Oracle Utilities Cloud Services

Security Guide

For 23A Releases

F76046-01

April 2023

ORACLE

Oracle Utilities Cloud Services 23A Security Guide

Contents

Chapter 16

Chapter 17

Chapter 1

Cloud Services Security Guide

Welcome to Oracle Utilities Cloud Service Security Guide. This guide describes how you can configure security for the following Oracle Utilities Cloud Services:

- Oracle Utilities Billing Cloud Service
- Oracle Utilities Customer Care and Billing Cloud Service
- Oracle Utilities Customer Cloud Service
- Oracle Utilities Digital Asset Cloud Service
- Oracle Utilities Market Settlements Management Cloud Service
- Oracle Utilities Meter Solution Cloud Service
- Oracle Utilities Operational Device Cloud Service
- Oracle Utilities Rate Cloud Service
- Oracle Utilities Work and Asset Cloud Service

This chapter includes the following:

Audience

Oracle Utilities Cloud Service *Security Guide* is intended for Oracle Utilities Cloud Service administrators, security administrators, application developers, and others tasked with performing the following operations securely and efficiently for the cloud service:

- Designing and implementing security policies to protect the data of an organization, users, and applications from accidental, inappropriate, or unauthorized actions
- Creating and enforcing policies and practices of auditing and accountability for inappropriate or unauthorized actions

- Developing interfaces that provide desired services securely in a variety of computational models, leveraging Oracle Utilities Cloud Service and directory services to maximize both efficiency and ease of use

To use this document, you need to a basic understanding of how the Oracle Utilities Cloud Service works, and basic familiarity with the security aspects of the Oracle Cloud Infrastructure.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit Oracle's Accessibility Program website.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit My Oracle Support or Oracle Accessibility Learning and Support if you are hearing impaired.

Related Documents

For more security-related information, see these Oracle resources:

- Oracle Cloud Services Agreement
- Cloud Services Agreement Policies
- Data Processing Agreement
- Oracle Cloud Hosting and Delivery Policies
- SaaS Cloud Services Pillar Document
- Oracle Corporate Security Practices
- Technical Best Practices for Oracle Utilities Application Framework-based Products (Doc Id: 560367.1)
- Oracle Utilities Application Framework - Batch Best Practices (Doc Id: 836362.1)
- Web Services Best Practices for Oracle Utilities Application Framework (Doc Id: 2214375.1)
- Oracle Utilities SaaS Cloud Security (Doc Id: 2595978.1)
- Oracle Cloud Infrastructure Identity and Access Management
- Oracle Utilities Cloud Service Administration Guide - Identity and Access Management
- Oracle Utilities Cloud Service Implementation Guide

These documents are available from My Oracle Support and Oracle Documentation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Notes:

- Screen images in this document are for illustrative purposes only.
- Menu options in this document assume the use of Alphabetic sorting. If alternatives are used, then adjust the advice accordingly.

Critical Patches

As part of the service, all security patches identified by Oracle will be automatically applied to your Oracle Utilities Cloud Service.

Chapter 2

What's New In Security

The security features and enhancements described in this section comprise the overall effort to provide superior access control, privacy, and accountability with this release of Oracle Utilities Cloud Service.

With each release of the product new and improved security features are made available since the last release. This section outlines the significant changes since the last release. Refer to the release notes provided for additional advice.

The following sections describe new security features of Oracle Utilities Cloud Service (Release 23A) and provide pointers to additional information:

- Application Security Query Portal
- Improved User Group Portal
- OAuth Token Request in Payload
- Encrypted Files and Digital Signature Support
- Removal of SDK Files

Application Security Query Portal

This release includes a new portal to enables security administrators the ability to identify and manage application service security using broader objects, such as menus, dashboard zones, batch processes and more, as a reference point to reduce security maintenance costs.

Improved User Group Portal

This release includes an enhanced user group portal to enable security administrators the ability to manage user group definitions using mass actions to reduce security maintenance costs. The enhanced portal includes user group membership and related object maintenance from a single portal including improved permission expiry identification.

OAuth Token Request in Payload

This release enables implementations to specify the OAuth token exist in the payload as well as the header for external third-party interfaces that require the token in the payload. The Message Sender has been extended to enable the presence of the token in the payload using an appropriate context setting on the definition.

Encrypted Files and Digital Signature Support

This release enables implementations to digitally sign and/or encrypt export files via an enhancement to the plug-in export batch template. The RSA digital signature and/or PGP based encryption can be managed via a configurable key ring to handle a wide variety of settings and standards as well as support key rotation as necessary.

Removal of SDK Files

This release removes some server-based Oracle Utilities Software Development Kit helper files used for legacy screen development. These are only used for older versions of the product and have limited use outside development. The following files have been removed:

- optionalJSPInclude.jsp
- optionalCMJSPInclude.jsp
- availableUserExits.jsp
- checkXalan.JSP
- imageTest.jsp
- exitReference.jsp
- generateMDXMLs.jsp
- jvmInfo.jsp
- showOracleAuditUser.jsp

Chapter 3

Introducing Security

One of the key aspects of the Oracle Utilities Cloud Services is security, which not only confirms the identity of an individual user but determines the data and functions, once identity is confirmed, that user has access to within the Oracle Utilities Cloud Services.

This chapter includes the following:

Security Features

Security is one of the key features of the Oracle Utilities Cloud Services architecture protecting access to the Oracle Utilities Cloud Services, its functionality and the underlying data stored and managed via the Oracle Utilities Cloud Services.

- **Integration Cloud Service:** The Oracle Utilities Cloud Services has been integrated with Oracle Cloud Infrastructure Identity and Access Management (IAM) embedded in your service, standalone or in federated mode. This integration manages user presence and user authentication services for your service.
- **Firewall and IP Management:** Access to your Oracle Utilities Cloud Services is controlled via a firewall and IP address management.
- **Secure Transport Support:** Transmission of data across the network utilizes the secure encryption methods supported by the Oracle Cloud Infrastructure.
- **Inbuilt Authorization Model:** Once a user is authenticated then the internal authorization model is used to determine the functions and data the user has access within Oracle Utilities Cloud Services.

Chapter 4

Authentication

From a security point of view, authentication is all about identification of the user. It is the first line of defense in any security solution. In simple terms, it can be as simple as the *challenge-response* mechanism we know as userid and password.

The authentication aspect of security for the Oracle Utilities Cloud Services is delegated to Oracle Cloud Infrastructure Identity and Access Management (IAM).

This chapter includes the following:

Online Authentication

The Oracle Utilities Cloud Services delegates the responsibility of authentication of the online users to Oracle Cloud Infrastructure Identity and Access Management (IAM). This allows security administrators to centrally manage cloud users centrally.

The Oracle Utilities Cloud Services uses Security Assertion Markup Language (SAML), OAuth2, and other protocols to integrate to Oracle Cloud Infrastructure Identity and Access Management (IAM). This integration is automatically deployed when the Oracle Utilities Cloud Services is deployed. Synchronization between the Oracle Cloud Infrastructure Identity and Access Management (IAM) and the Oracle Utilities Cloud Services uses the Identity Cloud Adapter.

For more information, refer to the Oracle Cloud Infrastructure Identity and Access Management documentation.

Batch Authentication

The Batch component of the architecture uses Oracle Cloud Infrastructure Identity and Access Management (IAM) and cloud security to authenticate users to execute batch processes. From an authentication point of view, the deployment of the Oracle Utilities Cloud Services automatically configured authentication for the batch processes.

Web Service Authentication

The Web Service component of the Oracle Utilities Cloud Services is housed in the Oracle Utilities Cloud Services infrastructure and utilizes Oracle Cloud Infrastructure Identity and Access Management (IAM) and Inbound Web Services security configuration to authenticate users using the relevant configured WS-Policy.

From an authentication point of view, the deployment of the Oracle Utilities Cloud Services automatically configured authentication for web services.

Chapter 5

Authorization

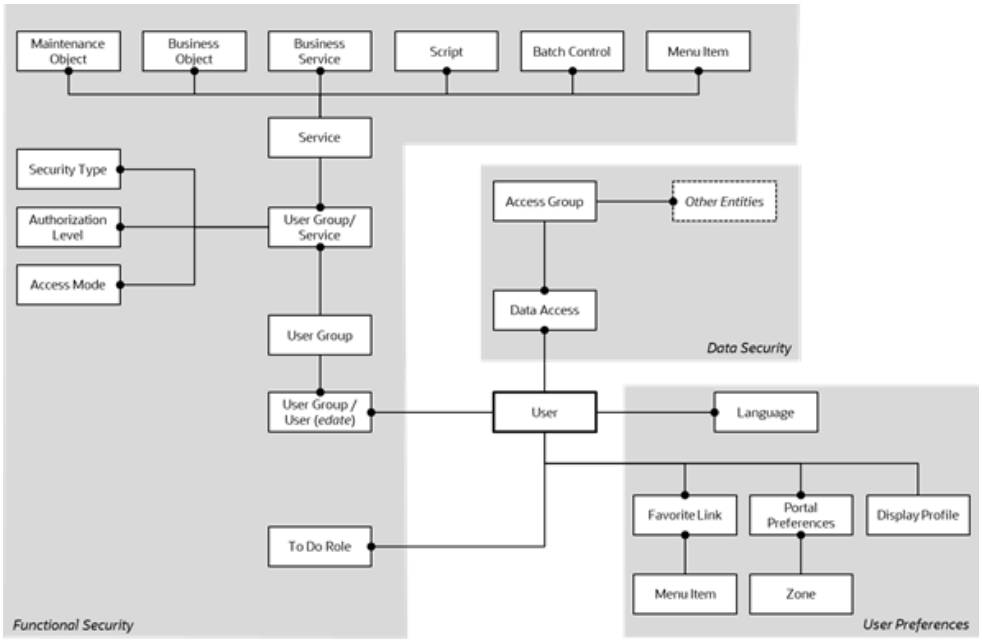
Once a user is identified, they must be authorized to specific functions and data within the Oracle Utilities Cloud Service. The Oracle Utilities Cloud Service uses an inbuilt security model for authorization. This model contains all the data necessary for the definition of authorizations to function and data. Information in the security model can be manually entered using online transactions and can be imported and synchronized from Oracle Cloud Infrastructure Identity and Access Management (IAM). The latter is typically used with customers with many online users to manage.

> **Note:** Customers utilizing the Cloud Accelerator will preload a security configuration that may be altered to suit individual needs.

This chapter includes the following:

Authorization Model

The following data model describes the security authorization model of Oracle Utilities Cloud Service.



Users

A record of each user is stored in the User entity, which defines the attributes of the user including identifier, name, Portal preferences, Favorites, Display Profile (such as format of dates and so on), and Language used for screens and messages, and other attributes. Users are attached to To Do Roles that allow the user to process any error records for background processes. For example, if a particular background process produces an error, it is possible to define the users that will process and address the error.

> **Note:** To maintain consistency, it is recommended to maintain user records in Oracle Cloud Infrastructure Identity and Access Management (IAM) and perform a synchronization from that service rather than altering users in the User entity.

User Groups

Users are also attached to User Groups. This relationship is effective dated, which means that the date period it is active across is also defined. This can be useful for temporary employees such as contractors or for people who change roles regularly.

User Groups are mechanisms for grouping users, usually around job roles. Each user group is then attached to the Application Services that the group is authorized to access. The Application Services are the functions within Oracle Utilities Cloud Service. Loosely, these correspond to each of the screens accessible in Oracle Utilities Cloud Service. In this attachment, the Access Mode is also defined with standards being Add, Modify, Read, and Delete. With this combination, it is possible to define what functions and what access can those functions for user groups (and hence users).

Additionally, it is possible to define the authorization level of the User Group to that function. For example, you may find that a certain group of users can only approve payments of a certain level unless authorization is obtained. The Authorization Level is associated with a Security Type that defines the rules for the Application Service.

> **Note:** To use security types, the implementation must develop server side or client-side user exits to implement code necessary to implement the security level.

Services can be attached to individual menus, batch controls, maintenance objects, business objects, business services, and scripts to denote the service to be used to link user groups to access these objects. In this case, business object security overrides and maintenance object security. The same applies to business services security overriding that Application Service it is based on.

The Oracle Utilities Cloud Service allows you to limit user access to specific data entities to prevent users without the appropriate rights from accessing specific data. By granting a user access rights to an account, you are granting the user access rights to the account's bills, payments, adjustments, orders, and so on.

Access Groups

Access Groups define a group of accounts that have the same type of security restrictions. Data Access Roles define a group of users that have the same access rights (in relation to access to entities that include access roles). When you grant a data access role with rights to an access group, you are giving all users in the data access role rights to all entities in the access group.

The following summarizes the data relationships involved with data security:

- Entities reference a single access group. An access group may be linked to an unlimited number of relevant entities.
- A data access role has one or more users associated with it. A user may belong to many data access roles.
- A data access role may be linked to one or more access groups. An access group may be linked to one or more data access roles.

Chapter 6

Managing Security

Once the security definitions are established, these must be managed from the Oracle Utilities Cloud Service, security infrastructure and security repositories are used.

This chapter includes the following:

- Online User Management
- Managing Batch Users
- Managing Web Services Users
- User Authentication
- Deploy Users from Oracle Cloud Infrastructure Identity and Access Management

Online User Management

To manage online users, several facilities must be configured:

- Maintain users within the Oracle Cloud Infrastructure Identity and Access Management (IAM) as per the Create User Accounts instructions.
- Activate the users within IAM to enable their access. Conversely, deactivating users within IAM disables access to the service.
- Map IAM groups to product template users as outlined in **User Provisioning for Oracle Utilities Cloud Services** of the *Cloud Service Administration Guide*.
- Attach user groups to Application Services to define the subset of service and actions valid for that group of users. Refer to Define User Groups to Application Services for more details of this process.
- Attach data access groups to the users to define the subset of data that the user has access. Refer to Define Users to Data Access Groups for more details of this process.
- Attach users to the appropriate user groups to define the subset services and valid actions the users can perform within the Oracle Utilities Cloud Service. Refer to Define Users to User Groups for more details of this process.

User Management

This section describes the User object from the Oracle Utilities Cloud Service. All information is inherited from the User definition in Oracle Cloud Infrastructure Identity and Access Management (IAM). The User object records the security information used for identification of the users and their permissions. Oracle Utilities Cloud Service also provides a function to maintain the following security information for the user:

Field	Description
Userid	This is the unique user identifier used within the Oracle Utilities Cloud Service for authorization activities. Limited to eight characters.
Login Id	This is the unique user identifier used within the Oracle Utilities Cloud Service for authentication purposes. This must match the value used in the security repository to successfully use the Oracle Utilities Cloud Service. Limited to 256 characters, which can be similar or different from Userid.
Last Name	Last name of the user. Limited to 50 characters.
First Name	First name of the user. Limited to 50 characters.
User Enable	Indicates whether the user is active or inactive in the security system. Valid values are *Yes* (default) and *No*. Yes indicates the user is active and can use the system while No indicates the user is inactive and cannot use the system. Refer to User Enable and Disable for more information.
User Type	Describes the type of user. Valid values are *Blank* and *Template*. Blank refers to normal users. Refer to Template Users for more information about the Template user type.
Language	Default language used by user. For non-English languages, the Language pack must be installed.
Display Profile Id	The display profile associated with the user that controls the displayed currency, dates, and so on.
Time Zone	Time zone assigned to the user account. This is only applicable to specific services. Refer to Oracle Utilities Cloud Service online documentation for more information about its applicability.
Email Address	Optional email address associated with the user that can be used for interfaces requiring email addresses.
Dashboard Width	Describes the default width of the **Dashboard** portal. Setting the value to "0" disables the dashboard.
Dashboard Location	Indicates the preferred location of the **Dashboard** portal. This is only enabled for use with the Screen Layout Profile user experience.
Dashboard State	Indicates the preferred initial state of the **Dashboard** portal. This is only enabled for use with the Screen Layout Profile user experience.
Home Page	The default home page associated with the user.
Portals Profile User Id	The user identifier from which to inherit portal definitions. For more information, refer to Template Users.
Favorites Profile User Id	The user identifier from which to inherit favorite definitions. For more information, refer to Template Users.

Field	Description
To Do Summary Age Bar	The color schemes for the **To Do Summary** portal in the Dashboard. This can be used to indicate relative age of To Do entries.
User Groups	This is a list of user groups and their associated expiry dates. Refer to Define Users to User Groups for more information.

Template Users

By default, portal preferences and favorites are set at an individual user level. It is possible to inherit the portal and favorites from other users to reduce the maintenance effort for security information. Changes to the profile user are automatically inherited to any users where the profile user is attached.

To use this functionality, you must perform the following:

- Set up each user to be used as a template and set the **User Type** to *Template*.
- For any user that will inherit the portal preferences and favorites, specify the appropriate template user in the following fields:
  - **Portal Preferences:** Use the Portals Profile User Id to specify the Template User to be used to inherit the portal preferences.
  - **Favorites:** Use the Favorites Profile User Id to specify the Template User to be used to inherit the favorites preferences.
- Once changes are made to the Template Users' portal preferences and favorites, the changes automatically apply to any attached users.

Assign To Do Types

The Oracle Utilities Cloud Service generates To Do records for any function or error condition that requires human intervention. The To Do record contains a type and role to be used assist in assigning the appropriate resources to work on the condition indicated by the To Do.

> **Note:** You can explicitly assign To Do records to users or user groups. This section covers the latter condition. To Do Roles must be set up prior to using this function. Refer to the online Administration Help for a discussion about the To Do function.

For security purposes, users need to be attached to the relevant roles for the To Do facility to limit which To Do Types an individual user can work upon. To manage the To Do Roles to be assigned to users, navigate to the **To Do Roles** tab of the User Maintenance function and select the **Add** or **Delete** icon. You can use the **Search** icon to find existing To Do Roles. Once users have been attached to the To Do Roles, they can access the associated To Do Types assigned to the role or any To Do directly assigned to them.

Assign User Portal Preferences

The Oracle Utilities Cloud Service user interface is made up of portals containing individual zones. Each portal and zone can be associated with an Application Service for security purposes. Users attached to the User Groups and Application Services can view and use the portals and zones.

> **Note:** Portal preferences can be inherited from other users if Template Users are used.

The order of display and other factors are defined at an individual user basis. To define the portal preferences for a user, navigate to the **Portal Preferences** tab of the User Maintenance function, select a portal, and set your zone preferences:

Field	Description
Display	Indicates whether to include the zone or exclude it from the portal. Refer to Zone Visibility of the online Administration Guide for more information.
Initially Collapsed	Indicates whether to display the zone in collapse or expand mode during the initial load. Zones are collapsed only when expanded Marking zones as "initially collapsed" speeds up the portal loading time.
Sequence	Defines the relative order of the zones within the portal. A value of zero takes the default sequence from the portal definition.
Refresh Seconds	Defines the zone automatic refresh rate but is only applicable to a subset of zone types. A value of zero disables auto-refresh.
Security Access	Indicates whether the zone is accessible or not to the user. It is possible to for a zone to have zones that are not accessible to an individual user.

Assign Bookmarks

You can attach bookmarks to your user profile to access pages including the context of the pages. You can use the **Bookmark** button to define bookmarks that attach the page and context to the user profile.

> **Note:** Bookmarks are added at runtime by end users using the **Bookmark** button. This function only displays or deletes the bookmarks assigned by the user.

It is possible to view and remove bookmarks on the use profile by navigating to the **Bookmarks** tab of the User Maintenance function. You can set your bookmark preferences through the following fields:

Field	Description
Sequence	Internal sequence used for sorting.
Name	The name of the bookmark. The URL for the bookmark is hidden and is not editable.

You can use the **Delete** icon to remove existing bookmarks from your list.

Assign Favorite Links

Users can set several favorite functions or menu items that they can access using keyboard shortcuts or via the **Favorites** zone on the Dashboard.

> **Note:** Favorites can be inherited from other users if Template Users are used.

Configuration of favorite functions or menu items is through the **Favorite Links** tab of the User Maintenance function. Users can set favorite link preferences through the following fields:

Field	Description
Sequence	The relative sequence number of the favorite link used for sorting purposes.
Navigation Option	The navigation option to display the favorite links. This can reference the zone or maintenance function to display after selecting the favorite link.
Security Access	Indicates whether the Navigation Option is accessible or not to the user.

To manage the Favorites to be assigned to users, select the **Add** icon to assign the favorite link with the appropriate Navigation Option and Sequence or select the **Delete** icon to remove an existing Navigation Option from the list. You can use the **Search** icon to find existing Navigation Options.

Assign Favorite Scripts

Users can set several Favorite BPA Scripts that they can access using the **Favorite Scripts** zone of the Dashboard.

> **Note:** Favorites can be inherited from other users if Template Users are used.

Configuration of favorite scripts is through the **Favorite Scripts** tab of the User Maintenance function. Users can set favorite script preferences through the following fields:

Field	Description
Sequence	The relative sequence number of the favorite used for sorting purposes.
Script	The BPA script to use to display the favorite function or menu items.
Security Access	Indicates whether the BPA script is accessible or not to the user.

To manage the Favorites to be assigned to users, select the **Add** icon to assign the favorite link with the appropriate Script and Sequence or select the **Delete** icon to remove an existing Script from the list. You can use the **Search** icon to find existing BPA scripts.

Assign User Characteristics

Oracle Utilities Cloud Service can extend objects within Oracle Utilities Cloud Service with Characteristics, which act as additional data attributes for providing more information or custom algorithms for processing.

Note: Oracle Utilities Cloud Service ships with a predefined set of Characteristic Types. To use User Characteristics, the appropriate characteristic types must be created and attached to the user object. Refer to the online Administration documentation for more information.

The User object in Oracle Utilities Cloud Service can also be customized using characteristics by navigating to the **Characteristics** tab of the User Maintenance function. The following fields can be set for the favorites:

Field	Description
Characteristic Type	The characteristic type associated with the User object.
Sequence	The relative sequence number of the characteristic used for processing purposes.
Characteristic Value	Depending on the configuration of the characteristic type, the characteristic value may be free-formatted, an attachment, in a specific format, or a specific set of values.

To manage the Characteristics to be assigned to users, select the **Add** icon to assign the characteristic (indicating the characteristic type) with the appropriate Sequence or select the **Delete** icon to remove an existing characteristic from the list.

Define Users to User Groups

Access to Oracle Utilities Cloud Service services requires User Group connections that are connected to Application Services. The connections define the linkage for functions that are accessible to users.

The attributes of the user-user group links are as follows:

- The link is subject to an expiry date to allow representation of transient security configurations.
- Each link is owned and subject to Data Ownership Rules. By default, all site-created links are owned as Customer Modifications.
- User groups are set up according to site preferences. These can be job related, organization level-related, or a combination of factors.
- A user must be a member of user group to access the system. A user can be a member of multiple user groups.
- Users can be members of user groups with overlapping permissions to Application Services. In cases of overlapping permissions, the highest valid permission is used.

You can manage the user and user group link by navigating to the **Main** tab of the User Maintenance function. You can use the **Add** icon to insert a user group with the appropriate expiry date or use the **Delete** icon to remove existing user groups from the list. Use the **Calendar** icon to select the expiry date and set the link's effective date. Use the **Context Menu** icon to navigate to the user group details to review more information. The user's security is referenced for menu and function access regardless of the access channel (online, web service, or batch) used.

Define User Groups to Application Services

One of the fundamental Oracle Utilities Cloud Service security configuration is to define user groups to Application Services. The Application Service can represent an Oracle Utilities Cloud Service service, a menu, or an object. Linking a user group to a service allows Access Mode configuration, which defines the valid actions that the user group can perform against the service.

> **Note:** Oracle Utilities Cloud Service ships will all the Application Services predefined for base functions. These can be used or replaced with custom definitions. A starter set of User Groups is loaded with Oracle Utilities Cloud Service that can be used as basis for further security user groups.

Additionally, each service can specify Security Types that allow for custom security rules to be applied at runtime. Refer to Security Types for more information.

The methods used to maintain the links between user groups and Application Services are the Application Service Portal and User Group Maintenance. These methods are valid for most sites and can be used to manage the same information from different prospective.

Application Service Portal

The Application Service portal enables you to define an application service, set the access modes for the Application Service, and specify the user groups to which to connect the Application Service.

You can configure the following **Main** tab settings by navigating to **Administration** then **Application Services**:

Field	Description
Application Service	The unique identifier of the Application Service used in configuration of security on objects, menus, services, and so on. For custom definitions, Oracle recommends adding a "CM" prefix to distinguish these from Application Services provided by OUCS.
Description	A brief description for documentation purposes that appears on security screens when the Application Service is specified.
Access Modes	Lists the valid access modes for the Application Service. The modes must match the internal actions supported by the objects used by the Application Service. Use the **Add** icon to insert an access mode. Note that an access mode can only be defined once on an Application Service. Use the **Delete** icon to remove an existing access mode from the list. The Access Mode link to the Application Service is ownership-controlled and by default, all created links are owned as Customer Modifications. Refer to Data Ownership Rules for more information.

You can also configure the following zones in the **Application Security** tab to display user group memberships and manage relationships:

Field	Description
Application Service Details	Summarizes the access modes and security types of the Application Service.

Field	Description
User Groups With Access	Lists the user groups with access to the Application Service, along with the associated expiry dates, access modes, security types, and associated authorization levels. Use the Deny Access function to limit the access of user groups to the Application Service.
User Groups Without Access	Lists the user groups without access to the Application Service. Use the Grant Access function to allow user groups to access the Application Service.

After granting access to user groups, you can set the access mode and security group specifications for the user group:

Field	Description
Expiry Date	Specifies the date when access to the user group expires.
Access Mode	Shows the access mode defined on the Application Service definition. Use the **Add** icon to insert an access mode or use the **Delete** icon to remove an existing access mode from the list.
Owner	Ownership of the link. Refer to Data Ownership Rules for more information.
Security Type	The security type code associated with the Application Service. Use the **Add** icon to insert a security type or use the **Delete** icon to remove an existing security type from the list.
Authorization Level	The authorization level assigned to the user group when running the Application Service for the security type.

User Group Maintenance

The User Group Maintenance allows you to define the Application Services that user groups can access and to connect users to user groups. You can manage the user groups by navigating to **Administration**, selecting the **User Group** menu item, and perform the following actions:

- Use the **Context Menu** icon to edit existing permissions.
- Use the **Delete** icon to remove the association between the user group and Application Service.
- Use the **Add** icon to associate a user group with an Application Service.

Adding or editing associations automatically displays the **Application Services** tab, which enables you to maintain the access modes and security types for the association through the following fields:

Field	Description
Expiry Date	Specifies the date when access to the user group expires.
Access Mode	Shows the access mode defined on the Application Service definition. Use the **Add** icon to insert an access mode or use the **Delete** icon to remove an existing access mode from the list.

Field	Description
Owner	Ownership of the link. Refer to Data Ownership Rules for more information.
Security Type	The security type code associated with the Application Service. Use the **Add** icon to insert a security type or use the **Delete** icon to remove an existing security type from the list.
Authorization Level	The authorization level assigned to the user group when running the Application Service for the security type.

You can manage the users associated with the user groups through the **Users** tab fields:

Field	Description
User	The authorization user identifier to associate with the user group.
Expiration Date	Indicates the date when the association between the user and user group expires.
Owner	Ownership of the link. Refer to Data Ownership Rules for more information.

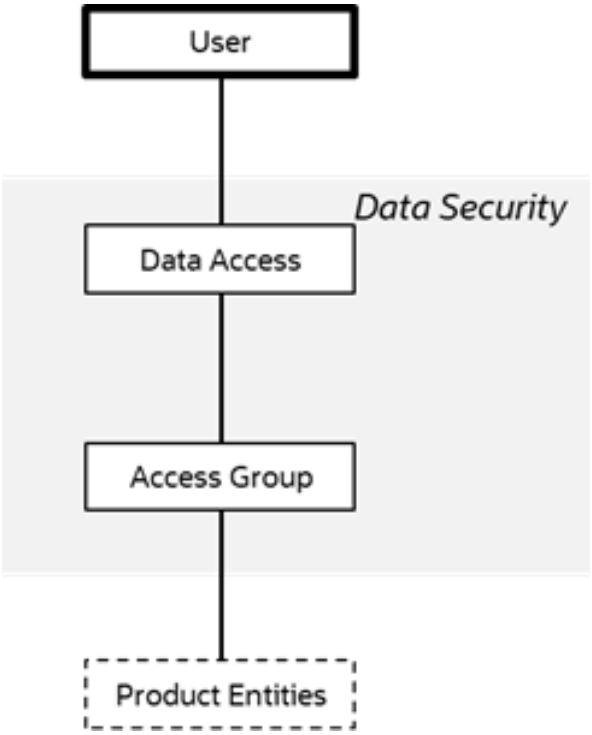
Define Users to Data Access Groups

Data Access Groups define the subset of data objects that are accessible to the users. The levels of data access definition are as follows:

- **Data Access Roles:** These define the groups of data permissions that are accessible to users. Users are connected to Data Access Roles and Data Access Roles are connected to Data Access Groups.
- **Data Access Groups:** These are tags attached to Oracle Utilities Cloud Service entities that implement data security. Note that attaching a Data Access Group to an Oracle Utilities Cloud Service entity does not automatically implement data security. Queries for the object must be altered to be consider the Data Access Group. Refer to the online Administration Guide for more information.

  Note: Only some services support Data Access Roles and Data Access Groups. Refer to the online Administration Guide for more information.

This image illustrates the relationship between Data Access Roles and Data Access Groups:



You can maintain Data Access Roles and Data Access Groups in the **Access Security** tab of the User Maintenance function. You can use the **Add** icon to insert a data access role and these fields to configure the settings or use the **Delete** icon to remove an existing data access role from the list.

Field	Description
Default Access Group	The default access group for a new user-created object that is subject to Access Security. This can be overridden by logic within the object if necessary.
Data Access Role	Lists of data access roles to which the user is attached.
Expiration Date	The date when the association between the user and data access role will expire.

User Enable and Disable

One feature of security is to attach user records to some objects (automatic or configurable) for audit purposes. You cannot delete a user record if the user performs any work in Oracle Utilities Cloud Service and is attached to some audit objects across Oracle Utilities Cloud Service.

> **Note:** Activating or deactivating users within Oracle Cloud Infrastructure Identity and Access Management (IAM) enables or disables users from using Oracle Utilities Cloud Service.

The User Enable function on the User object allows you to activate or deactivate a user by setting the appropriate value for **User Enable**. The implications of the User Enable value are as follows:

Value	Implications
Enable	• The user can access the system. • The user can process records according to the authorization model. • The user must be active in the Security Repository to fully access Oracle Utilities Cloud Service.
Disable	• The user cannot access the system regardless of the security setup. • The user record is retained for audit purposes only. • The user does not have to exist in the Security Repository. The key use cases for this option are as follows: • **Support for personnel (permanent or temporary) leaving:** Manually deactivate users once they leave the organization and keep their information for auditing purposes. • **Logical deletion:** If the user record needs to be deleted for any reason, selecting this option logically removes the user record, preventing access to the system. • **Temporary disablement:** If business rules need to isolate the user record, selecting this option for the appropriate users can effectively deactivate their access to Oracle Utilities Cloud Service. **Note:** Deactivation of the user record will take effect when the user logs in to the system or after the security cache refreshes.

Advanced User Management

The **User Group Portal** supports multiple actions including:

- Setting an expiration date across multiple user group access modes for multiple application services.
- Removing multiple access modes for multiple application services from user groups.
- Adding multiple permissions from multiple application services.
- Maintaining multiple security types across multiple application services

Managing Batch Users

Oracle Utilities Cloud Service provisions users of batch processes as users via Oracle Cloud Infrastructure Identity and Access Management (IAM). The user being used as a job processing parameter on any method must be a valid provisioned user with appropriate access to required services.

Managing Web Services Users

Oracle Utilities Cloud Service provisions users of web services as users via Oracle Cloud Infrastructure Identity and Access Management (IAM). The user being used within the relevant WS-Policy format must be a valid provisioned user with appropriate access to required services.

User Authentication

The User object includes the Userid and Login Id identifiers whose roles are as follows:

- The Userid is used internally for authorization and passed to the database connection as CLIENT_IDENTIFIER. This user cannot be changed after the user has created any records in the system as it is used for record ownership in some objects and in auditing. The maximum length of Userid is eight characters.
- The Login Id is used for authentication to the security repository configured for Oracle Utilities Cloud Service. The Login Id can match the Userid but can differ to reflect site standards. Unlike the Userid, the Login Id can be changed at any time to reflect changes in the organization such as name changes or acquisition. The maximum length of Login Id is 256 characters.

  Note: The Login Id must match, in the same case, as the entry in IAM.

When maintaining a user, Oracle recommends all changes be performed in IAM to preserve consistency.

Oracle Utilities Cloud Service maintains a Security Hash, which is part of the User object, that it checks during login. At application login time and if the security hash does not match the user, the user is not authorized to access Oracle Utilities Cloud Service. Oracle Utilities Cloud Service automatically performs maintenance of security hash values.

> **Note:** Direct manipulation of the User object may result to invalidation of the security hash, which leads to login issues. All user changes must be performed via IAM or directly using Oracle Utilities Cloud Service (for federated implementations).

Deploy Users from Oracle Cloud Infrastructure Identity and Access Management

Refer to **User Provisioning for Oracle Utilities Cloud Services** of the *Cloud Services Administration Guide* for more information on the provisioning process.

Chapter 7

Advanced Security

While the default Security settings are adequate for most sites, there are several additional Advanced Settings that can be configured to support a wider range of security requirements. This section outlines the various security settings available and the configurations supported.

This chapter includes the following:

Menu Security Guidelines

By default, a menu option is displayed whenever a user has access to the underlying Application Service definition attached to objects that are indirectly linked to a menu entry. While this behavior is enough for most needs, it is possible to place an override on an individual menu item to override the lower level security levels. This is particularly useful where implementations intend to replace base-supplied menu items with custom menu items.

By linking a menu item to a new service that can reference the underlying objects and specifying an Application Service (optionally also including an Access Mode) would override the permissions on the underlying objects.

It is possible to specify the Application Service on a menu item by using the **Menu Items** tab of the **Menu** option on the **Administration** menu.

Security Types

By default, users have full access to the objects via the access methods specified in their user groups. If the implementation plans to implement additional levels or rules, then the Application Service must use Service Types. The Service Type definition allows additional tags to be attached to service definitions and then code written to detect and take advantage of the presence of the tag to limit security access to specific object data. For example, whether data is masked or not or some limit is placed on values of data.

To define security types, use the **Security Types** menu option on the **Administration** menu:

Field	Description
Security Type	The identifier for the security code.
Description	A brief description of the security code's purpose.
Authorization Levels	Lists the authorization level codes and associated descriptions. The codes are free-formatted but should be representative of the desired function. Use the **Add** icon to insert a security code or use the **Delete** icon to remove an existing code.
Application Service Id	Lists Application Services associated with the security code. Use the **Add** icon to insert a security code or use the **Delete** icon to remove an existing code.

Note: Include security codes in objects to fully implement the rules associated with the security types.

Default Generic Application Services

By default, all sets of Application Services are defined against base functions. In line with Data Ownership Rules, some of these records can be altered and new functions added. A set of generic Application Services are also shipped with Oracle Utilities Cloud Service to provide a mechanism for defining new zones, new objects, or new menu items for rapid deployment.

The following generic Application Services (optional use) secure objects, zones, and menu items:

- F1-DFLTAPS - This secures zones and menu options but only supports the Execute access method.
- F1-DFLTS - This secures business objects and supports the Add, Modify, Delete, and Inquire access methods.

Data Masking Support

Oracle Utilities Cloud Service can mask data within objects in an appropriate fashion. Oracle Utilities Cloud Service does not store the data in masked fashion, it is configured to be displayed in a masked format for users using Security Types.

Oracle Utilities Cloud Service supplies the F1-MASK internal algorithm type, which performs basic data masking. The parameters available in this algorithm type are as follows:

- **Masking Character** - The character to be used as a mask. The default character is an asterisk (*).
- **Number of Unmasked Characters** - The number of suffix characters to unmask. Commonly, the last *x* characters are displayed unmasked to allow some identification. A value of zero masks all characters.
- **Unmasked Characters** - List of characters without spaces to leave unmasked. This is commonly used to denote delimiter characters to enhance recognition.
- **Application Service** - Used for security authorization checking. The Application Service allows global or local services to be configured to indicate security access to data masks.
- **Security Type** - The security type that flags the users that will view the data in masked or unmasked format. User groups need to be connected to the Application Service and security type, and given the Authorization Level to determine the level of data masking.
- **Authorization Level** - The authorization level that determines if the user can access the unmasked data. All other authorization levels in the security type will indicate masked data.

To mask data, perform the following:

- Configure an algorithm entry using the F1-MASK algorithm type for the desired configuration. Algorithm entries can be shared across fields to be masked using the **Algorithm** menu option of the **Administration** menu.
- Attach user groups to the Application Service with the appropriate Authorization Level for the Security Type.
- Create or update a feature configuration with a Data Masking feature type by using the **Feature Configuration** menu option of the **Administration** menu.
- For each field to mask, add an entry to the **Options** section of Feature Configuration and configure the following settings:
  - **Option Type:** *Field Masking*
  - **Sequence:** A numeric value for sorting purposes
  - **Value:** A tag string delimited by a comma to indicate the data masking definition.
    - The supplied algorithm only supports fields defined as strings.
    - Enter `alg="algorithm name"` to reference the masking algorithm. The corresponding Algorithm Type must reference the Data Masking algorithm entity.
    - For data accessed via a scheme-based object call, reference a metadata field name from its schema definition. For example, to mask a credit card number with a schema of `<creditCard mdField="CCNBR" mapField="EXT_ACCT_ID"/>`, set the option value `field="CCNBR", alg="algorithm name"`.

- For data accessed by a page maintenance service call, indicate the table name and field name where the data resides. For example, `table="table_name"`, `field="fld_name"`, and `alg="algorithm name"`.
- A WHERE clause can be specified, which is useful for data that resides in a child table where only of a certain type needs to be masked. For example, `table="CI_PER_ID"`, `field="PER_ID_NBR"`, `alg="algorithm_name"`, `where="ID_TYPE_CD='SSN'"`.
- For data stored as a characteristic, indicate the characteristic type as `CHAR_TYPE_CD='char type'`, `alg="algorithm name"`. This needs to be defined only once regardless of which characteristic entity the Char Type may reside. Note that only ad-hoc characteristics are supported at the present time.
- For data displayed via a search service call, indicate the search name and the appropriate field to mask along with the masking algorithm. For example, `search="SearchServiceName"`, `field="PER_ID_NBR"`, `where="D_TYPE_CD='SSN'"`, `alg="algorithm name"`. To find the search service name, launch the search in question then right-click the filter area, select **View Source**, and search ServiceName. To find the field name to mask, return to the search window and right-click the search area then select **View Source**. Look for the **Widget Info** section and find the field name in the search results but exclude the $. Note that the WHERE statement can only apply to fields that are also part of the search results.

Secure Online Debug Mode

Oracle Utilities Cloud Service's online debug mode provides the ability to diagnose issues, solve problems, and trace code. As an Oracle Utilities Cloud Service feature, this is security-controlled.

To use the function on any of the user groups, a user must include Inquire access to the F1DEBUG Application Service, which enables the debug facility from the URL.

Secure Online Cache Management

Oracle Utilities Cloud Service online cache management function resets the online cache to force new values to be loaded. As an Oracle Utilities Cloud Service feature, this is security-controlled.

To use the function on any of the user groups, a user must include Change access to the F1ADMIN Application Service, which enables the cache management facility from the URL.

Groovy Support

Oracle Utilities Cloud Service supports Groovy for extensions via the script engine, and augments the Java and Scripting support to provide alternatives. The implementation of Groovy has some limitations for security reasons:

- Groovy APIs with direct access to operating system functions have been block listed for security reasons and therefore cannot be used. Alternative functions are provided to provide safe access to selected operating system functions.
- Access to Groovy syntax is governed by an allowlist that defines the valid subset of Groovy classes available for the Oracle Utilities Cloud Service. Refer to the allowlist on the **Dashboard** zone of the Script maintenance function for more information about the supported classes.

Oracle Cloud Object Storage Support

By default, use of the FILE-BATCH variable was restricted to local mounted storage where it is possible to use network storage via mapped directories. It is now possible to use Oracle Cloud Object Storage Device as a source of import files or locations to write files.

To use this feature, Oracle recommends the following:

- Create or edit a lookup value for the F1-FileStorage extendable lookup for each cloud service used with the following Connection Details:

Connection Details	Notes
File Adapter	Use *Oracle Cloud Object Storage*
REST Endpoint URL	Cloud storage's endpoint URL. Exclude the Service Name or Container Name from the URL
User Name	The cloud username to use
Password	The corresponding password for the cloud username

- To use the definition, use the parameter in the FILE-PATH variable in the Batch Control definition or batch configuration file for relevant batch controls with the `file-storage://<ExtendableLookupValue>/<serviceName>` format, where `<ExtendableLookupValue>` is the name of the lookup value configured in F1-FileStorage and `<serviceName>` is the service name for the Oracle Cloud Object Storage service.

SYSUSER Account

By default, the Oracle Utilities Cloud Service installation supplies an initial SYSUSER account. This account is defined in the default security realm of the provided templates, provided as the initial User object in the authorization model, and used as default user in some transactions.

You cannot physically remove the SYSUSER account as this is used by the initial installation and owned by the Oracle Utilities Cloud Service. You can deactivate this account under the following conditions:

- Alternative identities have been configured for the authentication and authorization components of Oracle Utilities Cloud Service.
- Every facility in the implementation that uses the SYSUSER account as the default identity has been changed to an alternative to prevent misconfiguration of the facility.

  Note: Oracle recommends that you use the appropriate alternatives for transactions instead of the SYSUSER account.

The Batch Control facilities use the SYSUSER account as the default identity. Replace SYSUSER in batch control configuration files, batch edit configuration files, or Oracle Scheduler configuration when using the account for batch control submission.

You can deactivate the SYSUSER account by:

- Removing SYSUSER from configured security realms for authentication, preventing the user from authenticating.
- Setting the **User Enable** attribute (SYSUSER user object) to *Disable*, deactivating the account from any unauthorized activity in Oracle Utilities Cloud Service.

IP Allowlist

Inbound and outbound communications from the service can be controlled via IP Address Allow Listing. The security infrastructure assess inbound and outbound communications with the allowlist, and allows or prevents traffic.

Allowlists for inbound and outbound traffic is managed via Oracle Cloud Infrastructure Identity and Access Management (IAM) using network perimeters.

Chapter 8

Audit Facilities

Oracle Utilities Cloud Service inbuilt, configurable auditing facility provides the capability to register accesses to data from online and Web Services users. Auditing allows for the configurable tracking of changes to key data and allows authorized users to track changes on individual user. Use of this facility is optional and can be switched on or off at any time.

> **Note:** This facility does not audit batch processes for performance-related reasons.

This chapter includes the following:

Audit Configuration

Note: This section covers the **soft-table implementation** of auditing. There is a specialist Audit algorithm support on business and maintenance objects to add information to log entries attached to these objects. Flush the online data cache to enable auditing on Oracle Utilities Cloud Service.

Audit configuration for Oracle Utilities Cloud Service is performed at the table level. Enable auditing on each table by navigating to the **Administration** menu then the **Table** menu option, and configuring the following field settings:

- **Audit Table** - You need to configure a database table to store the audit information. By default, the CI_AUDIT table can be used to store audit information. When using a custom table, make sure that the structure of this table is similar to CI_AUDIT to ensure compatibility.
- **Audit Program** - You must configure a class or program that will record and process the audit information. By default, OUCS provides the following pre-built programs:
  - `com.splwg.base.domain.common.audit.DefaultTableAuditor` - The default Java-based class that audits changes on any fields configured to track auditing information.

    - `com.splwg.base.domain.common.audit.ModifiedTableAuditor` - An alternative to the DefaultTableAuditor class. However, this class does not audit inserts or deletions of empty string field data. For example, changes from null values to empty spaces or empty spaces to null values are not logged.
- **Audit Conditions** - Switches that indicate the conditions for auditing the field. Activate at least one of these switches for auditing:
    - **Audit Delete Switch** - Audits delete operations against the field.
    - **Audit Insert Switch** - Audits insert operations against the field.
    - **Audit Update Switch** - Audit update operations against the field.

Audit Query by Table, Field, and Key

Once auditing is activated, changes are logged in the configured audit table by the selected audit class or program, and you can query the audit information by using tables, fields, and keys as search filters.

To perform an audit query, navigate to the **Administration** menu, select the **Audit Query By Table/Field/Key** menu option, and specify your search filters:

- Audit Table Name - Select a table to list additional filters
- Audit Field Name
- Creation Start Date/Time and Creation End Date/Time - Date range comprising the dates and times when changes were made to the fields

The query results provides the following information:

- Create Date/Time
- User Name
- Primary Key
- Audited Field Name
- Audit Action (Insert, Update, or Delete)
- Value Before Audit
- Value After Audit

Audit Query by User

Once auditing is activated, changes are logged in the configured audit table by the selected audit class or program, and you can query the audit information by using users as search filters.

To perform an audit query, navigate to the **Administration menu**, select the Audit **Query By User** menu option, and specify your search filters:

- User ID
- Audit Table

- Creation Start Date/Time and Creation End Date/Time - Date range comprising the dates and times when changes were made to the fields

The query results provides the following information for the selected User ID:

- Row Creation Date/Time
- Audited Table Name
- Primary Key
- Audited Field Name
- Audit Action (Insert, Update, or Delete)
- Field Value Before Audit
- Field Value After Audit

Read Audit

Oracle Utilities Cloud Service's inbuilt, configurable auditing facility can also be used to register data when accessed for auditing purposes. Read Audit (or read auditing) is different from standard auditing as it focuses on zones and in the current release, read audit is only available for the following zone types:

- F1-DE
- F1-DE-QUERY
- F1-DE-SINGLE
- F1-MAPDERV
- F1-MAPEXPL

The zone configuration provides you with the ability to configure an Audit Service script that is called whenever the zone is displayed to determine the criteria and results to display.

The information audited can be determined by using programs and logged based on your requirements. Refer to the online help for descriptions and samples for Read Auditing configuration.

> **Note:** Services are shipped with sample generic Audit query codes that are specific to Oracle Utilities Cloud Service. You can reuse or alter these codes to fulfill your requirements. Refer to the Oracle Utilities Cloud Service online documentation for more information and samples.

Chapter 9

Database Security

The Oracle Database used in Oracle Utilities Cloud Service utilizes the security features of the Oracle Cloud Infrastructure platform and is optimized for use with the Oracle Utilities Cloud Service component.

This chapter includes the following:

Cloud Database Security Setup

Oracle Utilities Cloud Service includes a preconfigured database installation that does not require additional administration by users, and handles all the maintenance and management of the database. While user interaction is minimal, the following configurations are used for Oracle Utilities Cloud Service for security purposes:

- Automatic creation and maintenance of database users for administration, application, and reporting purposes. Automatic allocation of the database users to relevant Oracle Utilities Cloud Service components at service provisioning time.
- Inclusion of the Oracle SQL Developer for Web in Oracle Utilities Cloud Service and use of the identity provided by Oracle Cloud Infrastructure Identity and Access Management (IAM).
- Inclusion of the following functions in the database and preconfigured policies:
  - Partitioning
  - Advanced Compression
  - Hybrid Columnar Compression
  - Transparent Data Encryption
- Protection and management of encryption keys by the native key management features of the Oracle Cloud Infrastructure platform.
- Use of the Database Vault to control access by privileged accounts. All policies are preconfigured for Oracle Utilities Cloud Service.
- Use of Oracle Resource Management on all access modes. All policies are preconfigured for Oracle Utilities Cloud Service.

Chapter 10

Encryption Feature Type

Oracle Utilities Cloud Service provides the capability to mask and encrypt data for protecting sensitive information through the Encrypted Feature Type feature configuration.

Note that at least one Feature Configuration should exist for Encryption Feature Type with an option per field to encrypt. You can maintain encryption feature configurations by navigating to the **Administration** menu and selecting the **Feature Configuration** menu option.

This chapter includes the following:

Encrypted Fields Configuration

Note: You must run F1-ENCRS and/or F1-ENCRT after adding or updating encryption to reflect the changes.

To define a field to encrypt, add an option with the following attributes:

Attribute	Description
Option Type	Set to *Field Encryption*.
Sequence	Set to a number not in use. High sequence numbers override low sequences.

Attribute	Description
Value	Specify the encryption in the format of a command string. For example, `table="F1_ATTACHMENT",field="PK_VAL5",alias="ouaf.system",encryptedField="PK_VAL2",hashAlias='HmacSHA256-1024',hashField="PK_VAL3", where="PK_VAL1='Encrypted'"`. • table - A table name existing in the metadata. • field - An existing field in the metadata that will be encrypted. Must only be in a string format, other field formats are not supported. Using a higher level of encryption may increase the field's storage requirements. • alias - Keystore alias to encrypt the data. • where - Data filter, useful for child tables to determine specific values to encrypt. Do not use for adhoc characteristics • wrap - Specifies whether to wrap or not the value with the `ENC()` market. Valid values are `true` and `false`. Set to "false" unless your code includes additional processing that handles the special marker. OUCS fields should use `wrap=false`. • maskAlg - The algorithm to mask the data if the field will also be masked. For example, `maskAlg="CMCCR"` • maskField - The field to use as the mask if the field will also be masked. For example, `maskField="CNBR_MASK"` • hashAlias - Keystore alias to use if hashing the field for additional verification and indexing values. • hashField - The field to use as the hash value if hashing the field for additional verification and indexing values. • encryptedField - The field name to use when storing the encryption output to another field in the table. Add when using a higher level of encryption to hold the larger encrypted value.

Chapter 11

Web Services Security

The Inbound Web Services capability of Oracle Utilities Cloud Service, which is based on JAX-WS/JAX-RS implementation, allows for support for advanced security settings on individual services. This section applies to REST-based and SOAP-based services defined as inbound web services.

> **Note:** Refer to *Web Services Best Practices for Oracle Utilities Application Framework (Doc ID 2214375.1)* for additional implementation advice for web services security.

Oracle Utilities Cloud Service includes the following preonfigured Inbound Web Services configurations optimized for the Oracle Cloud Infrastructure:

- An internal web services capability rather than the Oracle Web Service Manager to reduce implementation cost.
- A multi-token WS-Policy (via K1-BASIC Web Service Annotation) for services authentication using `oracle/multi_token_rest_service_policy`. This policy supports several methods within a single policy.
- Other WS-Policy configurations are not available at present time. These do not need to be attached to any Inbound Web Service as annotations as these are global policies.
- A Web Services Catalog capability to control integration with Oracle Integration Cloud Services.
- Online service deployment is the only supported method at present time, which is available through the **Inbound SOAP Service Deployment** menu option. REST services are automatically deployed when active.

Chapter 12

Allowlist Support

Oracle Utilities Cloud Service's allowlist enforces the protection of resources within your implementation. Allowlists can also apply to non-cloud implementations and in some cases, extended to suit individual needs.

> **Note:** Oracle Utilities Cloud Service does not support allowlist customization.

This chapter includes the following:

SQL Allowlist

The SQL used in query zones and Groovy scripts can be limited in relation to supported SQL functions that prevent performance issues or inappropriate access to the database through Oracle Utilities Cloud Service functions.

Oracle Utilities Cloud Service provides F1-SQLFunctionWhiteList, which is an allowlist implemented as a Managed Content object. This is a non-changeable allowlist that lists the supported and usable SQL functions. Oracle Utilities Cloud Service generates a runtime error when running an SQL function that is not included in the allowlist.

HTML Allowlist

The HTML used in UI Maps can be limited in relation to supported HTML tags. Oracle Utilities Cloud Service provides F1-HTMLWhiteList, which is an allowlist implemented as a Managed Content object. This allowlist manages the list of valid HTML tags that can be used on HTML objects. Attempts to run a UI Map with an HTML tag not listed in F1-HTMLWhiteList are ignored as comments and may result to unexpected behaviors.

Groovy Allowlist

The Groovy language has been added as an alternative scripting language that can access low level APIs. As the language has access to low level APIs, it has been allowed to exclude parts of the language not appropriate for cloud implementations.

The Groovy allowlist confirms to the Oracle Cloud SDK's supported Groovy classes and methods. The Groovy allowlist appears on the Dashboard zone when implementations maintain scripts. Oracle Utilities Cloud Service does not support ADF extensions to Groovy. Refer to online documentation for more information and examples.

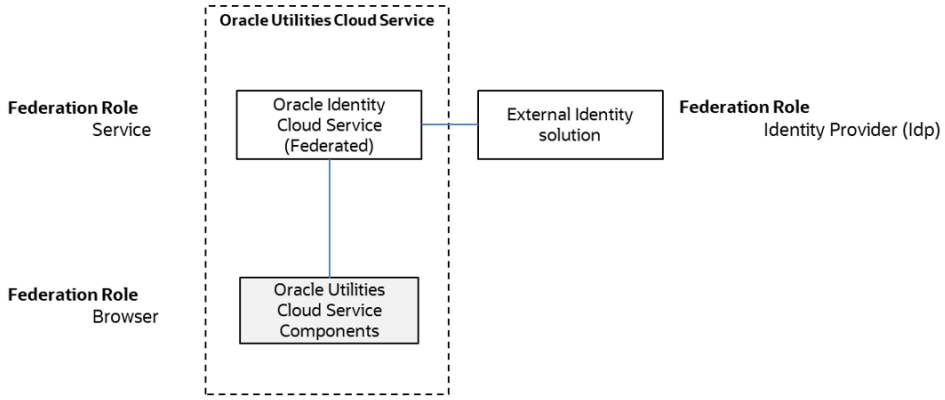
Chapter 13

Federated Security Support

Oracle Cloud Infrastructure Identity and Access Management (IAM) may be configured in Delegated Authentication mode to act as a service in federation when an external identity solution provides the identity of the Oracle Utilities Cloud Service implementation.

> **Note**: Delegated Authentication Mode is not supported with the IAM included in the base service. Customers requiring this capability must upgrade their IAM license.

In a federated security, the embedded IAM delegates security to a trusted external identity provider. Oracle Utilities Cloud Service acts as a conduit between the identity provider and the service in the federated security configuration. The relationship between the identity provider and service is illustrated below:



The completed federated security configuration governs all accesses to authenticate and authorize users to the Oracle Utilities Cloud Service.

This chapter includes the following:

- User Management Implications

User Management Implications

The user management implications when using the federated security model on Oracle Utilities Cloud Service are as follows:

- All users must be defined in the external identity provider using the tools provided by the provider external to the Oracle Utilities Cloud Service.
- Delegated authentication must be enabled with configuration of behavior of the integration between IAM and the identity provider.
- Users may be managed by IAM for deployment into Oracle Utilities Cloud Service as standard.
- If users are managed solely in the identity provider, IAM's Delegated Authentication must be altered accordingly, and users managed via IAM if permitted, or manually using the User object.

Chapter 14

Object Erasure Support

Oracle Utilities Cloud Service supports master object erasure, which addresses data privacy concerns and allows the removal of Personally Identifiable Information from Oracle Utilities Cloud Service whilst adhering to business rules. Note that object erasure is restricted to master data only, and transaction data erasure is through Information Lifecycle Management.

This chapter includes the following:

Object Erasure Configuration

The Object Erasure function provides the ability to define the following:

- An F1-OBJERSCH (Object Erasure) maintenance object that can map the reassure of the object and used as a basis for the business object to describe the storage of the Object Erasure information for individual objects.
- A maintenance object algorithm to the Maintain Object Erasure Schedule that defines the rules and retention for the object, including any obfuscation rules.
- A generic F1-OESMN batch control to implement the erasure or obfuscation rules in batch.

Refer to **The Approach to Implementing Object Erasure** section of the online documentation for more information about the process for configuring Object Erasure.

Chapter 15

Key Ring Support

Cryptography keys may be used to provide a signature or credentials to a request so that the system recognizes that the request comes from a trusted party. Keys may also be used to encrypt or decrypt files shared between two parties.

The Key Ring object is provided to reference the keys that are used over time for a given business use case. Only one key or key pair may be active at any given time.

The following sections include information about the functionality provided to support different key ring classes for particular use cases.

- RSA Signature Keys
- File Signing Keys
- OAuth Keys
- PGP File Encryption Keys

This chapter includes the following:

Maintaining Key Rings

The Key Ring maintenance function from the Administration menu is used to add, modify, and remove key ring definitions. To navigate to the option, select **Admin**, select **Security**, and select **Key Ring**.

Once within the function you may broadcast the key ring to maintain using the broadcast icon and use the **Edit** button to maintain the definition. You may use the **Add** function to add a new key ring entry.

When adding or maintaining a key ring the following information must be provided:

Field	Comments
Key Ring Business Object	Select the type of Key Ring to create: • OAuth Keys (F1-OAuthKeyRing) • Public Encryption Key (F1-ExtKeyRing) • RSA Signature Key Pair (K1-SignatureKey) - Used by Oracle Utilities Cloud Services only • Encryption Key Pair (F1-InternalEncryptionKey)
Key Ring	Name of the key ring. Custom key rings must be prefixed with CM to reduce risk of conflicts with Oracle keys.
Description	Short description of the key ring
Detailed Description	Optional, detailed description of the key ring

Save the additions/changes for the user using the **Save** function.

Generating Keys

Once the Key Ring is defined it must have at least one activated key pair. To generate a key pair, use the **Generate Key** button.

Once generated the key ring will appear in the **Key Pairs** zone with the appropriate fingerprint. To activate the key pair, use the **Activate** button to enable the key. It is recommended to only have one pair active for each key ring at most at any time. It is possible to support multiple, but this is not good security practice. Use the **View** under the Public Key column to view and pass on the public part of the key.

> **Note**: The private key is not visible from the product in line with security standards.

Using Key Rings

Key rings can be used within numerous objects within the product. Refer to the documentation for those objects on how to connect key rings. Once connected the object will appear in the **Key Ring References** zone.

Chapter 16

Redaction Rules

The Oracle Utilities Application Framework supports configurable redaction rules which allows exports using Content Migration Assistant (CMA) and Generalized Data Export (GDE) to scramble information as necessary for privacy purposes.

This capability is not used outside of Content Migration Assistant and Generalized Data Export.

This chapter includes the following:

Setting Up Redaction Functions

Before using Redaction Rules, a set of reusable Redaction Functions that describe the technique to be used to scramble information must be configured.

To maintain Redaction Functions, use the F1-RedactionFunction Extendable Lookup to define the technique to use including:

Field	Comments
Redaction Function	Identifier for function. Must be prefixed with CM for custom function entries to avoid conflicts with base provided functions
Description	Short description for function
Override Description	Override description to allow implementations to override short description of base provided functions
Detailed Description	Detailed description of function
Status	Status of function. Valid Values: • **Active**. Function is available for use. • **Inactive**. Function is not available for use. Only Active functions are applied.

Field	Comments
Function Type	Type of function. Valid Values are: • **Date Mask** used to mask dates • **Number Mask** to mask numbers • **Regular Expression** to mask general fields • **String Mask** to mask strings
Date Mask	Mask of date in ISO format. For example: YYYY-01-01 sets all dates where this function is used to the first day of the year of the record.
Start Offset	Start position offset in field for Number Mask and String Mask
End Offset	End position offset in field for Number Mask and String Mask
Replacement Digit	Digit to use as replacement between start and end offset for Number Mask
Regular Expression	Regex expression to find values within data for Regular Expression Mask
Replacement Expression	Regex expression to replace values found in regular expression for Regular Expression Mask
Replacement Character	Character to use as replacement in between start and end offset for Number Mask
Digits Only	Replace Digits only in string. Used for String Mask only. For example, replacing digits in phone numbers.

Setting Up Redaction Rules

The Redaction Rule Maintenance function from the Administration menu is used to add, modify, and remove Redaction Rule definitions. To navigate to the option, select **Admin**, select **Security**, and select **Redaction Rule**.

To maintain the Redaction Rules, specify the following:

Field	Comments
Redaction Rule	Identifier for rule. Must be prefixed with CM for custom Redaction Rules to avoid conflicts with base provided rules
Description	Short description for rule
Field Source Type	Source of field. Valid Values: • **Physical Field**. Field definition on a particular table. • **Referenced Field**. Set to apply to field across tables. • **XML Storage**. Element within CLOB.
Redaction Function	Redaction function to apply

Field	Comments
Table	Table Name for Field. Table must be defined as a Table object
Field	Field Name on Table. Field must be defined to Table on the specified Table object
Filter Expression	SQL WHERE Filter for field values to limit usage of redaction if necessary. For example: `OWNER_FLG = 'CM' AND…` The filter is limited to fields on the table. Leaving this value blank applies redaction to all values of the field.
Reference Field	Reference Field to apply redaction to.
XPath Expression	The XPath expression to determine the field in the CLOB to apply the rule to

Once Redaction Rules have been defined, they are automatically used by Content Migration Assistant (CMA) and Generalized Data Export (GDE). To bypass use of the Redaction Rules for Generalized Data Export, specify the appropriate value for the doNotApplyRedactRules parameter on the execution for the initial and/or ongoing extracts.

Chapter 17

Java Script Support

The Configuration Tools and legacy screen utilities used by the Oracle Utilities Application Framework supports a wide range of standards, but for security reasons use of Java script is restricted in certain circumstances to prevent injection.

The table below outlines which objects allow HTML formatting and Javas Script.

Component	Allows HTML formatting	Allow Java Script
UI Maps	Yes	Yes
Script Steps	Yes	Yes
Display Step in BPA	Yes	Yes
Object Description	Yes	No
FK Ref (UI Maps and Data Explorers)	Yes	No
FK Ref (legacy pages)	No	No
Data Explorer	Yes	No
Help Text	Yes	No
Others	No	No

All HTML code is run through the product HTML sanitization via the F1-HTMLWhitelist.