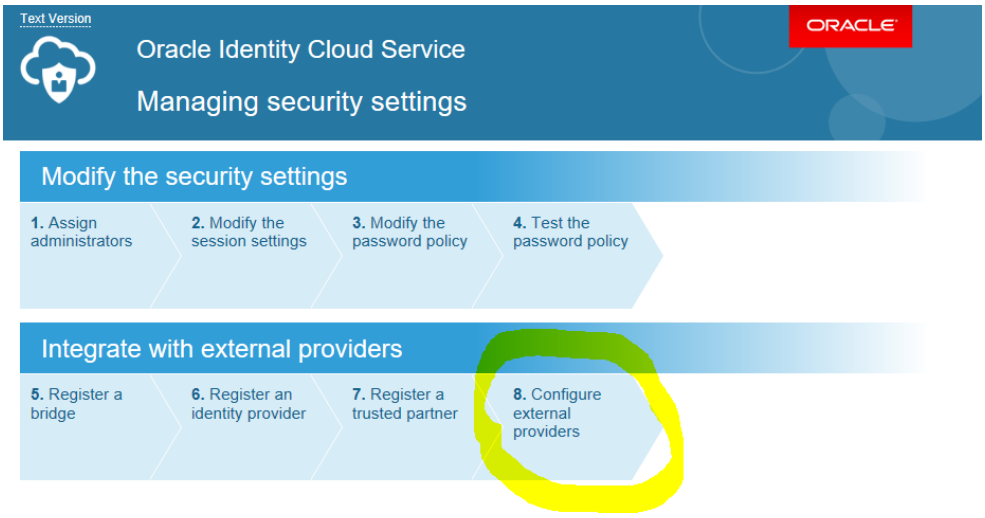
- Configure Microsoft Active Directory Bridge or implement user data synchronization via REST SCIM API or flat file import.
- Setup the Security Assertion Markup Language 2.0 Identity Provider.
- Verify Federated Single Sign-On.

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.



- Follow the instructions under **Configure External Provider**.



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).

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** on page 4-4, **Setting Up an Online Application User** on page 5-5, and **Setting Up Application Users** on page 6-2 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** on page 4-7 for more details).
  - Copy the information into Application Role import file and import users and/or groups to the Application Role (see **Importing** on page 4-7 for more details).

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** on page 5-3 for more detailed configuration instructions.