Oracle Utilities Cloud Services

Security Guide

Release 25.10
G39750-02
October 2025

Oracle Utilities Cloud Services Security Guide, Release 25.10

G39750-02

Contents

1

Introduction

Welcome to Oracle Utilities Cloud Services 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 Rate Cloud Service
- Oracle Utilities Work and Asset Cloud Service

This document includes the following:

- What's New In Security
- Introducing Security
- Authentication
- Authorization
- Managing Security
- Advanced Security
- Audit Facilities
- Database Security
- Encryption Feature Type
- Web Services Security
- Allowlist Support
- Federated Security Support
- Object Erasure Support
- Key Ring Support
- Redaction Rules
- Java Script Support
- Cookies Used by Cloud Services

Audience

The *Oracle Utilities Cloud Services Security Guide* is intended for Oracle Utilities Cloud Services 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 Services 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 Services works, and basic familiarity with the security aspects of the Oracle Cloud Infrastructure.

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 Services Implementation Guide
- Oracle Utilities Cloud Services Administration Guide - Identity and Access Management

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

Critical Patches

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

2

What's New In Security

With each release of the product new and improved security features are made available since the last release. Refer to the Oracle Cloud Applications Readiness site for the latest security-based changes.

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.

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.

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).

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.

Privileged Users

By default, the Oracle Utilities Cloud Services delivers a single initial privileged user SYSUSER in the installation. This user was intended to be used solely to add other initial users into your service. As this role is now provided by the Oracle Cloud Infrastructure Identity and Access Management solution provided with the service, the SYSUSER user is now delivered disabled by default.

For backward compatibility purposes, you may request to temporarily re-enable this user to migrate any configuration over to other users in this release. In future releases, the ability to re-enable the user will be revoked.

5

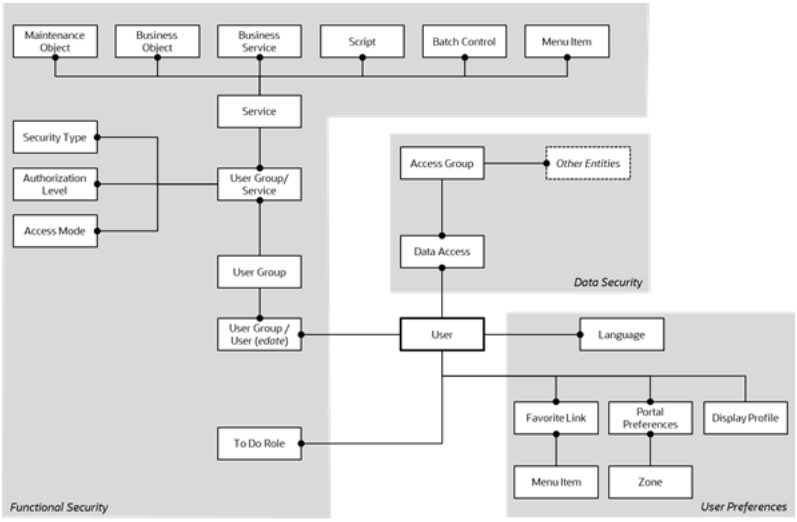
Authorization

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.

Authorization Model

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



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.
> It is now possible to configure a default template user on the F1- OIMUSR algorithm definition.

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.

6

Managing Security

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

This chapter includes the following:

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 *Oracle Utilities Cloud Services 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.

See **User - Main** in the online help provided with your service for information about user identity attributes.

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.

See **User - Main** in the online help provided with your service for information about creating template users.

Assign To Do Types

Oracle Utilities Cloud Services generatesTo 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.

See **User - Main** in the online help provided with your service for information about associated To Do Types with users and user groups.

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.

See **User - Portal Preferences** in the online help provided with your service for information about managing user portal preferences.

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.

See **User - Bookmarks** in the online help provided with your service for information about managing bookmarks.

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 Sidebar.

See **User - Favorite Links** in the online help provided with your service for information about managing favorite links.

Assign Favorite Scripts

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

See **User - Favorite Scripts** in the online help provided with your service for information about managing favorite scripts.

Assign User Characteristics

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

See **User - Characteristics** in the online help provided with your service for information about managing user characteristics.

Define Users to User Groups

Access to Oracle Utilities Cloud 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.

See **User - Main** in the online help provided with your service for information about managing user groups for a user.

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.

See **Defining User Groups** in the online help provided with your service for information about managing relationships between user groups and application services.

Application Services 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.

See **Defining Application Services** in the online help provided with your service for information about managing application services.

User Group Maintenance

User Group Maintenance allows you to define the Application Services that user groups can access and to connect users to user groups.

See **Defining User Groups** in the online help provided with your service for information about managing user groups.

Define Users to Data Access Groups

Data Access Groups define the subset of data objects that are accessible to the users.

See **Data Access Role - Access Group** in the online help provided with your service for information about managing data access groups.

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 the Oracle Utilities Cloud Service and is attached to some audit objects across the Oracle Utilities Cloud Service.

See **User - Main** in the online help provided with your service for information about enabling or disabling users.

Managing Batch Users

Oracle Utilities Cloud Services provision 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 Services provision 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 Services maintain 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 Services. Oracle Utilities Cloud Services automatically perform 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 Services (for federated implementations).

Deploy Users from Oracle Cloud Infrastructure Identity and Access Management

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

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.

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.

See **Defining Menu Options** in the online help provided with your service for information about managing menu security.

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.

See **Defining Security Types** in the online help provided with your service for information about managing 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 Services 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-DFLTS - This secures business objects and supports the Add, Modify, Delete, and Inquire access methods.

Data Masking Support

Oracle Utilities Cloud Services can mask data within objects in an appropriate fashion. Oracle Utilities Cloud Services do 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 Services supply the F1-MASK internal algorithm type, which performs basic data masking.

See **User Interface Masking** in the online help provided with your service for information about data masking.

Secure Online Debug Mode

Oracle Utilities Cloud Services' 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 Services' 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 Services support 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 **Sidebar** 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 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.

SCIM 2.0 Provisioning

By default, it is possible to provision users from the Oracle Cloud Infrastructure Identity and Access Management (IAM) using a pre-built adapter. It is also possible to directly provision users from a SCIM 2.0 compliant security repository. Refer to the online documentation provided with your service for more details of the SCIM 2.0 support.

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.

8
Audit Facilities

Oracle Utilities Cloud Services' inbuilt, configurable auditing facility provides the capability to register access 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.

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 Services.

Audit configuration for Oracle Utilities Cloud Services 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 on the cloud.
- **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.

See **Audit Query by Table/Field/Key** in the online help provided with your service for information about querying audit data based on tables, fields, and keys.

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.

See **Audit Query by User** in the online help provided with your service for information about querying audit data by user.

Read Audit

Oracle Utilities Cloud Services' 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.

9

Database Security

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

Cloud Database Security Setup

Oracle Utilities Cloud Services include a pre-configured 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 Services 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 Services components at service provisioning time.
- Inclusion of the Oracle SQL Developer for Web in Oracle Utilities Cloud Services and use of the identity provided by Oracle Cloud Infrastructure Identity and Access Management (IAM).
- Inclusion of the following functions in the database and pre-configured 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 pre-configured for Oracle Utilities Cloud Services.
- Use of Oracle Resource Management on all access modes. All policies are pre-configured for Oracle Utilities Cloud Services.

10

Encryption Feature Type

Oracle Utilities Cloud Services provide 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.

Encrypted Fields Configuration

See **Encrypting Sensitive Data** in the online help provided with your service for information about encryption configuration.

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

11

Web Services Security

The Inbound Web Services capability of Oracle Utilities Cloud Services, 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 Services include the following pre-configured 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.

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 Services do not support allowlist customization.

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 Services generate 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 Services provide 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 Classes and Methods for Use in Groovy Scripts . The Groovy allowlist appears on the Dashboard zone when implementations maintain scripts. Oracle Utilities Cloud Services do not support ADF extensions to Groovy. Refer to online documentation for more information and examples.

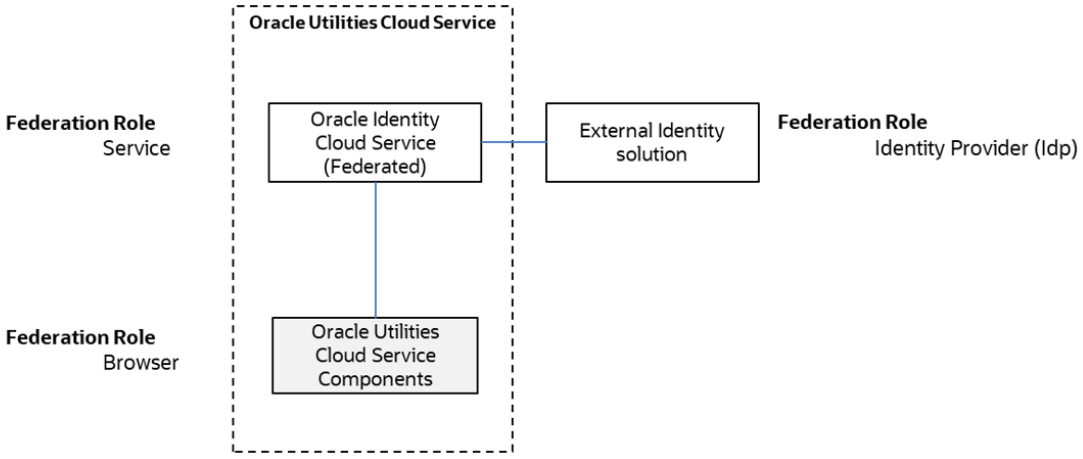
13

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.

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.

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.

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.

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

Maintaining Key Rings

The Key Ring maintenance function from the Administration menu is used to add, modify, and remove key ring definitions.

See **Understanding Key Rings** in the online help provided with your service for information about managing key rings.

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.

See **Understanding Key Rings** in the online help provided with your service for information about generating key pairs.

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.

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.

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.
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

Redaction rules must be configured for application to data to be redacted.

See **Defining Redaction Rules** in the online help provided with your service for information about maintaining redaction information.

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.

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 Java 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.

18

Cookies Used by Cloud Services

Oracle Utilities cloud services use several cookies for managing the behavior of the service.

The table below provides information that may assist you when you configuring cookie controls at the network level.

All cookies except for ORA_OUAF_Login_language cookie, are session cookies that are stored in memory and are removed when the browser or session is closed.

Cookie	Usage
ORA_OUAF_Login_language	This is a persistent cookie that is used to store the users preferred language used for the provided login screen. For details of its contents refer to Do Weblogic CCB Cookies Contain Any Trace Information? (Doc ID: 2443627.1) available from My Oracle Support.
JSESSIONID	The JSESSIONID cookie, which expires when the user's browsing session ends, helps the server to manage user sessions. It is a standard container cookie. While not accessible to scripts, this cookie can be deleted from the client-side. However, the cookie will be re-sent during the next request from the user. This cookie tracks each request from the same browser, ensuring that the same session data is available on the server side. It does not contain any personal data. This cookie is automatically secured by the cloud service.
ORA_OUAF_Language	This is an internal cookie that stores the active language used by the browser. This may change if the user switches languages during the session. The cookie is used by the server to render the screen using the language correctly.
ORA_OUAF_Language_Dir	This is an internal cookie that stores the active language direction used by the browser. This may change if the user switches languages during the session. The cookie is used by the server to render the screen using the language correctly. By default, it is set to ltr for most implementations and rtl for Arabic implementation.
ORA_OUAF_Locale_Info	This is an internal cookie that stores the locale information used for sorting. This may change if the user switches languages during the session.
ORA_OUAF_SESSION_EXP ORA_OUAF_SERVER_TIME ORA_OUAF_CLIENT_TM_OFFSET	This is a set of internal cookies that are used to determine inactivity timeouts for user sessions. It is used by the server to inform the user of the session timeout.

Cookie	Usage
ORA_OUAF_START_LOGIN	This is an internal cookie used to whether the login screen used so that it can be reused for the session timeout. This value is determined from the server configuration.

Glossary

Index