

Oracle® Revenue Management and Billing
Version 2.6.0.0.0

Security Guide

Revision 9.0

E86907-01
May, 2017

ORACLE®

Oracle Revenue Management and Billing Security Guide

E86907-01

Copyright Notice

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Trademark Notice

Oracle, Java, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

License Restrictions Warranty/Consequential Damages Disclaimer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure, and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or de-compilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data delivered to U.S. Government end users are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data shall be subject to license terms and restrictions as mentioned in Oracle License Agreement, and to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). No other rights are granted to the U.S. Government.

Hazardous Applications Notice

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Third Party Content, Products, and Services Disclaimer

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products, or services.

Preface

About This Document

This document describes how to configure security for the Oracle Revenue Management and Billing (ORMB) application using the default security features. To use this document, you need a basic understanding of how the product works, and basic familiarity with the security aspects of Oracle WebLogic and Oracle Database.

Intended Audience

This document is intended for the following audience:

- Product, Database and Security Administrators
- Development Team
- Consulting Team
- Implementation Team

Organization of the Document

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

Section No.	Section Name	Description
Section 1	Introduction	Explains how the security features of Oracle Revenue Management and Billing protects access to the product, its functionality and the underlying data stored and managed through the product.
Section 2	Security Features in ORMB V2.6.0.0.0	Lists and describes the security features of Oracle Revenue Management and Billing Version 2.6.0.0.0, which provide superior access control, privacy, and accountability.
Section 3	Authentication	Explains how online, batch, and web service authentication is handled in Oracle Revenue Management and Billing Version 2.6.0.0.0.
Section 4	Authorization	Describes how the identified users are authorized to use specific functions and data within the product. It also provides detailed information about the security authorization model used by Oracle Utilities Application Framework (OUAF).
Section 5	Managing Security	Describes how to manage the security definitions from the product, security infrastructure and from the security repositories.

Section No.	Section Name	Description
Section 6	Advanced Security	Lists and describes the advanced security settings that can be configured to support various security requirements.
Section 7	Audit Facilities	Explains how to configure the audit facility to track changes made to the key data.
Section 8	Database Security	Lists a predefined set of database users and roles shipped with the product. It also explains various database security methods that can be used to provide restricted access to the database users.
Section 9	Security Integration	Lists and describes the additional security features or security products that can be integrated with the product to augment the security setup.
Section 10	Keystore and Truststore Support	Explains how to use keystore to encrypt and decrypt data, such as passwords. It describes how to create and modify a keystore and how to synchronize data encryption.
Section 11	Encryption Feature Type	Explains how to create a feature configuration for encryption using the Encryption feature type.
Section 12	Web Services Security	Explains how the inbound web services capability, based upon a JAX-WS implementation, allows support for WS-Security and WS-Policy support on individual inbound web services from a number of perspectives.
Section 13	Whitelist Support	Explains the use of whitelists, which is enforced to protect resources within the oracle cloud implementation. These whitelists can also apply to non-cloud implementations and in some cases can be extended to suit individual needs.
Section 14	Custom Authentication Service Provider	Provides support for complex domain security configurations.

Related Documents

You can refer to the following documents for more information:

Document	Description
<i>Oracle Revenue Management and Billing Version 2.6.0.0.0 Release Notes</i>	Provides a brief description about the new features, enhancements, UI and database level changes, supported platforms, framework upgrade, supported upgrades, and technology upgrade made in this release. It also highlights the discontinued features, bug fixes, and known issues in this release.
<i>Oracle Revenue Management and Billing Installation Guide</i>	Lists the application server pre-requisites, supported platforms, and software and hardware requirements for installing the Oracle Revenue Management and Billing application. It explains how to install the Oracle Revenue Management and Billing application.
<i>Oracle Revenue Management and Billing Database Administrator's Guide</i>	Provides information about the Oracle Database Server and Client required for installing the Oracle Revenue Management and Billing database. It explains how to install database with and without demo data. It provides database configuration guidelines including recommended settings for the Oracle Exadata Database machine.
<i>Oracle Revenue Management and Billing Server Administration Guide</i>	Explains the Oracle Revenue Management and Billing (ORMB) architecture and technical know-how required for configuring and using the ORMB application. It explains how to configure and deploy web and business application servers. In addition, it explains how to monitor client machines, web and/or business application servers, and database connections.

You can also refer to the following artifacts on [My Oracle Support](#) using the respective Doc ID or part number:

- *Advanced Security Oracle Utilities Application Framework (Doc ID: 1375615.1)*
- *Technical Best Practices For Oracle Utilities Application Framework Based Products (Doc ID 560367.1)*
- *Oracle Utilities Application FW - Batch Best Practices (Doc ID 836362.1)*
- *Production Configuration Guidelines Oracle Utilities Application Framework (Doc ID 1068958.1)*
- *Oracle Utilities Framework Application - Database Vault Integration features (Doc ID 1290700.1)*
- *Oracle Identity Management Suite Integration Oracle Utilities Application Framework (Doc ID 1375600.1)*
- *Oracle Database Vault Administrator's Guide (Part Number E23090-12)*
- *Oracle Audit Vault Administrator's Guide (Part Number E14459-12)*
- *Oracle Database Advanced Security Administrator's Guide (Part Number E40393-07)*

- *Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server (Part Number E13713-06)*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server (Part Number E13707-06)*

Conventions

The following conventions are used across this document:

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

Note:

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.

Contents

1. Introduction.....	1
2. Security Features in ORMB V2.6.0.0.0.....	3
2.1 Batch Control Security	3
2.2 Support for Federated Login.....	4
2.3 URI Validation and Substitution.....	4
2.4 Bypassing Home Page	4
2.5 Whitelisted Groovy Support	5
2.6 SQL Whitelisting Support	5
2.7 Logging Changes.....	5
2.8 Support for Multiple Security Policies as Annotations	5
2.9 Enhanced Support for Oracle Web Services Manager.....	5
2.10 WS-Policy Direction Override Support.....	6
2.11 Web Services Catalog Enhancements	6
3. Authentication.....	7
3.1 About Authentication	7
3.2 Online Authentication.....	7
3.3 Batch Authentication	8
3.4 Web Service Authentication	8
4. Authorization.....	9
4.1 About Authorization	9
4.2 Authorization Model.....	9
5. Managing Security	11
5.1 About Managing Security.....	11
5.2 Managing Online Users.....	11
5.2.1 Managing Users	12
5.2.2 Template Users.....	14
5.2.3 Assigning To Do Types	14
5.2.4 Assigning User Portal Preferences.....	15
5.2.5 Assign Bookmarks.....	16
5.2.6 Assign Favorite Links.....	17
5.2.7 Assign Favorite Scripts	18
5.2.8 Assign User Characteristics.....	18
5.2.9 Defining Users to User Groups	19
5.2.10 Defining User Groups to Application Services.....	20
5.2.11 Define Users to Data Access Groups	26
5.2.12 User Enable and Disable	28

5.3	Managing Batch Users	29
5.4	Managing Web Services Users.....	29
5.5	Authentication User.....	30
6.	Advanced Security	31
6.1	About Advanced Security.....	31
6.2	JEE Authentication Group	31
6.3	Logon Configuration.....	32
6.4	Data Ownership Rules.....	32
6.5	Configuring JMX Security	33
6.5.1	Default Simple File Based Security	33
6.5.2	SSL based Security	34
6.5.3	Using Other Security Sources	35
6.6	Menu Security Guidelines	35
6.7	Security Types	36
6.8	Default Generic Application Services.....	37
6.9	Administration Delegation.....	37
6.10	Secure Communications (SSL).....	38
6.11	Data Masking Support.....	38
6.12	Securing Files.....	42
6.13	Password Management	43
6.14	Securing Online Debug Mode	44
6.15	Securing Online Cache Management.....	44
6.16	Web Services Security.....	44
6.17	Message Driven Bean Security.....	45
6.18	SOAP Security.....	46
6.19	Groovy Support.....	46
7.	Audit Facilities.....	47
7.1	About Audit	47
7.2	Audit Configuration.....	47
7.3	Audit Query by Table/Field/Key.....	48
7.4	Audit Query By User.....	49
7.5	Read Auditing	50
7.6	Integrating to Audit Vault	50
8.	Database Security	52
8.1	About Database Security.....	52
8.2	Database Users	52
8.3	Database Roles.....	53
8.4	Database Permissions	53
8.5	Using Transparent Data Encryption	53

8.6	Using Database Vault	53
9.	Security Integration	54
9.1	About Security Integration.....	54
9.2	LDAP Integration	54
9.3	Single Sign On Integration.....	54
9.3.1	Kerberos Support.....	54
9.4	Oracle Identity Management Suite Integration.....	55
10.	Keystore and Truststore Support.....	56
10.1	Creating the Keystore and Truststore	56
10.2	Altering the Keystore/Truststore Options	57
10.3	Synchronize Data Encryption	58
10.4	Upgrading from Legacy to Keystore.....	60
10.5	Importing Keystores/Truststores	61
11.	Encryption Feature Type.....	62
11.1	Overview	62
11.2	Configuration of Encrypted Fields.....	63
12.	Web Services Security.....	65
12.1	About Web Services Security	65
12.2	Annotation Security	65
12.3	Oracle WebLogic WS-Policy Support	66
12.4	Oracle Web Services Manager Support	66
12.4.1	Access Control Support.....	66
12.5	Support for Multiple Policies	67
12.6	Importing Certificates for Inbound Web Services.....	67
13.	Whitelist Support.....	68
13.1	About Whitelist Support	68
13.2	URL Whitelist.....	68
13.2.1	Implementing a Custom URL Whitelists	69
13.3	SQL Whitelist.....	70
13.4	HTML WhiteList.....	70
13.5	Implementing a Custom HTML Whitelist.....	70
13.6	Groovy Whitelist	70
14.	Custom Authentication Service Provider.....	71
14.1	What does this Security Provider do?.....	71
14.2	Where would I use this Security Provider?	71
14.3	Implementing the Security Provider	72

1. Introduction

One of the key aspects of the product is security which not only confirms the identity of an individual user but, once identity is confirmed, what data and what functions that user has access to within the product. Security is one of the key features of the product architecture protecting access to the product, its functionality and the underlying data stored and managed via the product.

From an architecture point of view the following summarizes the approach to security:

- **Web Based Authentication** – The product provides a default method, using a traditional challenge and response mechanism, to authenticate users.
- **Support for JEE Web Application Server Security** – The supported JEE Web Application Servers can integrate into a number of internal and external security stores to provide authentication services. The product can use those configurations, to liaise via the JEE Web Application Server, to authenticate users for online and Web Services based security.
- **Operating System Security** – For non-online and non-web service based channels, the product utilizes the operating system security (including any additional products used to enhance the base operating system security).
- **Non-Cookie Based Security** – After authentication the user's credentials form part of each transaction call to correctly identify the user to the internal authorization model to ensure the user is only performing permitted actions. This support is not browser cookie based.
- **Secure Transport Support** – Transmission of data across the network can utilize the secure encryption methods supported for the infrastructure.
- **Inter-Component Security** - Calls within the product and across the tiers are subject to security controls to ensure only valid authenticated and authorized users using Java Authentication and Authorization Services (JAAS).
- **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 to within the product.
- **Native Web Services Security** – Web Services available from the product are natively available from the JEE Web Application Server. A wide range of security policies are available.
- **Keystore Support** - Keys for encryption can be externalized in JCEKS based keystore.
- **Integration with Other Security Products** – Implementation of security varies from customer to customer so the product allows integration of other security products to offer enhanced security implementations, either directly or indirectly.

In addition to the security features described in the [Security Features in ORMB V2.6.0.0.0](#) section, Oracle Revenue Management and Billing provides the following additional security resources:

- **Oracle Database Vault** – Oracle Database Vault provides fine-grained access control to your sensitive data, including protecting data from privileged users. *Oracle Database Vault Administrator's Guide* and *Database Vault Integration (Doc ID: 1290700.1)* describes how to use Oracle Database Vault.

- **Oracle Audit Vault** – Oracle Audit Vault collects database audit data from sources such as Oracle Database audit trail tables, database operating system audit files, and database redo logs. Using Oracle Audit Vault, you can create alerts on suspicious activities, and create reports on the history of privileged user changes, schema modifications, and even data-level access. *Oracle Audit Vault Administrator's Guide* explains how to administer Oracle Audit Vault.
- **Oracle Advanced Security** - See *Oracle Database Advanced Security Administrator's Guide* for information about advanced features such as transparent data encryption, wallet management, network encryption, and the RADIUS, Kerberos, Secure Sockets Layer authentication.
- **Oracle Identity Management Suite** – Oracle offers a range of specialist security products to manage user identities, password management, single sign on, access management, identity governance, fraud detection and directory services. The Oracle Identity Management Suite Administrator Guides and Oracle Identity Management Suite Integration with Oracle Utilities Application Framework based products (Doc ID: 1375600.1) provides additional information about these products and integration capabilities.

2. Security Features in ORMB V2.6.0.0

The following security features are available in Oracle Revenue Management and Billing (ORMB) Version 2.6.0.0.0:

- Batch Control Security
- Support for Federated Login
- URI Validation and Substitution
- Bypassing Home Page
- Whitelisted Groovy Support
- SQL Whitelisting Support
- Logging Changes
- Support for Multiple Security Policies as Annotations
- Enhanced Support for Oracle Web Services Manager
- WS-Policy Direction Override Support
- Web Services Catalog Enhancements

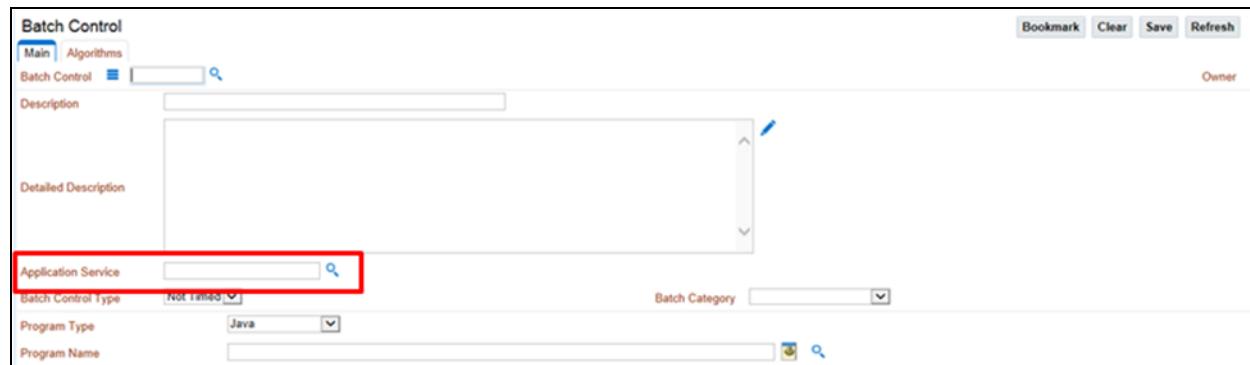
These security features provide superior access control, privacy, and accountability while using ORMB.

2.1 Batch Control Security

In past releases, security for batch processes was provided at the service level and parameter level for any of the services called by the batch job represented by the batch control. In this release it is now possible, optionally, to attach an application service at the batch control level to control which users can submit particular batch controls. This provides a simplified ability to control access at the job level rather than service level.

This can be used in testing environments to limit which batch controls can be submitted by testers and in production can be used to lockdown critical batch controls to specific users.

The Application Service is now configurable on the Batch Control. For example:



The screenshot shows the 'Batch Control' configuration page. At the top, there are tabs for 'Main' (which is selected) and 'Algorithms'. Below the tabs are fields for 'Description' and 'Detailed Description'. A red box highlights the 'Application Service' field, which contains a search bar and a magnifying glass icon. To the right of the search bar are buttons for 'Bookmark', 'Clear', 'Save', and 'Refresh'. Below the search bar are dropdown menus for 'Batch Control Type' (set to 'Not Timed') and 'Batch Category'. At the bottom of the form are dropdown menus for 'Program Type' (set to 'Java') and 'Program Name', followed by a search bar and a magnifying glass icon.

Note: For backward compatibility, leaving this Application Service blank we revert to service level security.

2.2 Support for Federated Login

In this release the first layer of federated login has been implemented with the introduction of an Oracle Utilities Application Framework specific Security Provider for use within the Oracle WebLogic product domain. In past releases, these additional checks have been done as part of the login process. Using this provider it is possible to shift when these checks are performed and in particular when multiple authentication sources are used in the domain security configuration.

This security provider has the following functionality:

- Allows the domain security to directly interrogate the Oracle Utilities Application Framework security model within the domain security configuration. The Oracle Utilities Application Framework Security Provider checks that the user identity exists within the product security and that the user is enabled. If the user is not defined or is disabled then a security violation is passed back to the Oracle WebLogic domain to deal with in an appropriate manner.
- When using federation or multiple authentication sources it is now possible to designate when the Oracle Utilities Application Framework Security Provider is used to check the applicability of the user in terms of the product. This would allow the security to be verified within any phase of the login process.
- The Security Provider allows for configuration of the authentication group and any users exempt from the provider (for configuration of privileged accounts).

The use of the Security Provider is optional and if used, can be used with implementations using federated and non-federated configurations.

2.3 URI Validation and Substitution

In past releases, any URI setting such as URL, File Path and File URL was hardcoded on the relevant object to provide an interface. This would mean that transferring data across environments would need manipulation of these setting manually to correctly orient such settings on a target environment.

In this release a number of new facilities have been introduced to help make these settings transferrable and secure:

- URI can be whitelisted to ensure valid and secure locations. The whitelist is configurable and is checked at access time for each URI call.
- URI specifications can now include substitution variables to allow parameterization of URI components. A substitution list is provided to implement the physical path per environment. This file is maintained in \$SPLEBASE/etc/substitutionVariableList.xml (or %SPLEBASE%\etc\substitutionVariableList.xml in Windows).

2.4 Bypassing Home Page

In past releases, external calls to particular pages were routed through the user's home page which may cause delays in navigating from external systems. In this release it is now possible to navigate directly to a page or portal and bypassing the home page using the `initNav=false` URL option on the call. For example:

```
<system-url>/cis.jsp?script=F1-GotoPrtl&mo=F1-MIGRPLAN&pkValue1=F1-AlgorithmType&initNav=false
```

Note: It is recommended to use the F1-GotoPrtl script for inbound calls to use this facility.

2.5 Whitelisted Groovy Support

In past releases Groovy was added as a supported language for service script based customizations. The scope of support of the Groovy language has been restricted according to the Cloud SDK whitelist for Cloud implementations.

2.6 SQL Whitelisting Support

In this release, a property setting has been added to allow restriction of the SQL functions that can be used when defining an SQL statement in a query zone, inline within a Groovy script or using the Select Records algorithm for plug-in based batch jobs. An error is issued if the SQL statement contains functions not listed in the whitelist. The whitelist is maintained as managed content as F1-SQLFunctionWhitelist.

2.7 Logging Changes

In this release, the logging has been enhanced to mask the information captured in the logs depending on the user of the log. This is the initial part of an overall enhancement to separate technical messages from business messages to provide a focused efficient logging system.

2.8 Support for Multiple Security Policies as Annotations

In past releases, support for multiple WS-Policies for web services required using the inbuilt externalized policy support in either Oracle WebLogic or Oracle Web Services Manager. In this release it is now possible to attach multiple policies to allow implementations to use this facility within the Inbound Web Service definition itself as multiple annotations.

A sequence number has been added for annotations on Inbound Web Services. For example:



2.9 Enhanced Support for Oracle Web Services Manager

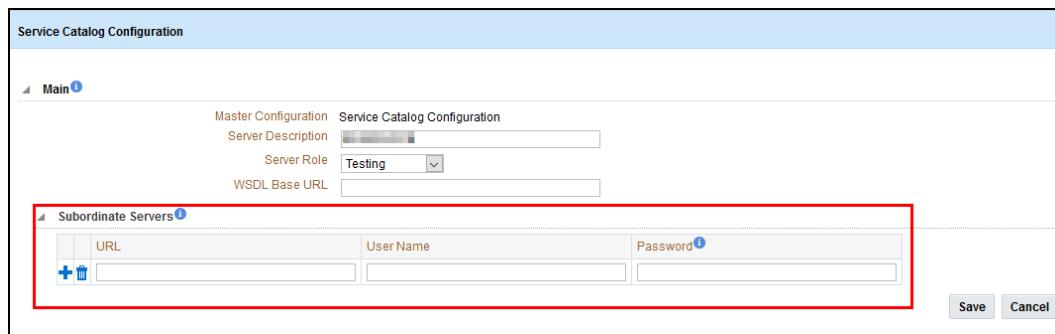
In past releases WS-Policies were restricted to one source, with either using annotations, Oracle WebLogic or Oracle Web Services Manager. In this release it is possible to add Oracle Web Services Manager as a delegated source, via an annotation, for the WS-Policy applied to an individual Inbound Web Service. This allows annotations and Oracle Web Services Manager policies to be implemented as multiple policies with the specification of the Inbound Web Service and their relationship modelled via the annotation sequence.

2.10 WS-Policy Direction Override Support

In this release the policy annotation type has been enhanced to specify which direction the policy applies to, whether it is for inbound communications, outbound communications or both. This allows the policy annotation type to be restricted to apply to Inbound Web Services and/or Outbound Messages.

2.11 Web Services Catalog Enhancements

In this release the Web Services catalog feature used for the Oracle Integration Cloud Service has been extended to support subordinate servers for licensing purposes. It is possible to designate a master server with related subordinate servers for supporting multiple product installations from a single connection. The credentials for those subordinate servers can be encrypted using the Encryption feature configuration. For example:



3. Authentication

3.1 About Authentication

From a security point of view authentication is 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 user ID and password. It can be also as complex as using digital certificates as the identification mechanism and numerous other schemes for user identification.

The authentication aspect of security for the product is delegated to the infrastructure used to run the product. This is due to a number of reasons:

- **Authentication Scheme Support** – The JEE Web Application Server supports a number of industry standard security repositories and authentication methods. These can be native to the JEE Web Application Server or additional products that can be integrated.
- **Enterprise Level Identity Management** – Identity Management is typically performed at an enterprise level rather than managed at an individual product level. The product typically is not the only application used at any site and managing security across the enterprise is more efficient.

3.2 Online Authentication

The product delegates the responsibility of authentication of the online users to the JEE Web Application Server. This means that any integration that the JEE Web Application Server has with specific security protocols or security products can be used with the product for authentication purposes. The configuration of authentication is therefore performed within the JEE Web Application Server itself.

Typically the JEE Web Application Server support one or more of the following:

- **Inbuilt Security** – The JEE Web Application Server typically supplies a default basic security store and associated security management capability that can be used if no other security repository exists.
- **LDAP Based Security** – The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing and maintaining distributed directory information services. LDAP is used to standardize the interface to common security repositories (such as Oracle Internet Directory, Microsoft Active Directory etc). LDAP support may be direct or indirect via Identity Management software like Oracle Virtual Directory or Oracle Identity Federation.
- **SAML Based Security** – Security Assertion Markup Language (SAML) is an XML based data format for exchanging authentication and authorization information between parties.
- **DBMS Based Security** – The JEE Web Application Server can store, manage and retrieve security information directly from a database.
- **Operating System Based Security** - The JEE Web Application Server can store, manage and retrieve security information directly from the underlying operating system.

- **Oracle Utilities Application Framework Security Provider** – The Oracle Utilities Application Framework includes an optional custom WebLogic Security Provider that allows implementations to verify user identity and whether the user is enabled as part of a security domain configuration. If the security provider is not used, these attributes are checked at login time.

These security configurations can be natively support or can be augmented with additional products.

Refer to the Security Guides supplied with your JEE Web Application Server for details of the security configuration process.

3.3 Batch Authentication

The Batch component of the architecture utilizes the operating system based security (including any extensions to that security) to authenticate users to execute batch processes. From an authentication point of view:

- Batch users must be defined in the operating system and associated with the operating system security group assigned at product installation time. This ensures users have appropriate access to product resources and the ability to write logs.
- Threadpools can be started by any valid operating system user but ideally threadpools and submitters should be executed by the same operating system user.
- Before any threadpool or submitter is executed the user must execute the `splenviron` utility to set the environment variables for the product correctly. This can be done at the command line for each threadpool and submitter or globally using the logon profile for the operating system user.

3.4 Web Service Authentication

The Web Service component of the product is housed in the JEE Web Application Server and utilizes the native Web Services security mechanism supported by that server.

From an authentication point of view:

- The Web Service is deployed using an administration account using the utilities provided from the product online (for developers) or using command line utilities.
- The Web Service is managed using the administration account using the administration console provided with the JEE Web Application Server.
- The JEE Web Application Server allows security policies and/or security access rules to be configured at an individual Web Service point of view. Any of the valid policies and security rules supported by the JEE Web Application Server can be used.
- Web Service management products such as Oracle Web Services Manager can be used to augment security for Inbound Web Services.

4. Authorization

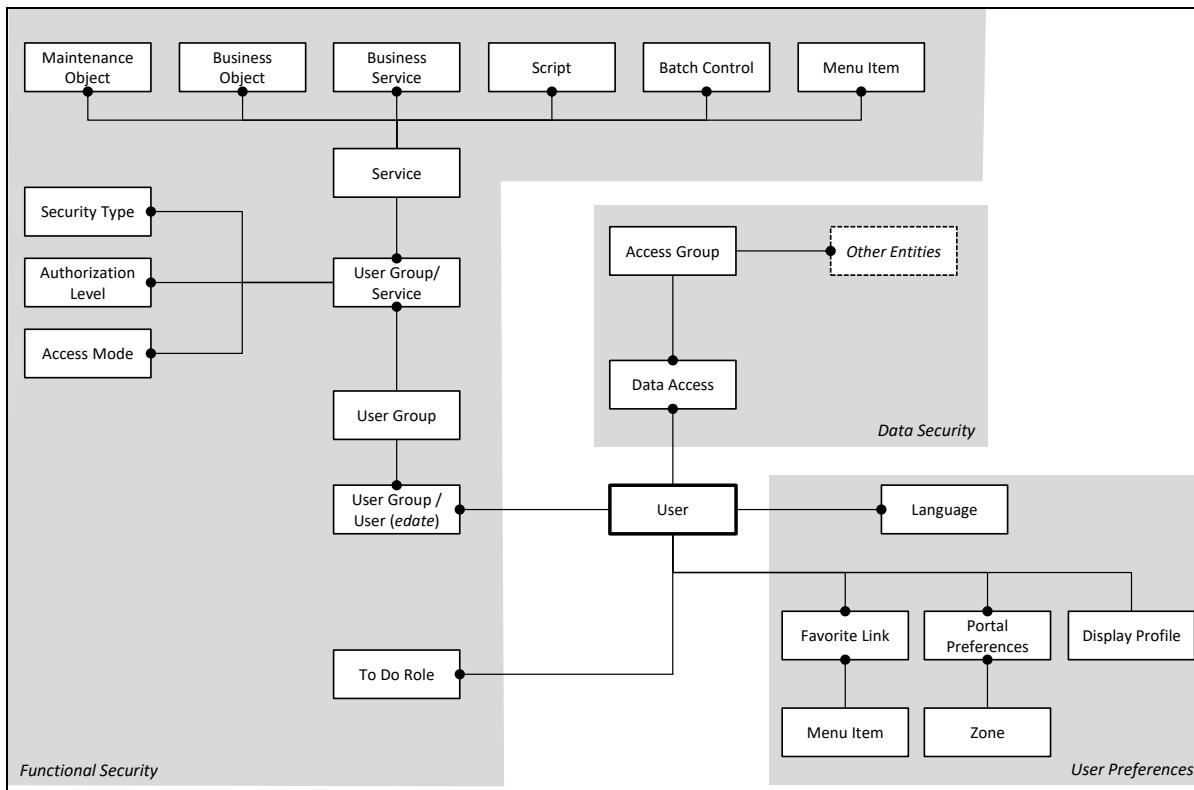
Once a user is identified they must be authorized to specific functions and data within the product.

4.1 About Authorization

Oracle Utilities Application Framework uses an inbuilt security model for authorization. This model contains all the data necessary for the definition of authorizations to function and data.

4.2 Authorization Model

The following data model describes the security authorization model.



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 etc), and Language used for screens and messages and other attributes. Users are attached to To Do roles which allow the user to process any error records for background processes. For example, if the XXX background process produces an error it is possible to define which users will process and address those errors.

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 a mechanism 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 product. Loosely they correspond to each of the screens accessible in product. 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 is allowed to those functions for user groups (and hence users).

Additionally, it is possible to define the authorization level that is allowed for 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 additional authorization is obtained. The Authorization Level is associated with a Security Type which defines the rules for that 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 any Maintenance Object security. The same applies to Business Services security overriding the Application Service it is based upon.

Oracle Utilities Application Framework allows you to limit a user's access to specific data entities to prevent users without appropriate rights from accessing specific data. By granting a user access rights to an account, you are actually granting the user access rights to the account's bills, payment, adjustments, orders, etc.

An Access Group defines a group of Accounts that have the same type of security restrictions. A Data Access Role defines a group of Users that have the same access rights (in respect of access to entities that include access roles). When you grant a data access role 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 points summarize 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 group. An access group may be linked to one or more data access roles.

Information in the security model can be manually entered using online transactions and also can be imported and synchronized using a LDAP import function provided with the Web Services Adapter. The latter is typically used with customers who have lots of online users to manage.

The authorization model is used by all modes of access to the product. Native interfaces (java classes) are used by all objects and a PL/SQL procedure is provided for reporting interfaces.

5. Managing Security

5.1 About Managing Security

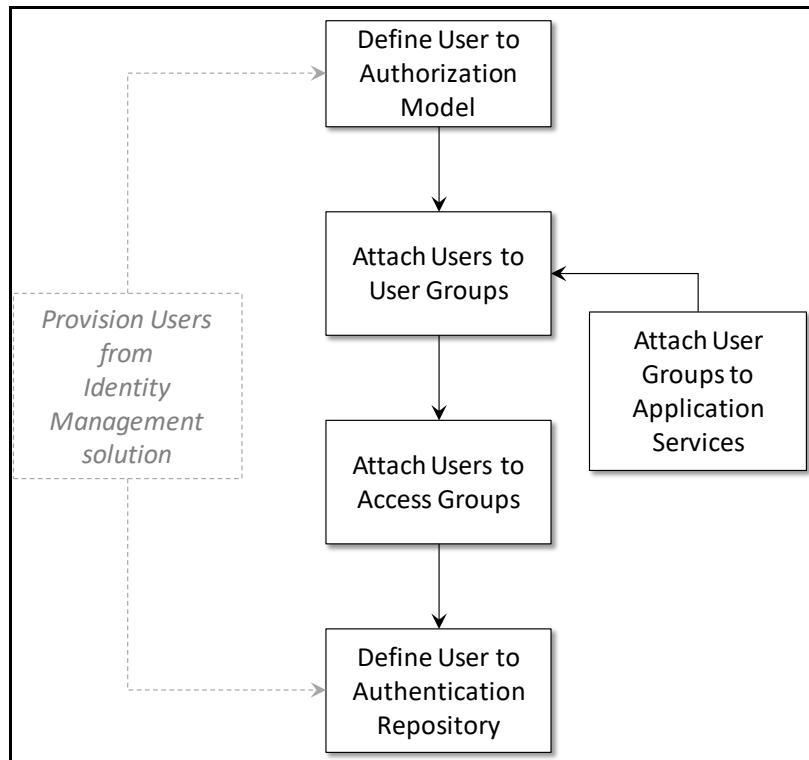
Once the security definitions are established they must be managed from the product itself, security infrastructure and security repositories used.

5.2 Managing Online Users

To manage online users a number of facilities must be configured:

- The security repository and rules must be configured in the JEE Web Application Server to enable authentication. Refer to the *JEE Web Application Server Administration Guides* for more information.
- The product group used to connect users to JEE resources should be created in the security repository and configured in the product configuration. The default value for this setting is `cisusers`. Refer to the *Oracle Revenue Management and Billing Server Administration Guide* for more information on this setting.
- Users need to be connected to the product group within the security repository to indicate that they can access the JEE resources.

The process for managing online users is outlined in the following process:



- Users should be defined to the authorization model to define their profile and permissions within the product. Refer to the [Managing Users](#) section for more details of this process.

- Attach user groups to application services to define the subset of service and actions valid for that group of users. Refer to the [Defining User Groups to Application Services](#) section for more details of this process.
- Attach Data Access Groups to the users. This defines the subset of data that the user has access to. Refer to the [Define Users to Data Access Groups](#) section for more details of this process.
- Attach users to the appropriate user groups to define the subset services and valid actions the user can perform within the product. Refer to the [Defining Users to User Groups](#) section for more details of this process.

5.2.1 Managing Users

The user object in the product is used to record the security information used for identification of the user and their permissions.

The product provides a maintenance function to maintain these definitions within the product. To maintain the users the following is performed:

- Navigate to the **Admin Menu → U → User** menu option. Using the + option on the menu allows navigation to the add function.
- The User maintenance object is displayed which maintains the security information for a user.
- A screen similar to the one shown below is displayed:

	User Group	Expiration Date	Owner
	ALL_SERVICES	System User Group	12-31-2100
			Framework

Field	Comments
User ID	This is the unique user identifier used within the product used for authorization activities. Limited to eight (8) characters in length.
Login ID	This is the unique user identifier used within the product used for authentication purposes. This must match the value used in the security repository to successfully use the product. Limited to 256 characters in length. This value can be the same or different to the User ID.
Last Name	Last Name of user. Limited to 50 characters in length.
First Name	First Name of user. Limited to 50 characters in length.
User Enable	Whether the user is active in the security system or not. Valid Values: Yes (default) – User is active and can use the system, No – User is disabled and cannot use the system. Refer to the User Enable and Disable section for more details.
User Type	The type of user. Valid Values: Blank = Normal user, Template = Template User.
Language	Default Language used for user. For non-English languages, Language pack must be installed to use specific languages.
Display Profile ID	The display profile associated with the user. This controls the display of currency, dates etc...
Time Zone	Time Zone allocated to user account ¹ .
Email Address	Optional Email address associated with user. This is used by utilities and can be used for interfaces requiring email addresses.
Dashboard Width	Default width for Dashboard Portal. Setting this value to zero (0) will disable the dashboard altogether.
Home Page	The default home page associated with the user.
Portals Profile User ID	The user ID used to inherit portal definitions from. Refer to the Template Users section for more information.
Favorites Profile User ID	The user ID used to inherit favorite definitions from. Refer to the Template Users section for more information.

¹ This feature is only applicable to specific products. Check your product online documentation for more details about applicability.

Field	Comments
To Do Summary Age Bar	The settings for the color coding of 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 the Defining Users to User Groups section for more information.

- Save the additions/changes for the user using the Save function on the top of the screen.

5.2.2 Template Users

By default portal preferences and favorites are set at an individual user level. It is possible to inherit the portal preferences and/or 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.

To use this functionality the following must be performed:

- Setup each user to be used as template and indicate the user type is set to Template to indicate such.
- For any user that will inherit the portal preferences and/or favorites specify the appropriate template user in the following fields:
 - Portal Preferences – Use the Portals Profile User ID to indicate which Template user can be used to inherit the portal preferences from.
 - Favorites – Use the Favorites Profile User ID to indicate which Template user can be used to inherit the favorites and favorite scripts from.
- Once any changes are made to the Template users' portal preferences and/or favorites they will automatically apply to any attached users for these features.

5.2.3 Assigning To Do Types

Note:

To Do records can be assigned to explicit users or to a group of users. This section covers the latter condition. To Do roles must be setup prior to using this functionality.

Refer to the *Oracle Revenue Management and Billing Online Help* for more information about the To Do functionality.

The product 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.

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 define the To Do roles for a user, navigate to the To Do Roles tab of user maintenance function. This will display a screen similar to the one below:

To manage the To Do Roles to be assigned to a user the following must be performed:

- Use to add a new To Do Role
- Use to remove an existing To Do Role from the list.

The **Search** () icon can be used to find the existing To Do Role or it can be typed in.

Once the users have been attached to the To Do Roles then they can access the associated TO Do types assigned to that role or any To Do directly assigned to them.

5.2.4 Assigning User Portal Preferences

Note:

Refer to the *Oracle Revenue Management and Billing Online Help* for more information about the Portal/Zone functionality. Portals and Zones must be setup prior to using this functionality.

Portal Preferences can be inherited from other users if Template users are used. In this case the ability to set for portal preferences for users attached to a template user is disabled.

The product user interface is made up of Portals containing individual Zones. Each of the portals and zones can be associated with an application service for security purposes. Users that are attached to User Groups that are also attached to those application services can view and use the portals and zones.

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 user maintenance function. This will display a screen similar to the one below with a list of the portals the user has access to, via the user groups they are attached to:

To maintain the preferences for a specific portal expand the portal entry in the list by clicking the name of the portal or using the Expand All functionality. For example:

The following zone preferences can be set for the user:

- **Display** – Whether the zone is included or not in the portal. This allows specific zones to be displayed at startup time while other zones can be hidden and only displayed upon conditions in other zones. Refer to the *Oracle Revenue Management and Billing Online Help* for more information about the Zone Visibility.
- **Initially Collapsed** – Whether the zone is displayed collapsed on initial load. Zones are only executed when they are expanded. Marking zones as Initially Collapsed can prevent them from being executed and can speed up portal rendering times.
- **Sequence** – Defines the relative order of the zones within the portal. A value of zero (0) takes the default sequence from the portal definition.
- **Refresh Seconds** – Defines the zone auto refresh rate (this is only applicable to particular zone types). A value of zero (0) disables auto-refresh.
- **Security Access** – This is an information field that indicates whether the user has access to the zone or not². Refer to the online documentation for more information.

5.2.5 Assign Bookmarks

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.

Each user can attach bookmarks to their profile to access pages including the context of that page.

The definition of the bookmarks can be performed using the **Bookmark** button which attaches the page and context to the user profile. It is possible to view and remove bookmarks on the user profile by navigating to the **Bookmarks** tab on the User maintenance function. This will display a screen similar to the one below:

² While unlikely, it is possible to have a portal contain particular zones not permitted for access to an individual user.

The following fields can be set for the bookmarks:

- **Sequence** - Internal sequence used for sorting
- **Name** - Name of bookmark. The URL for the bookmark is hidden and not able to be edited manually.

Use  to remove an existing bookmark from the list.

5.2.6 Assign Favorite Links

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

Each individual user can set a number of favorite functions or menu items that they can access using keyboard shortcuts or via the Favorites zone on the Dashboard.

The definition of the users Favorite Links can be configured by navigating to the Favorite Links tab of user maintenance function. This will display a screen similar to the one below:



	Sequence	Navigation Option	Security Access
 	10	CI0000000919 	User Group + Yes
 	20	CI0000000841 	To Do Role + Yes

The following fields can be set for the favorites:

- **Sequence** – The relative sequence number of the favorite used for sorting purposes.
- **Navigation Option** – The Navigation option to use to display the favorite. This can reference the zone or maintenance function to display when this favorite is chosen.
- **Security Access** – This is an information field that indicates whether the user has access to the Navigation Option or not.

To manage the Favorites to be assigned to a user the following must be performed:

- Use  to add a new Favorite with the appropriate Navigation Option with the appropriate Sequence to indicate where in the favorites list the option should be placed.
- Use  to remove an existing Navigation Option from the list.

The **Search** () icon can be used to find the existing Navigation Option or it can be typed in.

Favorites are then available to be displayed in the Favorites portal on the Dashboard.

5.2.7 Assign Favorite Scripts

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

Each individual user can set a number of favorite BPA Scripts that they can access using the Favorite Scripts zone on the Dashboard.

The definition of the users Favorite Scripts can be configured by navigating to the Favorite Scripts tab of user maintenance function. This will display a screen similar to the one below:

The following fields can be set for the favorites:

- **Sequence** – The relative sequence number of the favorite used for sorting purposes.
- **Script** – The BPA Script to use to display the favorite.
- **Security Access** – This is an information field that indicates whether the user has access to the Script or not.

To manage the Favorites to be assigned to a user the following must be performed:

- Use to add a new Favorite indicating the Script with the appropriate Sequence to indicate where in the favorites list the option should be placed.
- Use to remove an existing Script from the list.

The **Search** () icon can be used to find the existing Script or it can be typed in.

Favorites are then available to be displayed in the Favorite Scripts portal on the Dashboard.

5.2.8 Assign User Characteristics

Note:

To use this facility the appropriate characteristic types must be created and attached to the user object. Refer to the *Oracle Revenue Management and Billing Online Help* for more information.

The product ships with a predefined set of characteristic types.

One of the features of the product is the ability to extend the object within the product using user defined fields called Characteristics. Characteristics act as additional data attributes that can be used to simply provide additional information or used in custom algorithms for processing.

The user object in the product can also be customized using characteristics. This can be achieved by navigating to the Characteristics tab of user maintenance function. This will display a screen similar to the one below:

	Characteristic Type	Sequence	Characteristic Value
	Database tag	10	CALLCENTER

The following fields can be set for the favorites:

- **Characteristic Type** – The characteristic type associated with the user object. This is a drop down list of the valid characteristic types associated with the object.
- **Sequence** – The relative sequence number of the characteristic used for processing purposes.
- **Characteristic Value** – This is the value of the characteristic. Depending on the configuration of the characteristic type this value may be free format, an attachment, a specific format or a specific set of values.

To manage the Characteristics to be assigned to a user the following must be performed:

- Use to add a new Characteristic indicating the Characteristic Type, the appropriate Sequence to indicate where in the favorites list the option should be placed and the value associated with the Characteristic Type.
- Use to remove an existing Characteristic from the list.

5.2.9 Defining Users to User Groups

To access the services within the product users must be connected to user groups which are in turn connected to application services. This defines the linkage for functionality that the user has access to.

The link between users and user groups has the following attributes:

- The linkage between users and users groups is subject to an expiry date to allow representation of transient security configurations.
- Each link between a user and user group is owned and subject to Data Ownership Rules. By default, all site created links are owned as Customer Modifications.
- User Groups are setup according to your site preferences. They can be job related, organization level related or a combination of factors.
- A user can be a member of any number of users groups but should be at least a member of one group to access the system.
- Users can be members of groups with overlapping permissions to application services. In the case of overlapping permissions, then the highest valid permission is used.

This can be achieved by navigating to the Main of user maintenance function. This will display a screen with zones at the bottom of the screen similar to the one below:

User Group	Expiration Date	Owner
   ALL_SERVICES  System User Group	12-31-2100	 Framework

The user groups are listed that the user has access to and can be manipulated using the following:

- Use  to add a new User Group indicating the User Group Name with the appropriate expiry date to indicate relevance of the connection. The Search icon () can be used to find the existing User Group or it can be typed in.
- Use  to remove an existing User Group from the list.
- Use  corresponding to the **Expiration Date** field to specify the date till when the user will belong to the user group.
- Use  to view the user group details.

The users security is then used for menu and function access regardless of access channel used (i.e. online, web service or batch).

5.2.10 Defining User Groups to Application Services

Note:

A starter set of User Groups are loaded with the product that can be used as the basis for further security user groups.

The product ships with all the application services predefined for base functions. These can be used or replaced with custom definitions as desired.

One of the fundamental security configurations for the product is to define the user groups to the application service. An application service can represent an individual service within the product, an individual menu or an individual object. When linking a user group to a service the access modes can be configured which defines the valid actions the user group can perform against the service.

Additionally each service can specify Security Types which allow for custom security rules to be applied at runtime. Refer to the [Security Types](#) section for more details of this facility.

To maintain the linkages between user groups and application services there are two different methods:

- Application Services Portal – When maintaining each Application Service it is possible to connect and disconnect the user groups and determine which groups have access to what functions.
- User Group Maintenance – When maintaining User Group definitions it is possible to connect Application Services to the group and manage users in that group from a single maintenance function.

Both methods are valid for most sites and can be used to manage the same information from different prospective.

5.2.10.1 Using the Application Services Portal

The Application Service portal allows administrators to define an application service, the valid access modes available for the Application Service and the user groups the application service is connected to.

To access the Application Services Portal, navigate to the **Admin Menu → A → Application Service** option. This will display a screen similar to the following:

Access Mode	Owner
Add	Framework
Change	Framework
Delete	Framework
Enable/Disable	Framework
Inquire	Framework

On the **Main** tab, the following can be configured:

- **Application Service** – The Application Service identifier. This is a service identification token used in configuration of security on the objects, menu or service etc. For custom definitions it is recommended to prefix this value with CM to avoid conflict with product provided application services.
- **Description** – This is a short description used for documentation purposes. This value is displayed on any security screen when the Application Service is specified.
- **Access Modes** – A list of valid access modes is defined and displayed for the Application Service. These modes must match the internal actions supported by the objects which this Application Service is used. When using this list:
 - Use to add a new Access mode from the drop down list of valid actions. An individual Access Mode can only be defined once for an individual Application Service.
 - Use to remove an existing Access Mode from the list.
 - The Access Mode link to the Application Service is ownership controlled. By default, all created links are owned as Customer Modifications. Refer to the [Data Ownership Rules](#) section for more details on ownership of data.

The **Application Security** tab is a portal that provides the ability to display the user group membership and manage that relationship. The portal is made up with a number of zones to provide information and maintenance capabilities:

- **Application Service Details** – This zone summarizes the access modes and security types defined for an application service. For example:

The screenshot shows the 'Application Service Details' zone. At the top, there are buttons for 'Bookmark', 'Duplicate', 'Delete', and 'Refresh'. Below that, a navigation bar has 'Main' and 'Application Security' selected. A sidebar on the left lists 'Access Mode' options: Add, Change, Delete, Enable/Disable, and Inquire. A 'Security Type' section is also present. The main content area displays the application service details: 'Application Service' CILTUSEP and 'Description' User.

- **User Groups With Access** – This zone lists the user groups that have access to the Application Service along with the associated expiry date, access modes and security types (and associated authorization level). It is possible to deny access by a particular group to the application service using the Deny Access functionality. The list can be filtered to user groups for a particular user to assist in isolating particular user groups. For example:

The screenshot shows the 'User Groups Linked' zone. At the top, there are buttons for 'Bookmark', 'Duplicate', 'Delete', and 'Refresh'. Below that, a navigation bar has 'Main' and 'Application Security' selected. A sidebar on the left lists 'Access Mode' options: Add, Change, Delete, Enable/Disable, Administrator, and Inquire. A 'Security Type' section is also present. The main content area displays a table of user groups linked to the application service CILTUSEP. The table includes columns for User Group, Description, Expiration Date, Access Mode, Security Types with Authorization, and Deny Access. The 'Deny Access' column contains five 'Deny Access' buttons, each corresponding to a user group row. A search bar at the bottom allows users to filter results by user ID, first name, and last name.

User Group	Description	Expiration Date	Access Mode	Security Types with Authorization	Deny Access
1 ALL_SERVICES	System User Group	01-01-2100	Add,Administrator,Change,Delete,Enable/Disable,Inquire		<input type="button" value="Deny Access"/>
2 C1_BSERVICES	All Services(C1- Banking Admin)	01-01-2100	Add,Administrator,Change,Delete,Inquire		<input type="button" value="Deny Access"/>
3 C1_CLSERVICES	All Services(C1- Collection Admin)	01-01-2100			<input type="button" value="Deny Access"/>
4 HCADMIN	Services for Healthcare Insurance Admin	01-01-2100	Add,Administrator,Change,Delete,Inquire		<input type="button" value="Deny Access"/>
5 INADMIN	All Services for Insurance Admin	01-01-2100	Add,Administrator,Change,Delete,Inquire		<input type="button" value="Deny Access"/>

- **User Groups Without Access** – This zone list the user groups that do not have access to the Application Service to grant access, if desired, using the Grant Access functionality. The list can be filtered to user groups for a particular user to assist in isolating particular user groups. For example:

User Group	Description	Grant Access
1 CI_RP	Report User Group	Grant Access
2 INUSER	All Services for Insurance users	Grant Access

Use to show user groups with specific user

User ID:

First Name:

Last Name:

Search

Once a group is granted access then the specification of the valid access modes and security groups can be provided for the particular user group. For example:

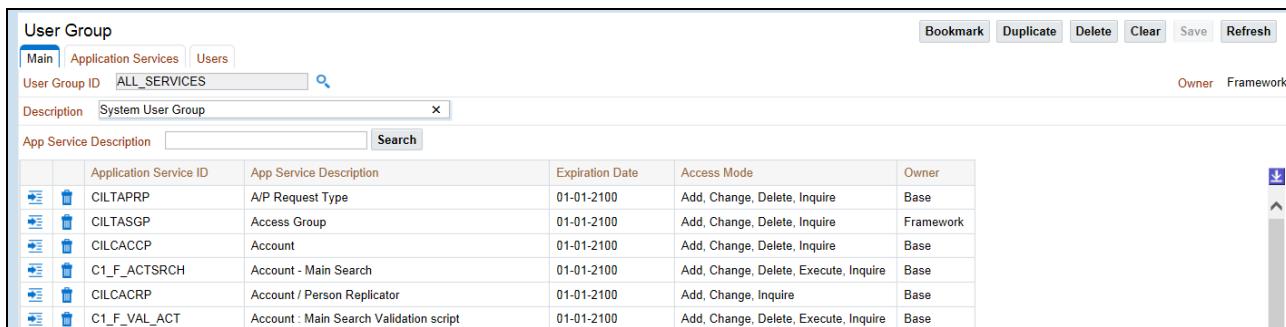
Application Service	User Group	Application Service ID	Expiration Date	Access Mode	Owner
TF_USERGRP	TF_USERGRP	CILTUSEP	<input type="text"/>	<input type="text"/>	Framework

- **Expiry Date** – Date this access will expire. Use the **Date** () icon to use the Date selection widget.
- **Access Mode** – Valid Access mode as defined on Application Service definition.
 - Use  to add a new Access Mode. The **Search** () icon can be used to find the existing Access Mode or it can be typed in.
 - Use  to remove an existing Access Mode from the list.
- **Owner** – Ownership of link (refer to the [Data Ownership Rules](#) section)

- **Security Type** – Security Type code associated with Application Service.
 - Use  to add a new Security Type. The **Search** () icon can be used to find the existing Security Type or it can be typed in.
 - Use  to remove an existing Security Type from the list.
- **Authorization Level** – The Authorization Level assigned to this User Group when executing this Application Service for the Security Type. The **Search** () icon can be used to find the existing Authorization Level or it can be typed in.

5.2.10.2 Using User Group Maintenance

When editing an individual user group it is possible to define the accessible application services and connect users to the user group from the user group maintenance function. To do this, navigate to the **Admin Menu → U → User Group** menu option. This will display a screen similar to the following:



The screenshot shows a table with the following data:

	Application Service ID	App Service Description	Expiration Date	Access Mode	Owner
	CILTAPRP	A/PI Request Type	01-01-2100	Add, Change, Delete, Inquire	Base
	CILTASGP	Access Group	01-01-2100	Add, Change, Delete, Inquire	Framework
	CILCACCP	Account	01-01-2100	Add, Change, Delete, Inquire	Base
	C1_F_ACTSRCH	Account - Main Search	01-01-2100	Add, Change, Delete, Execute, Inquire	Base
	CILCACRP	Account / Person Replicator	01-01-2100	Add, Change, Inquire	Base
	C1_F_VAL_ACT	Account : Main Search Validation script	01-01-2100	Add, Change, Delete, Execute, Inquire	Base

The services that this user group has access to are shown with the associated expiry date and access modes for the user group. The following actions maintain the information:

- Use  to edit an existing permission.
- Use  to remove an associate between a user group and an application service.
- Use  on the Application Services tab to add a new association between an application service and an individual user group. For example:

When editing an existing association or adding a new association the Application Services tab is displayed to maintain the association with associated Access Modes and Security Types. For example:

Access Mode	Owner
A	Framework
C	Framework
D	Framework
R	Framework

As with the Application Service Portal, it is possible to define the following from this screen:

- **Expiry Date** – Date this access will expire. Use the **Date** () icon to use the Date selection widget.
- **Access Mode** – Valid Access mode as defined on Application Service definition.
 - Use  to add a new Access Mode. The **Search** () icon can be used to find the existing Access Mode or it can be typed in.
 - Use  to remove an existing Access Mode from the list.
- **Owner** – Ownership of link (refer to the [Data Ownership Rules](#))
- **Security Type** – Security Type code associated with Application Service.
 - Use  to add a new Security Type. The **Search** () icon can be used to find the existing Security Type or it can be typed in.
 - Use  to remove an existing Security Type from the list.
- **Authorization Level** – The Authorization Level assigned to this User Group when executing this Application Service for the Security Type. The **Search** () icon can be used to find the existing Authorization Level or it can be typed in.

Additional from the User Group maintenance screen it is possible to manage the users associated with this user group. The Users tab is used to define this information. For example:

User	Expiration Date	Owner
SYSUSER	System, English	Framework

The screen allows users to be associated with the user group with the following information:

- **User** – This is the authorization user identifier to be connected to the user group. The **Search** () icon can be used to find the existing User or they can be typed in
- **Expiration Date** – Date the association between the user and user group will expire. Use the **Date** () icon to use the Date selection widget.
- **Owner** - Ownership of link (refer to the [Data Ownership Rules](#)).

Use  to add a new User or use  to remove an individual user from the list.

5.2.11 Define Users to Data Access Groups

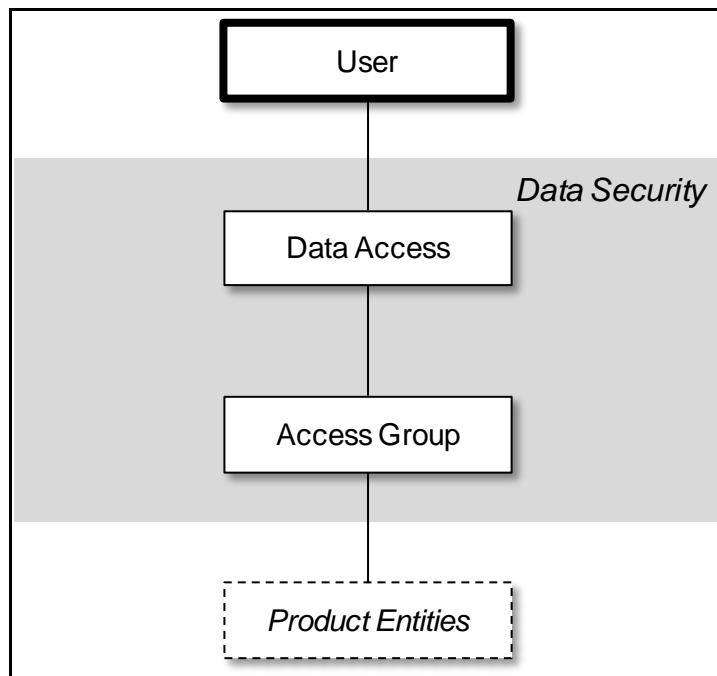
Note: Not all products support Data Access Roles and Data Access Groups. Refer to the *Oracle Revenue Management and Billing Online Help* for more information.

Data Access Groups are used to define the subset of data objects the user is permitted to access. There are two levels to the definition of data access:

- **Data Access Roles** – User are connected to Data Access Roles which defines the groups of data permissions the user has access to. Data Access Roles are connected to Data Access Groups (a.k.a. Access Groups).
- **Data Access Groups** – Data Access Groups are tags that are attached to entities in the product to implement data security³. Data Access Groups are maintained using Access Group maintenance. Refer to the *Oracle Revenue Management and Billing Online Help* for more information about this facility.

³ Attaching a Data Access Group to a product entity it does not automatically implement data security. Queries for that object must be altered to take into account the Data Access Group. Refer to the Oracle Utilities SDK for more details.

The relationships between these objects are illustrated in the figure below:



To maintain the Data Access Roles and Access Groups a user has access to navigate to the Access Security tab of the user maintenance function. This will display a screen similar to the following:

Data Access Role				Expiration Date
			***	System Default 01-01-2100

User SYSUSER - System, English

The above Data Access Roles provide the User with the rights to 1 Access Group(s.).

Access Group *** - System Default

Data access is provided by the role Data Access Role *** - System Default

The screen will allow the definition and display of the following information:

- **Default Access Group** – When this user creates a new object that is subject to Access Security then this default is used for the value of the Access Group of the new object. This can be overridden by logic within the object if necessary.
- **Data Access Role** – List of Data Access Roles this user is attached to. The **Search** () icon can be used to find the existing Data Access Role or they can be typed in.
- **Expiration Date** - Date the association between the user and data access role will expire. Use the **Date** () icon to use the Date selection widget.

Use  to add a new Data Access Role or use  to remove a Data Access Role from the list.

5.2.12 User Enable and Disable

One feature of security is that the user record is attached to some objects for audit purposes (some objects are automatic, such as financials, and some are configurable). When a user does any work in the product and the user has been attached to some audit object across the whole product, the user cannot be deleted. This is due to auditing requirements.

There is a feature on the user object to enable or disable a user by setting the appropriate value for User Enable on the User object. This has the following implications:

User Enable	Implications
Enable	<ul style="list-style-type: none"> • User can access system. • User can process records according to the authentication model. • User must be active in Security repository to fully access the product.
Disable	<ul style="list-style-type: none"> • User cannot access the system regardless of other security setup • User record is retained for audit purposes only. • User does not have to exist in the Security Repository.

This facility has a number of key use cases:

- **Support for Personnel (Permanent or Temporary) Leaving** – It is possible to manually disable users once they leave the organization.
- **Logical Deletion** – If you want to delete a user due to any reason, then you need to disable the user.
- **Temporary Disablement** – If business rules need to isolate users then setting the User Enable for appropriate users can effectively disable them from the product.

Note: When a user is disabled, it will apply when the user next attempts to login or when the security cache is refreshed.

5.3 Managing Batch Users

Each time a batch process is executed the security components of the product must authenticate the user against a security repository and authorize the user to access the components the batch process needs to complete its operations.

The batch component of the architecture uses a number of security mechanisms:

- **Authorization** – Any batch users must be defined to the operating system configured security repository and be a member of the operating system group assigned to the product.

Note: The user ID used does not have to match the authorization user used within the product.

- **Authorization** – The authorization user is defined within the product as per the online users and is specified as a job parameter at execution time or in configuration files supplied for the batch process. Refer to *Oracle Revenue Management and Billing Server Administration Guide* for more information about the parameters used for batch processing.

To manage batch user therefore the following is recommended:

- Add the authentication user used to initiate the threadpool and submitter processes for a batch process to the configured operating system repository.
- Specify a valid user authorization identifier as a parameter for the batch process. This identifier must be authorized to the valid actions against the main objects used in the batch process. Refer to the product functional documentation on the objects used in each of the product batch processes.

5.4 Managing Web Services Users

Note: Native Security support is only supported for XAI Inbound Services using the BusinessAdapter Adapter.

From a product perspective a Web Service is a channel into the objects within the product. Any of the objects, services and scripts available in the product can be exposed as JAX-WS 2.0 based Web Service. From a security perspective Web Services uses the following security mechanisms:

- **Authentication** – The Web Services component of the product uses the Web Services support native to the JEE Web Application Server. This allows security tokens supporting many standards to be used to authentication individual web service calls.
- **Authorization** – The Web Services component uses the same authorization model as the online user and batch components use.

Note: The user for authentication is used to map to the authorization user within the user object in the same way that online users are mapped.

To manage Web Services security users the following is recommended:

- Users for authentication are added to the security repository configured with the JEE Web Application Server. This should match the Login ID used for the authorization model.

- Security Policies need to be attached to Web Services using the JEE Web Application Server. For Oracle WebLogic the security policies available using Oracle Web Services Manager is available for use with individual Web Services. Multiple policies are supported. Refer to the *Oracle Fusion Middleware Security and Administrator's Guide* for Web Services for more information and the policies available.
- Users must be defined to the authorization model with appropriate access to underlying services used by the Web Service. For Web Services based upon Business Objects, Business Services and Scripts, users need appropriate access to the Application Service defined on these objects.
- Transaction Types in the Web Services translate to Access Modes within the Application Service calls.

For more information about Web Services, refer to the *XAI Best Practices* (Doc ID: 942074.1).

5.5 Authentication User

In the user object there are two different user identifiers namely User ID and Login ID. The different identifiers have differing roles:

- The user ID, which is up to 8 characters in length, is used internally for authorization and is passed to the database connection as the `CLIENT_IDENTIFIER` on the database connection. 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 Login ID, which is up to 256 characters in length, is used for authentication to the security repository configured on JEE Web Application container. The Login ID can match the User ID but can differ to reflect site standards. Unlike the user ID, the Login ID can be changed at anytime to reflect changes in the organization such as name changes or acquisition.

Note: The Login ID must match, in the same case, as the entry in the configured security repository for the JEE Web Application Server.

When maintaining a user, it is important that the Login ID is only changed using the maintenance function, LDAP Import or any XAI/Inbound Web Service based upon the USER object and not directly using other means (such as direct SQL) as a Security Hash is generated at maintenance time and is checked at login time. At application login time, if the security hash does not match the user is deemed not authorized and will be refused access to the product. To ensure security hashes are correct use the Synchronize Data Encryption function to reset the user security hash.

6. Advanced Security

6.1 About Advanced Security

While the default security settings are adequate for most sites, there are a number of 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.

6.2 JEE Authentication Group

The default installation of the product includes a default authentication group (role-name) defined within the JEE Web Application web descriptor (web.xml). This role name is used by the JEE Web Application to link the authorized users within the product to the associated JEE physical resources (i.e. pages, configuration files) within the JEE Web Application Server. The specification of the group in the web descriptor is in the security section⁴. For example:

```
<security-role>
  <description>OUAF Users</description>
  <role-name>cisusers</role-name>
</security-role>
```

By default, this group is set to cisusers, which is configurable for each web component. When the product is deployed to the JEE Web Application Server, this group is instantiated ready to be allocated to individual users. Users of the product must be attached to this group to use the product.

From a configuration point of view there are a number of options for this setting:

- The default group may be changed at installation and configuration time using the configuration settings as shown below as outlined in the *Oracle Revenue Management and Billing Server Administration Guide*. The group name should have no embedded blanks.

Component	Principal Name	Role Name
Online/Help	WEB_PRINCIPAL_NAME	WEB_ROLE_NAME
AppViewer	WEB_APPVIEWER_PRINCIPAL_NAME	WEB_APPVIEWER_ROLE_NAME

- If the JEE Web Application Server is configured to use an external security repository the configured administration group must exist in the security repository and the users must be connected to this group.

Note: If the JEE administration group is changed after installation time, users will need to be migrated to the new JEE administrations group either manually, using tools provided with the security repository or JEE Web Application Server.

⁴ The security role is used in a number of sections of the web application descriptor.

6.3 Logon Configuration

The default configuration for online authentication is using a logon screen for the online product, online help and online AppViewer applications. The product supplies a prebuilt logon screen for all three components preconfigured.

At logon it detects that a user has not logged on before (the presence of a JSESSIONID cryptographically-secure session cookie issued by the Web Application Server is used). Depending on the configuration (in the web.xml) of the applications, housed in the JEE Web Application Server, the following is performed:

- **FORM** – This is the default setting to support a logon screen with an associated error screen in case of unsuccessful logon. The product provides a prebuilt logon screen but can be replaced with custom logon screens⁵ by setting the following configuration settings appropriately for each web component as outlined in the *Oracle Revenue Management and Billing Server Administration Guide*:

Component	Login Screen	Login Error Screen
Online	WEB_FORM_LOGIN_PAGE	WEB_FORM_LOGIN_ERROR_PAGE
Help	WEB_HELP_FORM_LOGIN_PAGE	WEB_HELP_FORM_LOGIN_ERROR_PAGE
AppViewer	WEB_APPVIEWER_FORM_LOGIN_PAGE	WEB_APPVIEWER_FORM_LOGIN_ERROR_PAGE

- **BASIC** – The browser will issue a call to the operating system to display the default logon dialog supplied with the operating system. No logon dialog is supplied.
- **CLIENT-CERT⁶** - This is an advanced configuration to allow for certificated (one way or two way) to be used. Refer to the documentation supplied with the JEE Web Application Server for more details of the additional configuration required.

6.4 Data Ownership Rules

On each of the objects (and on selected child objects) an owner flag is included to determine the origin of the data. The owner is used by the product to determine the maintenance owner of key data as well as protect important data shipped with the product from accidental deletion.

The value of the flag is displayed on maintenance screens to visually indicate the data owner. The location of the information varies from the top left of maintenance pages, within lists of information (to apply to individual rows) and within sections of maintenance pages.

The flag has a number of valid values:

- **Base** – This is important information shipped with the product and cannot be deleted or modified using the delete or medication functions, respectively, regardless of user permissions. This is reserved for use by the product to ship key important information and to protect that information. Deletion of this information directly from a product database will result in unexpected results.

⁵ Custom logon screens should be placed in the cm directory of the web application server as outlined in the Oracle Utilities SDK.

⁶ **CLIENT-CERT** is supported but requires manual changes to configuration files. Refer to the Server Administration Guide on implementing custom templates.

- **Product Name** – The product name that owns the data is displayed. This is similar to the Base data ownership value but indicates which component the data is applicable to. All the rules that apply with the Base data ownership value apply to this value.
- **Customer Modification** – This indicates that the data was added by the implementation using the various methods and is owned by the implementation. Deletion of data is permitted using the valid deletion functions for authorized users.

In general sites, can only maintain Customer Modification owned records. Other ownership values are reserved to protect product installation supplied data.

6.5 Configuring JMX Security

The operations interface to the product is based upon Java Management Extensions (JMX) allowing components of the product to be managed and monitored from JSR160 compliant consoles including jconsole or Oracle Enterprise Manager.

Refer to the *Oracle Revenue Management and Billing Server Administration Guide* for more details of the JMX operations interface.

By default the JMX implementation and configuration uses the default simple file based security as outlined in the JMX specification.

6.5.1 Default Simple File Based Security

The default configuration is based upon a properties file containing name/value pairs corresponding to role/password pairs and authorization can be also based on a properties file containing name/value pairs corresponding to role/access pairs where access can be any of readonly access which grants read access to any remote operation and readwrite access which grants access to read and update operations in the interface.

Note: By default the user (BSN_JMX_SYSUSER) and password (BSN_JMX_SYSPASS) for the administrator are automatically added to the configuration files.

To use this facility the following file should be maintained using an appropriate editor (located in \$SPLBASE/scripts directory or %SPLBASE%\scripts in Windows):

- ouaf.jmx.access.file – This file contains the user ID and access permissions in the format separated by a blank space:

Field	Comments
User ID	Authentication user to access JMX.
Permission	Permission assigned to user. Valid values are: readonly – No update access and readwrite – Update access and can access update operations

- `ouaf.jmx.password.file` - This file contains the user ID and password in the format separated by a blank space:

Field	Comments
User ID	Authentication user to access JMX
Password	Password in plain text or encrypted format.

Note: These files are also tailored using custom templates. The `ouaf.jmx.access.file.template` and `ouaf.jmx.password.file.template` are used for the configuration.

6.5.2 SSL based Security

Note: For a full description of SSL setup refer to the **To Setup SSL** section of [Monitoring and Management Using JMX Technology](#).

To secure communications for JMX using the Java SSL support the following process needs to be performed:

- Security has to be setup using the [Default Simple File Based Security](#) or [Using Other Security Sources](#).
- A key pair and certificate need to be setup on your server. Refer to the [Monitoring and Management Using JMX Technology](#) or JEE Web Application Server Administration documentation for details and utilities available for this process.
- Set additional java parameters using the `WEB_ADDITIONAL_OPT` for the online/Web Services and `BATCH_MEMORY_ADDITIONAL_OPT` for Batch. Refer to the *Oracle Revenue Management and Billing Server Administration Guide* for details of these parameters. The following additional system properties must be set:

System Property	Comments
<code>javax.net.ssl.keyStore</code>	Keystore location
<code>javax.net.ssl.keyStoreType</code>	Default keystore type
<code>javax.net.ssl.keyStorePassword</code>	Default keystore password
<code>javax.net.ssl.trustStore</code>	Truststore location
<code>javax.net.ssl.trustStoreType</code>	Default truststore type
<code>javax.net.ssl.trustStorePassword</code>	Default truststore password
<code>com.sun.management.jmxremote.ssl</code>	Set to true
<code>com.sun.management.jmxremote.registry.ssl</code>	Set to true
<code>com.sun.management.jmxremote.ssl.need.client.auth</code>	Set to true

Note:

Additional options are also supported as documented in [Monitoring and Management Using JMX Technology](#).

Specification of system properties for java is as per the [java command line](#).

For sites using Oracle WebLogic in native mode, configuration of SSL requires configuring Oracle WebLogic to use SSL and altering the startup scripts for Oracle WebLogic to include the above options.

6.5.3 Using Other Security Sources

Whilst, by default, the file based repository is supported it is possible to configure the authentication of JMX to use an alternative data source such as an LDAP Server. This involves changing the JAAS configuration stored in the `java.login.config` file `$SPLBASE/splapp/config` directory (or `%SPLBASE%\splapp\config` directory on Windows).

In the JAAS configuration file there is a default `jmxrealm` that contains the default JMX LoginModule. This can be changed, using custom templates, to support an alternative source for authentication. Refer to the [LdapLoginModule](#) for information and examples of login configurations.

Note: To implement the custom security source custom templates for `java.login.config` must be implemented according to the process outlined in the *Oracle Revenue Management and Billing Server Administration Guide*. This configuration affects all modes of access (i.e. online, Web Services and Batch).

6.6 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. Whilst this behavior is sufficient 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 wish 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 on the Menu Items tab of the **Administration → M → Menu** option. For example:

Menu

Main Menu Items

Menu Name: CI_TODO
Menu Line ID: CI00000057

Owner: Framework

Menu Line Items 1 of 2 + Delete

Menu Item ID	CI00000350	Owner	Framework
Sub-menu Name	<input type="text" value=""/>	Search	
Sequence	<input type="text" value="1"/>		
Navigation Option	<input type="text" value="CI0000000193"/>	Search	To Do Entry
Image GIF Location and Name	<input type="text"/>		
Image Height	<input type="text" value="0"/>	Image Width	<input type="text" value="0"/>
Balloon Description	<input type="text"/>		
Long Label	<input type="text" value="To Do Entry"/>		
Override Label	<input type="text"/>		
Application Service	<input type="text" value=""/>	Search	
Access Mode	<input type="text"/>		

6.7 Security Types

By default users have full access to the objects via the access methods specified in their user groups. If the implementation wishes to implement additional levels or rules then the application service must use Service Types. The definition of a Service Type 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.

Security Type

Main MASKING

Security Type: MASKING

Description: Data Masking

Authorization Level	Description
+ Delete 1	Unmasked Data
+ Delete 2	Masked Data

Application Service ID: CMMASKING Search Data Masking

To define Security Types, **Administration → S → Security Types** option to display the Security Types maintenance function. For example:

On this function define the following in relation to the Security Type:

- Security Type – Identifier for Security Code
- Description – A short description of the use of the Security Code.

- Authorization Levels – A list of codes (Authorization Level) and associated descriptions. Use  to add a new Authorization Level or use  to remove an existing Authorization Level from the list. The Authorization Level values are free format but should be representative of the desired function. The Description is used to explain the value.
- Application Service Id – A list of associated Application Services to use this Security Code. Use  to add a new Application Service or use  to remove an existing Application Service from the list. The **Search** () icon can be used to find the existing Application Server or it can be typed in.

Note: To fully implement the rules associated with the security types, code must be included in objects to implement security logic.

6.8 Default Generic Application Services

By default all a set 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 the product to provide a mechanism for defining new zones, new objects or new menu items for rapid deployment.

There are two generic Application Services that can be used to secure objects, zones and menu items:

- F1-DFLTAPS – This is a generic execution Application Service which is designed to secure zones and menu options. It only supports the Execute Access Method.
- F1-DFLTS – This is a generic maintenance Application Service which is designed to secure business objects. It supports the Add, Modify, Delete and Inquire Access Methods.

Use of these generic Application Services is optional.

6.9 Administration Delegation

By default, the product provides a single administration account, as configured in the SPLADMIN configuration setting, in the ENVIRON.INI configuration file, to manage the operational aspects of the product. This operating system user is the owner of the product when it is installed and is typically used for all operational aspects of the product.

Note: It is not possible to change the product administration account after installation. If this is desired it is recommended to remove the product and reinstall using the alternative administration account.

Whilst the single administration account is sufficient for most needs it is possible to provide additional administration accounts to delegate administration tasks. To delegate administration, the following must be configured:

- Any administration user must be a member of the operating system group allocated to the product as outlined in the `SPLADMINGROUP` configuration setting in the `ENVIRON.INI` configuration file.
- If you are using Oracle WebLogic in embedded mode and using the `sp1` utility to manage the startup and shutdown of the product then the utility permissions must be altered to set the sticky bit⁷, using the `chmod +t` or `chmod +s` command, so that the utility must run as the product administration account.

Note: Permissions on the directories are set to restrict the administration functions. Do not alter the permissions on individual directories and file unless otherwise directed.

- If you are using Oracle WebLogic in native mode, then the console will execute the native facilities to start and stop the product. It is recommended that the user allocated to Oracle WebLogic at installation time be a member of the operating system group outlined in `SPLADMINGROUP` configuration setting in the `ENVIRON.INI` configuration file.

Note: Customers using Oracle Enterprise Manager, with or without Application Management packs, should use the administration delegation and credential management capabilities of that product to manage administration delegations.

6.10 Secure Communications (SSL)

By default, the product uses HTTPS for communication to the browser and across the tiers. The transport protocol can be encrypted using SSL/TLS to secure transmission of data across networks.

Note: Oracle strongly recommends that customers use SSL to secure transmission for production environments.

To implement SSL the following process must be completed:

- Configure the JEE Web Application Server to use the SSL protocol. For Oracle WebLogic customers refer to [Configuring SSL](#) in [Oracle Fusion Middleware Securing Oracle WebLogic Server](#).
- Set the SSL Port Number using the `WEB_WLSSLPORT` configuration parameter as outlined in the *Oracle Revenue Management and Billing Server Administration Guide*.
- Once the setup has been tested and verified refer to the documentation on disabling insecure protocols.

6.11 Data Masking Support

By default, the data in the product is unmasked for authorized users. If particular data within the object is considered a candidate for data masking then the masking capabilities with the product can be used to mask the data in an appropriate fashion.

⁷ Support for sticky bit varies from operating system to operating system

Note: The data is not stored in masked fashion; it is configured to be displayed in masked format for particular users using the [Security Types](#).

To mask data using the internal data masking capability:

- An internal algorithm type of F1-MASK is supplied with the product to perform basic data masking. For example:

Sequence	Parameter	Required	Owner
1	Masking Character	<input type="checkbox"/>	Framework
2	Number Of Unmasked Characters	<input type="checkbox"/>	Framework
3	Unmasked Characters	<input type="checkbox"/>	Framework
4	Application Service	<input type="checkbox"/>	Framework
5	Security Type	<input type="checkbox"/>	Framework
6	Authorization Level	<input type="checkbox"/>	Framework

- The following parameters are applicable to the algorithm:
 - **Masking Character** – The character to be used as a mask. By default the * character is used.
 - **Number of Unmasked Characters** – 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** – A list of characters, with no spaces, to leave unmasked. Commonly, this is used to denote delimiter characters to enhance recognition.
 - **Application Service** – [Application Service](#) used for security authorization checking. This allows global (or local) services to be configured to indicate security access to data masks.
 - **Security Type** – The [Security Type](#) used to flag which users will view the data in masked or unmasked format. User groups need to be connected to the Application Service, Security Type and given the Authorization Level to determine the level of data masking.
 - **Authorization Level** – The authorization level used to determine if a user has access to the data unmasked. All other authorization levels in the security type indicate masked data.

- Configure an Algorithm entry of Algorithm Type F1-MASK for the desired masking configuration. Algorithm entries can be shared across fields to be masked using the **Administration** → **A** → **Algorithm** option. For example:

Parameter	Sequence	Value
Unmasked Characters	3	
Application Service	4	CMMASKING
Security Type	5	MASKING

- Attach user groups to the Application Service with the appropriate Authorization Level for the Security Type.

- Create or update a Feature Configuration of Feature Type Data Masking using the **Administration → F → Feature Configuration** option. For example:

	Option Type	Sequence	Value	Detailed Description
	Field Masking	1		<p>field="field_name", alg="algorithm name"</p> <p>A "where" clause may also be specified. For example</p> <p>field="PER_ID_NBR", alg="algorithm name" where="ID_TYPE_CD=SSN"</p> <p>- For data that is accessed via a page maintenance service call, indicate the table name and the field name where the data resides, for example</p> <p>table="table_name", field="fld_name", alg="algorithm name"</p> <p>A "where" clause may also be specified. For example</p> <p>table="CI_PER_ID", field="PER_ID_NBR", alg="algorithm name", where="ID_TYPE_CD=SSN"</p> <p>- For data that is stored as a characteristic,</p>

- For each field to mask add an entry to the Options section of the Feature Configuration with the following values:
 - **Option Type** – Select Field Masking for Data Masking.
 - **Sequence** – Specify a sequence number for order of evaluation.
 - **Value** – Specify the tag string, delimited by ',', to indicate the definition of the data masking with the following tags depending on how the data is accessed:
 - Only fields defined as strings are supported by the supplied algorithm.
 - To reference the masking algorithm, enter alg="algorithm name". The algorithm's algorithm type must reference the Data Masking algorithm entity.
 - For data that is accessed via a schema-based object call, the field to be masked must reference a meta-data field name in its schema definition. For example, if you want to mask a credit card number, let's assume that field is defined in the schema is <creditCard mdField="CCNBR" mapField="EXT_ACCT_ID"/>. In this case, the option value should be field="CCNBR", alg="algorithm name".
 - For data that is accessed via a page maintenance service call, indicate the table name and the field name where the data resides, for example table="table_name", field="fld_name", alg="algorithm name".

- A WHERE clause may also be specified. This is useful for data that resides in a child table where only data 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 that is stored as a characteristic, simply indicate the characteristic type 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 on

Note: Only ad-hoc characteristics are supported at the present time.

- For data that is 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="ID_TYPE_CD='SSN'", alg="algorithm name". To find the name of the search service, launch the search in question, right click in the filter area and choose View Source. Search for ServiceName. The service name is listed there. To find the field name to mask, go back to the search window and right click on the results area and choose View Source. Look for the Widget Info section and find the field name in the SEARCH RESULTS (do not include the \$).

Note: The WHERE statement can only apply to fields that are also part of the search results.

- Use  to add a new Data Masking definition or use  to remove an existing Data Masking definition from the list.

6.12 Securing Files

Note: The utilities mentioned in this section apply to Linux and UNIX environments only.

The product file structure is protected by permissions set at the operating system level. By default, the settings provided with the product upon installation comply with Oracle standards in respect to permissions. For more details of the individual user permissions on product directories and subdirectories, refer to the *Oracle Revenue Management and Billing Server Administration Guide*.

If at any time, the permission are manually altered and need to be reset to the defaults then the following process can be used:

- Execute the `splenviron.sh` utility to set the environment variables for the product environment to reset. Refer to the *Oracle Revenue Management and Billing Server Administration Guide* for details of this process.
- Execute the `setpermissions.sh` utility to reset the environment permissions back to the defaults.

The environment permissions will be reset to the defaults supplied with the product.

6.13 Password Management

On a regular basis passwords are changed to maintain security rules. The product uses a number of passwords that may require changing on a regular basis. The following table lists all the passwords used in the product and guidelines for changing the password values used by the product.

Password Owner	Location	Comments
Online User	JEE Authentication Source	No configuration changes. User changes password in security repository directly or indirectly using security products. Security repository is configured in JEE Web Application Server ⁸ .
Web Service User	JEE Authentication Source	No configuration changes. User changes password in security repository directly or indirectly using security products. Security repository is configured in JEE Web Application Server.
Batch User	Operating System	No configuration changes. User changes password in security repository directly or indirectly using security products. Security repository is configured in operating system.
Database Users	BATCH_DBPASS DBPASS XAI_DBPASS	The database users are stored in ENVIRON.INI. Refer to the <i>Oracle Revenue Management and Billing Server Administration Guide</i> on process to change values. New Passwords need to be re-encrypted.
JMX Users	BSN_JMX_SYSPASS	The default JMX user is stored in ENVIRON.INI. Refer to the <i>Oracle Revenue Management and Billing Server Administration Guide</i> on process to change values. New Passwords need to be re-encrypted.
JEE Administration Account	WLS_WEB_WLSYSPASS WEB_WLSYSPASS	The default administration users are stored in ENVIRON.INI. Refer to the <i>Oracle Revenue Management and Billing Server Administration Guide</i> on process to change values. New Passwords need to be re-encrypted.

⁸ WEB_SPLPASS specifies the default password for the initial user. If this user is used past the installation the password may need to be changed. Refer to the Server Administration Guide for more details.

6.14 Securing Online Debug Mode

The product features an online debug mode which is used for problem solving and development personnel to trace their code or diagnose problems. As with other functions within the product the debug function is security controlled.

To use this facility any of the user groups an individual user must include Inquire access to the F1DEBUG application service. This will enable the debug facility from the URL.

For more information about the Debug facility refer to the *Oracle Revenue Management and Billing Server Administration Guide*.

6.15 Securing Online Cache Management

The product features an online cache management facility which is used to reset the online cache to force new values to be loaded. As with other functions within the product the cache management function is security controlled.

To use this facility any of the user groups an individual user must include Change access to the F1ADMIN application service. This will enable the cache management facility from the URL.

For more information about the cache management facility refer to the *Oracle Revenue Management and Billing Server Administration Guide*.

6.16 Web Services Security

Note:

This section outlines the Inbound Web Services security facility only.

Refer to *Migrating from XAI to IWS (Doc ID: 1644914.1)* for more information.

Inbound Web Services allow external web service based integrations to access functionality within the product. The security settings for the Inbound Web Services can be summarized as follows:

- Inbound Web Services rely on Web Services standards supported by the JEE Web Application Server for authentication support.
- Inbound Web Services support the WS-Policy standards supported by the JEE Web Application Server to provide both transport and message security. Refer to the Oracle WebLogic documentation for details on the WS-Policies supported. The following rules apply to those policies:
 - Oracle WebLogic policies are supported if the corresponding setup is performed within Oracle WebLogic. For example, encryption is supported if keystores are configured for encryption keys.
 - WS-Policies are attached within the Oracle WebLogic console or Oracle Fusion Middleware Control after deployment. These policies are maintained independently.
 - Element Level policies are not supported at present.
 - Security policies at the operation level are not supported directly but are supported via authorization.
 - The product ships an internal policy for backward compatibility (UserToken).

- Inbound Web Services use the underlying business objects, maintenance objects, business services and service scripts to determine authorization of records. This includes authorization for specific operations.
- Inbound Web Services can use Oracle Web Service Manager for additional WS-Policy support and web service access controls.
- Security policies can vary between individual Inbound Web Services.
- Multiple WS-Policies are supported per Web Service. The clients calling these services must conform to at least one of the policies attached.

By default, the WS-Client calling the product must supply an authentication token in the format configured on the WS-Policy on individual web service. By default, there is no default user on Inbound Web Services transactions. A default user may be configured on the ouaf.ws.defaultUser setting in the spl.properties file for the Inbound Web Services. Refer to *Oracle Revenue Management and Billing Server Administration Guide* for details of the process.

Note: Setting of a default user is not recommended for implementations unless backward compatibility is required for older XML Application Interface based services.

For backward compatibility, there are number of additional settings that cover Inbound Web Services:

Setting	Comments
ouaf.ws.defaultUser	Default user for authorization of Web Services calls
ouaf.ws.superusers	Delimited set of effective users used to translate calls from authentication users not known to the system.
ouaf.ws.deploy.user	Administration user used for deployment activities. This setting is only specified if differs from the administration settings.

6.17 Message Driven Bean Security

Note:

Refer to the *Oracle WebLogic JMS Documentation* for detailed information about JMS facilities provided.

Refer to the *Oracle WebLogic JMS Integration (Doc ID: 1308181.1)* whitepaper for details of the JMS integration implementation.

The Message Driven Bean (MDB) within the Inbound Web Services implementation allows JMS resources (such as JMS Queues or JMS Topics) to be read using the MDB and sent to an Inbound Web Service to be processed.

By default, the Message Driven Bean uses the JMS (JMSX) header fields for authentication and authorization purposes such as JMSX User ID.

If the JMS message security is not used, then a default user can be set in the ouaf.ws.defaultUser parameter in the spl.properties file.

6.18 SOAP Security

In this release, additional SOAP Header security, for outbound communications, has been added to support additional facilities in Service Oriented Architecture integrations and Oracle Web Services Manager. The following additional facilities are now supported in the SOAP Header:

- SOAP Insert Time Stamp - A set of timestamps can be added to the transaction to support WS-Security to avoid replay attacks.
- Additional SOAP Security inbuilt - The SOAP Header can now have inbuilt support for TEXT and DIGEST headers in addition to the BASIC support provided in past releases. This feature can be replaced using Oracle Web Services Manager with WS-Policy support for other advanced security configurations.
- SOAP Expiration Delay - It is possible to set a transaction expiration, in seconds, to control resource usage of the transaction.

Note: The only HTTP/HTTPS method supported is POST in this release.

Refer to the online documentation for a more detailed description of these settings.

6.19 Groovy Support

The product now supports Groovy for extensions, via the script engine. This support was added to augment the Java and Scripting support to offer an alternative. The implementation of Groovy has some limitations for security reasons:

- Groovy API's that have direct access to operating system functions have been blacklisted for security reasons and therefore cannot be used. Alternative functions are provided to provide safe access to selected operating system functions.
- It is possible to implement a custom whitelist for non-cloud implementations. Refer to the Server Administration Guide for more information.

Refer to the online documentation for more details of Groovy support.

7. Audit Facilities

The product has an inbuilt auditing capability to register accesses to data from online and Web Services users. Batch processing is not audited by default but can be enabled using the Oracle Utilities SDK using programmatic methods.

7.1 About Audit

Auditing allows for the configurable tracking of changes to key data by online and Web Services users. The product has an inbuilt, configurable audit facility that tracks changes and allows authorized users to track changes on an individual user and change basis.

The use of the inbuilt audit facility is optional and can be enabled or disabled at any time.

7.2 Audit Configuration

Note: This section covers the soft table implementation of Auditing. There is also specialist Audit algorithm support on Business Objects and Maintenance Objects to add information to log entries attached to these objects. Refer to the Oracle Utilities SDK and online Administration documentation for a description of programmatic implementation of Auditing.

The inbuilt Audit facility is configured at a table level. For each table you wish to enable audit upon the following needs to be configured:

- **Audit Table** – To store the audit information a database table must be configured to hold the audit information. By default, the CI_AUDIT table can be used for this purpose. If a custom table is used to store the information it should have the same structure as CI_AUDIT for compatibility purposes.
- **Audit Program** – To process the audit information a class or program must be configured to record the audit information. By default a number of prebuilt Audit programs are available for use:
 - com.splwg.base.domain.common.audit.DefaultTableAuditor – This is the default java based audit class provided by the product. It audits any changes to any fields configured to track auditing information.
 - com.splwg.base.domain.common.audit.ModifiedTableAuditor – This is an alternative to the DefaultTableAuditor but it will not audit inserts or deletes of empty string field data. For example, changes from null values to empty spaces and vice versa would not be logged.

Note: It is possible to implement custom Audit handlers using the base classes as parent classes. Refer to the Oracle Utilities SDK documentation on how to extend the product.

- **Audit Conditions** – A set of switches are configurable on each field you wish to include in auditing to determine the conditions of auditing. At least one of these switches must be enabled for auditing to be registered:
 - **Audit Delete Switch** – Enable this switch to audit delete operations against this field.
 - **Audit Insert Switch** – Enable this switch to audit insert operations against this field.
 - **Audit Update Switch** – Enable this switch to audit update operations against this field.

To maintain the audit information, navigate to the **Administration → T → Table** option and specify the table to enable auditing against. For example:

The screenshot shows the 'Table' configuration screen. The 'Audit Table' field is highlighted with a red box. Below the table, a grid of fields shows audit switch checkboxes for 'Audit Delete Switch', 'Audit Insert Switch', and 'Audit Update Switch' for each field.

Specify the Audit Table, Audit Program (and associated type) and configure the Audit Switches on the fields you wish to track.

Note: To enable Auditing on a running version of the product, the online data cache must be flushed or the product restarted. Refer to the *Oracle Revenue Management and Billing Server Administration Guide* for more details.

7.3 Audit Query by Table/Field/Key

Once Auditing is enabled changes are logged in the configured Audit Table using the Audit Program specified in the configuration. It is possible to query this Audit information by Table, Field and Key value to isolate changes. To access this query navigate to the **Administration → A → Audit Query By Table/Field/Key** option. For example:

The screenshot shows the 'Audit Query by Table/Field/Key' search interface. It includes fields for 'Audited Table Name', 'Audited Field Name', and date/time filters. Below the search bar is a table with columns for 'Create Date/Time', 'User Name', 'Primary Key', 'Audited Field Name', 'Audit Action', 'Value Before Update', and 'Value After Update'.

Specify any the following values for the filters:

- **Audit Table Name** – The name of the table that has been audited to query. When this table is chosen the screen will list additional fields to filter upon.
- **Audit Field Name** – The name of the field to track to filter the results.
- **Creation Start Date/Time and Creation End Date/Time** – Date and time range to limit the records returned.

The query will return the following results:

- **Create Date/Time** – Date and time the changes were made.
- **User Name** – Name of user who made the changes.
- **Primary Key** – Record key of the change.
- **Audited Field Name** – Name of field that was changed.
- **Audit Action** – Action that was recorded with change (i.e. Insert, Update or Delete)
- **Value Before Audit** – The field value before the change was made.
- **Value After Audit** - The field value after the change was made.

7.4 Audit Query By User

Once Auditing is enabled changes are logged in the configured Audit Table using the Audit Program specified in the configuration. It is possible to query this Audit information by individual users to isolate changes made by that user. To access this query navigate to the **Administration → A → Audit Query By User** option. For example:

Specify any the following values for the filters:

- **User ID** – Authorization User to track.
- **Audit Table** – The name of the table containing the audit information.
- **Creation Start Date/Time and Creation End Date/Time** – Date and time range to limit the records returned.

The query will return the following results:

- **Row Creation Date** – Date and time the changes were made.
- **Audited Table Name** – Name of table that was audited.
- **Primary Key** – Record key of the change.
- **Audited Field Name** – Name of field that was changed.
- **Audit Action** – Action that was recorded with change (i.e. Insert, Update or Delete)
- **Field Value Before Audit** – The field value before the change was made.
- **Field Value After Audit** - The field value after the change was made.

7.5 Read Auditing

Whilst the inbuilt Audit facility is mainly used to register changes in data, it can also be used to register whenever data is accessed for auditing purposes. The concept of read auditing is different from the standard auditing as it is related to zones⁹. On the zone configuration there is an ability to configure an Audit Service Script which is called whenever the zone is displayed to determine which criteria and result records are displayed.

The information audited can be programmatically determined and which information is logged according to your requirements. Refer to the online zone help for descriptions and samples to configure Read Auditing.

Note: Products ship with sample generic inquiry Audit code specific to the product. These can be reused or altered to suit your needs. Refer to the product documentation for details of these samples.

7.6 Integrating to Audit Vault

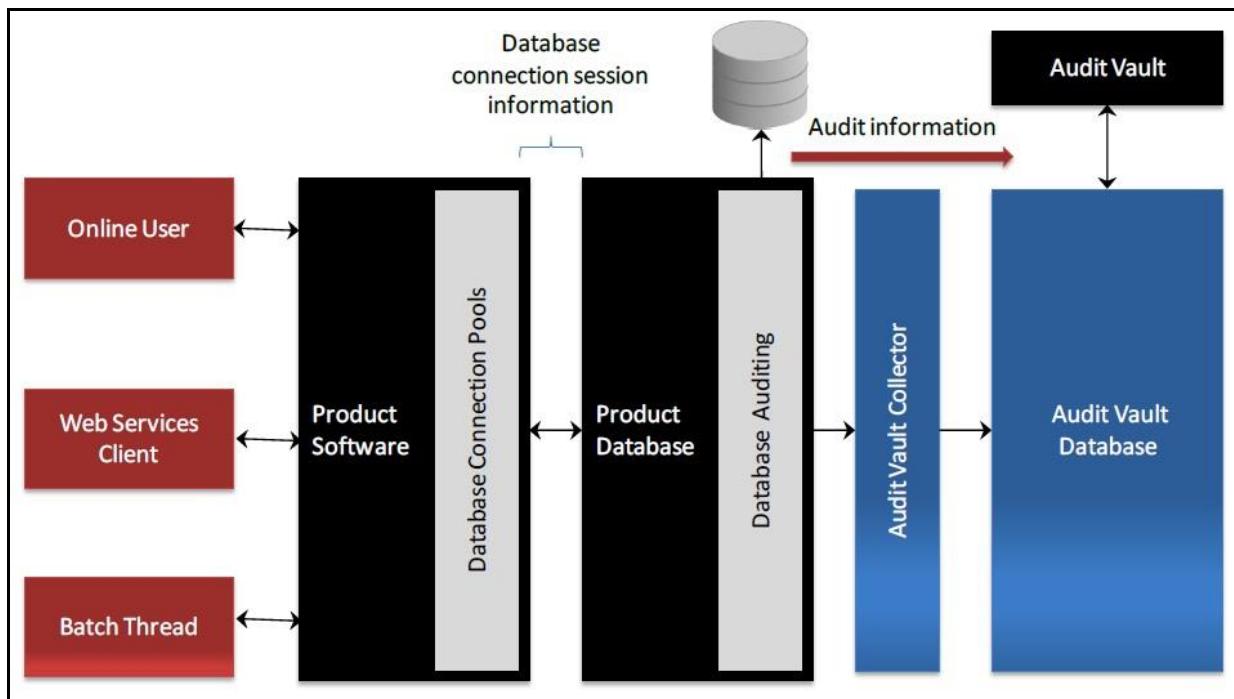
Note: Customers using Oracle 12.x and above, should use Unified Auditing to ensure consistent capture of audit information.

Oracle Utilities Application Framework contains an internal audit facility that provides a basic audit facility for recording changes and optionally, inquiring, data by online users. Whilst this facility is sufficient for most needs it may be replaced with using Oracle Audit Vault to provide an enterprise wide audit facility.

Oracle Utilities Application Framework supports the use of Audit vault in association or as a complete replacement for the inbuilt Auditing feature.

⁹ At the present time this parameter is available for F1-DE, F1-DE-QUERY, F1-DE-SINGLE, F1-MAPDERV and F1-MAPEXPL zone types only.

Audit Vault collects audit information at the database level, using the Database Auditing features of the Oracle Database, and loads them into a separate Audit Vault database. The information in that database can be queried, reported and managed using the Audit Vault front end. For example:



To use Audit Vault the following must be configured:

- **Setup Database Auditing** - The Database auditing feature must be enabled to store the relevant audit information. The level of auditing information and the location of the audit information is configurable. Refer to the *Oracle Database Security Guide* for a discussion of Database Auditing and Best Practices of Auditing for a discussion of the various methods available.
- **Design Database Auditing** - The tables, users and SQL statements to audit need to be specified on the product database. This typically done by the database administrator using the AUDIT statement.
- **Install and Configure Audit Collector** - On the host holding the product database an Audit Vault Data Collector needs to be configured to pass audit information to Audit Vault and implement data retention policies for audit information.
- **Configure Audit Vault** - Audit Vault can be configured to implement policies, alerts and reports on the Audit data. Audit Vault can be configured to set an Audit Data Retention Policy for its internal audit information.

8. Database Security

8.1 About Database Security

The Oracle Database supports a wide range of security configurations natively or via additional options available. For a full discussion of the available security options for the database refer to the [Oracle Database Security Guide](#).

8.2 Database Users

The product installation ships with a predefined set of users to be used by the product at configuration and runtime. These users are specified in the installation of the product to build the database and load its initial dataset.

The following users are available:

- SPLADM – This is the default DBA administration account which owns the product schema. This user is used to create and maintain the structures of the database. It is used by DBA personnel to maintain the product schema and indexes.
- SPLUSER – This is the default main product user used by the product to access the SPLADM schema. The product uses this physical user ID as a pooled user with pooled connections to the database. Variations on this account can be created for each channel of access using the following configuration settings.

Configuration Parameter	Comments
BATCH_DBUSER	Database User for Batch
DBUSER	Database User for online (Default: SPLUSER)
XAI_DBUSER	Database User for Web Services

- SPLREAD – This is the default read only user available for reporting tools or external direct interfaces to use on the product database. This user is not used by the product¹⁰.
- CISOPR, OPRPLUS – These are optional operator users that can be used to delegate backup and restore operations on the product.

Note: The values of these users can be altered to customer specific values at installation time. Refer to the *Oracle Revenue Management and Billing Installation Guide* and *Oracle Revenue Management and Billing Database Administrator's Guide* for more information.

¹⁰ For customers on older versions of particular products this user was also used for the ConfigLab component.

8.3 Database Roles

The product ships with a set of database roles to allow administrators to allocate new database users to the relevant components of the product. The following roles are shipped by default for the product:

- **SPL_USER** – This role is available for database users who require update, insert, delete and select access to the product schema. This role is used for product users.
- **SPL_READ** – This role is available for database users who require read only access to the product schema.

To use the roles the DBA grants the role to the database user to connect them to the schema in the desired fashion.

8.4 Database Permissions

Database permissions for the product are allocated at the role level with the role setting permissions to the schema objects. By default the roles have full access to all the objects in the product schema, as dictated by the role.

Unless otherwise stated, it is not recommended to alter the database users used by the product to specific additional permissions on the product schema as this may cause permission issues.

Customers wishing to restrict external parties, such as external tools or reporting engines, to specific objects may use all of the desired security facilities available in the database to implement those restrictions.

8.5 Using Transparent Data Encryption

Transparent Data Encryption (TDE) allows data to be encrypted at the storage level to protect the data files at the lowest level. From a product perspective, the implementation of Transparent Data Encryption requires no product configuration changes on the application server.

Note:

To implement Transparent Data Encryption, DBAs will have to execute appropriate alter statements on product tables to indicate the level of encryption.

For product tables with large amounts of data it is recommended to use the NOMAC feature to save disk space.

For more information about implementing Transparent Data Encryption refer to the *Oracle Database Security Guide*.

8.6 Using Database Vault

By default, the database administration account has SQL Data Manipulation Language (DML) access to the product schema, as dictated by the default permissions of the Oracle Database. It is possible to restrict the permissions of the DBA to SQL Data Definition Language (DDL) statements only using Database Vault. Refer to the [Database Vault Administrator's Guide](#) for details of this facility.

The product includes a prebuilt database vault solution, refer to the Database Vault Integration (Doc ID: 1290700.1) available from [My Oracle Support](#).

9. Security Integration

9.1 About Security Integration

Whilst the product provides a set of security facilities natively or via the JEE Web Application Server, it is possible to augment the security with additional security features or security products.

9.2 LDAP Integration

By default, Oracle WebLogic includes an internal security repository that uses the Lightweight Directory Access Protocol (LDAP) to provide authentication facilities¹¹. It is possible to replace the internal security repository with another LDAP compliant security source.

To use an alternative source as a security repository the following process must be used:

- The JEE Web Application Server must be configured to use the external LDAP security source for authentication. Refer to the documentation provided with the JEE Web Application Server for more details. For Oracle WebLogic customers, refer to the [Configuring LDAP Authentication Providers](#) section of the *Oracle Fusion Middleware Securing Oracle WebLogic Server Guide*.
- The product LDAP import feature can be used to initially populate the authorization model from the LDAP source as outlined in the LDAP Integration for Oracle Utilities Application Framework based product (Doc ID: 774783.1) available from [My Oracle Support](#).

Note: Whilst LDAP sources are the most common security repository, it is possible to use alternative security authentication sources as supported by the JEE Web Application Server. Refer to the documentation provided with the JEE Web Application Server for more details.

9.3 Single Sign On Integration

One of the common security integrations is the ability to implement Single Sign On with the product. This enables end users to access the product minimizing the need to re-authenticate each time.

The JEE Web Application Server can be configured to support Single Sign On. For more details refer to Single Sign On Integration for Oracle Utilities Application Framework based products (Doc ID: 799912.1) and Oracle Identity Management Suite Integration with Oracle Utilities Application Framework based products (Doc ID: 1375600.1) available from [My Oracle Support](#).

9.3.1 Kerberos Support

Single Sign-On (SSO) with Microsoft clients allows cross-platform authentication between Web applications running in the JEE Web Application Server and .NET Web service clients or browser clients (for example, Microsoft Internet Explorer) in a Microsoft domain. The Microsoft clients must use Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism.

Refer to [Configuring Single Sign-On with Microsoft Clients](#) for details of configuring Oracle WebLogic to use Kerberos.

¹¹ It also provides authorization services but these are not typically utilized by the product.

9.4 Oracle Identity Management Suite Integration

Oracle offers a comprehensive set of security products as part of the Oracle Identity Management Suite that can be used to augment the security setup at your site. The product can be integrated with the following components of Oracle Identity Management Suite:

- **Oracle Identity Manager** – Oracle Identity Manager can be used to centralize user provisioning to the product, password rule management and identity administration.
- **Oracle Access Manager** – Oracle Access Manager can be used to provide authentication, single sign on, access controls and user tracking.
- **Oracle Adaptive Access Manager** – Oracle Adaptive Access Manager can be used to provide fraud tracking and multi-faceted authentication.
- **Oracle Virtual Directory** – Oracle Virtual Directory can be used to provide virtualized LDAP security access to LDAP and non-LDAP security sources.
- **Oracle Internet Directory** – Oracle Internet Directory can be used as a LDAP security store.

Refer to the Oracle Identity Management Suite Integration with Oracle Utilities Application Framework based products (Doc ID: 1375600.1) whitepaper for more information, available from [My Oracle Support](#).

10. Keystore and Truststore Support

Oracle Utilities Application Framework supports the ability to store cryptographic keys and/or certificates. The keystore is used to encrypt and decrypt data such as passwords and product data. It is also possible to implement a trust store to ensure the integrity of certificates.

10.1 Creating the Keystore and Truststore

Note:

For backward compatibility, customers on older versions will have a default keystore and truststore created upon upgrade with backward compatible values.

If the keystore and truststore is not present, Oracle Utilities Application Framework will revert to the internal cryptography used in previous releases.

Passwords encrypted using this keystore will be prefixed with ENCKS and legacy password encryption uses prefix ENC.

Typically a keystore and truststore is created using the java keytool utility manually but Oracle Utilities Application Framework utilities have been extended to allow customers to create and manage the keystore from the command line.

Before creating the keystore the following settings must be set in the installation, as per the *Oracle Revenue Management and Billing Server Administration Guide*:

- KS_ALIAS - The alias used to encrypt/decrypt passwords by Oracle Utilities Application Framework to access the keystore. By default, it is set to ouaf.system.
- KS_ALIAS_KEYALG - The algorithm used by the KS_ALIAS entry in keystore to encrypt the passwords. By default, it is set to AES (i.e. Advanced Encryption Standard).
- KS_ALIAS_KEYSIZE - The strength of the keystore for the KS_ALIAS entry. By default, it is set to 128.
- KS_HMAC_ALIAS - The HMAC alias used by the Encryption Feature Type of Oracle Utilities Application Framework. By default, it is set to ouaf.system.hmac.
- KS_HMAC_ALIAS_KEYALG - The algorithm used by the KS_HMAC_ALIAS entry in keystore to encrypt the data. By default, it is set to HmacSHA256.
- KS_HMAC_ALIAS_KEYSIZE - The strength of the keystore for the KS_HMAC_ALIAS entry. By default, it is set to 256.
- KS_KEYSTORE_FILE - Location of the keystore file.
- KS_MODE - Keystore Padding mode. By default, it is set to CBC (cipher-block chaining).
- KS_PADDING - Key padding algorithm used for keystore. By default, it is set to PKCS5Padding.
- KS_STOREPASS_FILE - Keystore Password file.
- KS_STORETYPE - Keystore type. By default, it is set to JCEKS.
- TS_ALIAS - Alias used for trust store. By default this is set to ouaf.system
- TS_ALIAS_KEYALG - The algorithm to be used by the TS_ALIAS entry in truststore. By default this is set to AES.

- `TS_ALIAS_KEYSIZE` - The strength of the truststore for the `TS_ALIAS` entry. By default this is set to 128.
- `TS_HMAC_ALIAS` - The HMAC alias used by the truststore. By default this is set to `ouaf.system.hmac`.
- `TS_HMAC_ALIAS_KEYALG` - The algorithm to be used by the `TS_HMAC_ALIAS` entry in truststore to encrypt the data. By default this is set to `HmacSHA256`.
- `TS_HMAC_ALIAS_KEYSIZE` - - The strength of the truststore for the `TS_HMAC_ALIAS` entry. By default this is set to 256.
- `TS_KEYSTORE_FILE` - - Location of the truststore file.
- `TS_MODE` - Truststore Padding mode. By default this is set to `CBC`.
- `TS_PADDING` - Key padding algorithm used for truststore. By default this is set to `PKCS5Padding`.
- `TS_STOREPASS_FILE` - Truststore Password file.
- `TS_STORETYPE` - Truststore type. By default this is set to `JCEKS`

Once these settings are specified the keystore or truststore is created using the following command:

Linux/UNIX:

```
initialSetup.sh -k|-K
```

Windows

```
initialSetup.cmd -k|-K
```

This generates the keystore (|-K) or truststore (|-K) using the credentials outlined in the Keystore or Truststore Password file.

10.2 Altering the Keystore/Truststore Options

Note: This process should be used for any keystore/truststore change including copying keystores/truststores across environments.

After creating the keystore, if any of the keystore values need to be changed, then the system needs to be realigned to the new configuration. The following process must be performed:

- Logon to the machine where you wish to make the changes to the settings.
- Execute the `splenvirion[.sh] -e <environment>` command where `<environment>` is the environment on the machine to change.
- Shutdown the environment.
- Alter the keystore parameters to suit the new desired configuration using the `configureEnv[.sh] -a` utility.
- Execute the `initialSetup[.sh] -k|-K` utility to recreate the keystore (-k) or truststore (-K) with the new settings.
- Execute the `configureEnv[.sh]` once more and press enter on each password prompt to re-encrypt the passwords with the new settings.
- Execute the `initialSetup[.sh]` command to apply the changes to the configuration files.

Note: For customers using native installation, update the Deployments using the Oracle WebLogic console or Oracle Enterprise Manager to load the new versions of the product EAR files.

- If the encryption values have changed, the data encrypted in the database must be re-encrypted to match the new settings using the process outlined in the [Synchronize Data Encryption](#) section.

10.3 Synchronize Data Encryption

Note:

Failure to synchronize data when encryption values change will cause outages and unexpected behaviour in the product.

The product should be shutdown while running this process.

If at any time the encryption values change, the values that are encrypted using the old value must be updated to reflect the new settings. A new utility named com.splwg.shared.common.ChangeCryptographyKey is provided to synchronize data changes. The following keys are updated using this utility:

- Database Passwords used in Feature configurations such as Database Update features.
- XML Application Integration legacy passwords for JDBC.
- XAI Sender and Receiver Passwords (depending on Sender and Receiver type)
- Reporting tool integration passwords
- Multi-Purpose Listener passwords (for selected products)
- Email Adapter configuration.
- Web Services Passwords (legacy only)
- Security Hashes on user records

The following process is to be used:

- Logon to the machine you have made the changes upon as the product administrator.
- If you have not already done so, use the splenviron utility to set the environment variables for the product environment.
- Execute the following command:

Windows:

```
perl %SPLWEBASE%\run_java_standalone.plx
com.splwg.shared.common.ChangeCryptographyKey [-t|-l|-h|-p]
[old-settings]
```

Linux:

```
perl $SPLWEBASE/run_java_standalone.plx
com.splwg.shared.common.ChangeCryptographyKey [-t|-l|-h|-p]
[old-settings]
```

The following table lists and describes the command line options:

Command Line Option	Description
-t	Test Mode (no commit of changes)
-l	Convert Legacy/OUAF System key
-h	Convert User hashes only
-p	Convert encrypted passwords only
[old settings]	<p>You can use the following old settings:</p> <ul style="list-style-type: none"> - Dcom.oracle.ouaf.system.old.keystore.file=<oldfile> - Dcom.oracle.ouaf.system.old.keystore.passwordFileName=<oldpassfile> - Dcom.oracle.ouaf.system.old.keystore.type=<oldtype> - Dcom.oracle.ouaf.system.old.keystore.alias=<oldalias> - Dcom.oracle.ouaf.system.old.keystore.padding=<oldpadding> - Dcom.oracle.ouaf.system.old.keystore.mode=<oldmode> <p>Where,</p> <ul style="list-style-type: none"> • <oldfile>: Original Keystore file • <oldpassfile>: Original Password Store file • <oldtype>: Original Keystore type • <oldalias>: Original alias • <oldpadding>: Original Padding • <oldmode>: Original Mode <p>Note: The command line options such as -t, -l, -h, and -p should not be used with these old settings.</p>

Note:

Only specify the values that have been changed.

This command has to be run once for each alias.

After executing the `com.splwg.shared.common.ChangeCryptographyKey` utility, you must execute `<SPLEBASE>/bin/invokeDBUpdatePatch.cmd|sh` to reset the database patching credentials as follows:

- If you have not already done so, use the `splenviron` utility to set the environment variables for the product environment.
- Run the command with the `-b` option to go into interactive mode and reply to the prompts. Use the `-h` option to get help.

Windows:

```
%SPLEBASE%\bin\invokeDBUpdatePatch.cmd -b
```

Linux:

```
$SPLEBASE/bin/invokeDBUpdatePatch.sh -b
```

10.4 Upgrading from Legacy to Keystore

When upgrading from past releases of Oracle Utilities Application Framework and adopting the new keystore it is recommended to use the following process to adopt the keystore:

- Ensure all passwords have been updated by executing the `configureEnv` and pressing enter at each password prompt.
- Execute the process outlined in the [Synchronize Data Encryption](#) section by running the `com.splwg.shared.common.ChangeCryptographyKey` utility with the `-l` option to convert old keys to new keys. For example:


```
java ChangeCryptographyKey -l
```
- Ensure that you also execute the `invokeDBUpdatePatch.cmd|sh` utility mentioned in the [Synchronize Data Encryption](#) section.
- Optionally, it is possible to update the passwords using the `LegacyCryptographerUpdater` utility on individual passwords using the following command:


```
java LegacyCryptographyUpgrader [-f <file>] -p <password>]
```

Where options are:

Command Line Option	Description
<code>-f <file></code>	Read <code><file></code> for password and re-encrypt to stdout
<code>-p <password></code>	Decrypt old password <code><password></code> and re-encrypt to stdout. The password should be already in ENC format.

For more information, refer to the *Oracle Utilities Application Framework - Keystore Configuration (Doc ID 2014161.1)*.

10.5 Importing Keystores/Truststores

While the product supplies a default keystore and truststore it is possible to import existing keystores and/or truststores from alternative sources (such as a corporate level set of stores or from a trusted CA authority).

To import a keystore or truststore the following process should be followed:

- Logon to the machine you have made the changes upon as the product administrator.
- If you have not already done so, use the `splenviron` utility to set the environment variables for the product environment.
- Ensure the `KS_IMPORT_KEYSTORE_FOLDER` or `TS_IMPORT_KEYSTORE_FOLDER` are set in the `ENVIRON.INI` prior to continuing. These are the locations the files to be imported will be located for keystores and truststores respectively.
- Copy the new keystore or truststore to the locations specified in the `KS_IMPORT_KEYSTORE_FOLDER` or `TS_IMPORT_KEYSTORE_FOLDER` respectively.
- Execute the `initialSetup[.sh]` `-s` | `-S` to import the keystore (`-s`) or truststore (`-S`) successfully.

11. Encryption Feature Type

One of the major features of Oracle Utilities Application Framework is the ability to mask and encrypt data within the product to protect sensitive information. This encryption is implemented in a Feature Configuration using the Encrypted Feature Type.

11.1 Overview

Oracle Utilities Application Framework supports Feature Configuration which store specific configuration settings for features in the product to be implemented. Feature Configurations allow simple configurations to be implemented for specific features.

Feature Configurations can be maintained using the **Admin Menu → F → Feature Configuration menu item**. For example:

	Option Type	Sequence	Value	Detailed Description
				<p>car, indicate the table name and the field name where the data resides, for example table="table_name", field="fld_name", alias="key alias" A "where" clause may also be specified. This is useful for data that resides in a child table where only data of a certain type needs to be masked. For example table="CL_PER_ID", field="PER_ID_NBR", alias="key alias", where="ID_TYPE_CD=SSN". For data that is stored as a characteristic, simply indicate the characteristic type CHAR_TYPE_CD=char type, alias="key alias" This needs to be defined only once regardless of which characteristic entity the char type may reside on. Note that only ad-hoc characteristics are supported. Any encrypted field may optionally be "wrapped" with a special marker (e.g., ENC{}) to indicate that the field value is encrypted. This can be specified by the key wrap="true" or wrap="false". The default is false. The wrap field should be set to false unless additional processing in your code is included to handle the special marker. In addition, an encrypted field value may additionally store a hashed representation (suitable for verification or "indexing" a value) and a masked representation, suitable for presenting a user with a partial representation of the encrypted value. These representations require extra storage, either as a physical column on the same table as the encrypted data column, or a field defined at the same level on the schema defining the encrypted data</p>
+	Field Encryption	1		

For the Encryption feature, one Feature Configuration should exist for the Encryption Feature Type with an option per field to encrypt.

Note: If the product does not ship a Feature Configuration for Encryption, then it can be created as a Customer Modification. Prefix the name of the Feature Name with CM.

11.2 Configuration of Encrypted Fields

To define a field to encrypt an option must be added with the following attributes:

- Option Type should be set to Field Encryption.
- Sequence should be an appropriate sequence number. Typically this is a number that is not used already. Higher number values override lower level sequences.
- In the value you need to specify the specification of the encryption in the format of a command string.

Attribute	Description	Value Format
table	Used to specify the table name. The table must exist in the meta data.	table="SC_USER"
field	Used to specify the field name that you want to encrypt. The field must exist in the metadata.	field="FIRST_NAME"
alias	Used to specify the keystore alias that you want to use to encrypt the data.	alias="ouaf.system"
where	Used for filtering the data. It is used when you want to determine specific values for encryption.	where="ID_TYPE_CD='SN'"
wrap	Used to indicate whether the value should be wrapped with the ENC() marker or not. The valid values are: <ul style="list-style-type: none"> • true • false 	wrap=false
maskAlg	Used to specify the algorithm that you want to use to mask the field.	maskAlg="CMCCR"
maskField	Used to specify the field that you want to use to mask the field.	maskField="CNBR_MASK"
hashAlias	Used to specify the alias in the keystore. It is required when you want to hash a field.	hashAlias="ouaf.hmac.system"
hashField	Used to specify the field that you want use as the hash value for the hashed field.	hashField="CNBR_HASH"
encryptedField	Used to specify another field name in the table where you want to store the encrypted output. Note: You need to specify a value for this attribute only if you want to store the encrypted output.	encryptedField="PK_V_AL2"

For example:

```
table="F1_ATTACHMENT",field="PK_VAL5",alias="ouaf.system",encryptedField="PK_VAL2",hashAlias='HmacSHA256-1024',hashField="PK_VAL3",where="PK_VAL1='Encrypted'"
```

There are a few guidelines when using this facility:

- The aliases specified in alias and/or hashAlias must exist in the keystore used for the product.
- Fields to be encrypted must be in string format only. Other field formats are not supported.
- If using a higher level of encryption may increase the storage requirements for a field. If this is the case, adding an encryptedField to hold the larger encrypted value.
- The wrap field should be set to false unless additional processing in your code is included to handle the special marker. Product fields should use wrap=false. Wrapping an encrypted value can be useful in knowing whether a specific data is encrypted in cases where only some data on the table is encrypted.
- Ad-hoc characteristics cannot be specified in the WHERE tag.
- Hashing the value is handy for additional verification and indexing values.

12. Web Services Security

12.1 About Web Services Security

In the product the Inbound Web Services capability, based upon a JAX-WS implementation, allows support for WS-Security and WS-Policy support on individual Inbound Web Services from a number of perspectives.

Note: Refer to the *Web Services Best Practices* (Doc ID: 2214375.1) for additional implementation advice for web services security.

12.2 Annotation Security

It is possible to implement custom WS-Policy support using inbuilt annotation support on individual Inbound Web Service definitions. This allows the policies to be implemented within the product and allows for backward compatibility for sites using XML Application Integration (XAI).

The product supports custom WS-Policy files using the following method:

- The WS-Policy formatted XML file containing the policy definition is installed in the \$SPLBASE/splapp/iws/resources/policies directory (or %SPLBASE%\splapp\iws\resources\policies directory on Windows).
- A Web Service Annotation of type F1POLICY is defined using the Web Service Annotation maintenance function. In that Annotation entry the following should be configured:
 - **uri** – The name of the policy XML file located in the policies directory in the format "policy:<policyname>" where <policyname> is the name of the file containing the policy. For example: "policy:UsernameToken.xml".
 - **attachToWsdl** – Whether the WS-Policy file is attached to the WSDL.
 - **direction** - Specifies when to apply the policy as per weblogic.jws.Policy.Direction. For example: Direction.both
- The annotation is attached to the relevant Inbound Web Services to implement the policy using the Inbound Web Services maintenance function. For example:



Note: Multiple policies can be added as documented in Support for Multiple Policies.

12.3 Oracle WebLogic WS-Policy Support

Note: Customers wishing to use Oracle WebLogic policies should NOT configure policies via the annotations on the same web service. Use of Oracle WebLogic policies and annotations are mutually exclusive and can cause unintentional security violations.

Oracle WebLogic has inbuilt WS-Policy Message-Level¹² and Transport-Level support with predefined policies that can be used with Inbound Web Services at the container level. These policies can be attached within the container on individual services using the Oracle WebLogic console using Attach a WS-Policy to a Web Service using the policy type of WebLogic Web Service Policy.

Multiple policies can be supported directly by specifying additional policies in the Chosen Inbound Message Policies.

12.4 Oracle Web Services Manager Support

Note: Customers using annotations can also use Oracle Web Services Manager policies by specifying the F1-OWSM Policy type as an annotation.

Oracle Web Services Manager can be used to secure individual Inbound Web Services providing additional WS-Policies and access control support. As with Oracle WebLogic WS-Policy support, configuration is performed using the Oracle WebLogic console by specifying individual policies on individual Inbound Web Services by using the policy type of Oracle Web Services Manager (OWSM).

Refer to Using Oracle Web Service Manager Security Policies for additional information about Oracle Web Services Manager.

12.4.1 Access Control Support

Note: By default, all Inbound Web Services are accessible by all valid users.

Oracle Web Services Manager allows for access controls to be configured for Inbound Web Services to provide additional security access controls. This facility allows for multiple rules to be configured implementing access rules across the following areas:

- **Basic Policies** – Policies relating to identity, group, role, environment mode and generic global rules.
- **Date and Time Policies** – Policies relating to specific dates and times including periods of access.
- **Context Element Policies** – Policies relating to data within the service itself.

Policies can be individually specified per service operation or combined to implement complex access requirements.

Refer to Security Policy Conditions for more information about specific policies and how to enable policies on services.

¹² Message level policy support is restricted to the whole message not within parts of the message.

12.5 Support for Multiple Policies

Within each policy regime (annotation, Oracle WebLogic or Oracle Web Services Manager) it is possible to configure multiple policies where web service clients must conform to at least one policy specified. The following methods are supported:

- **Annotations** – On the Inbound Web Service each policy can be added as an individual annotation with the sequence number designating the order they are checked. It is also possible to delegate Oracle Web Services Manager for policies as part of an annotation using the F1-OWSM annotation type.
- **Oracle WebLogic/Oracle Web Services Manager** – In the web service deployment, it is possible to designate multiple policies in the Chosen Policies column of the individual web service WS-Policy configuration. The order of the policies is dictated by the position in the list of Chosen Policies.

12.6 Importing Certificates for Inbound Web Services

If your implementation uses certificates for security, the certificate must be deployed with the Inbound Web Services deployment. To perform this activity:

- Ensure the certificate is valid and is installed on the Oracle WebLogic servers used for deployment of the Inbound Web Services.
- Logon to the machine you have made the changes upon as the product administrator.
- If you have not already done so, use the `splenviron` utility to set the environment variables for the product environment.
- Execute the `initialSetup[.sh] -i [<host>:<port>]` where to import the certificate into the Inbound Web Service deployment.

13. Whitelist Support

13.1 About Whitelist Support

In the Oracle Cloud implementations of the product the use of whitelists is enforced to protect resources within the implementation. These whitelists can also apply to non-cloud implementations and in some cases can be extended to suit individual needs.

Note: Custom whitelists are not supported on Oracle Utilities SaaS Cloud Services.

13.2 URL Whitelist

Note:

The URL whitelist is blank by default unless otherwise configured as part of your customizations.

For this facility to be used the com.oracle.ouaf.uriValidation.enable parameter in the spl.properties file must be set to true.

It is possible to limit the values of URL's within the product for key objects with the configuration. This is implemented as a whitelist that can filter on scheme (aka protocol), hosts and ports. These are checked at runtime and can generate an error if they do not adhere to the whitelist.

The feature allows for the following:

- Individual scheme, hosts and port combinations can be configured to limit runtime access for specific features.
- Specification of the '*' wildcard is supported for scheme, hosts and ports.

The whitelist is configured using the following settings in the spl.properties file:

XML Tag	Comments
"<Parameter>"	Feature within product to limit. This is a preset string linked to a URI parameter in the product.
uri	URI tag
scheme	Protocol supported by <Parameter>. Valid values will vary depending on the <Parameter> value. For example, URL's support file, http, https etc
host	Host name(s) or IP Address(es) to filter upon.
port	Port number(s) to filter upon.

For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<whitelist>
...
  "Message Sender HTTP URL properties"
  <uri>
    <scheme>https</scheme>
    <host>myhost.mycompany.com</host>
    <port>*</port>
  </uri>
...
</whitelist>
```

Refer to the Server Administration Guide for more details of the usage and format of this file.

13.2.1 Implementing a Custom URL Whitelists

It is possible to establish a custom whitelist to implement URL whitelisting for non-cloud implementations. The format of the whitelist is the same as the above whitelist and this will augment and enhance the existing whitelist (if present). To support a custom whitelist perform the following steps:

- Logon to the machine you have made the changes upon as the product administrator.
- If you have not already done so, use the `splenviro` utility to set the environment variables for the product environment.
- If it does not already exist, clone the product whitelist located as indicated in the `com.oracle.ouaf.whitelist.file` parameter. Ensure the custom file is in the same location as this whitelist file and is prefixed with "cm" to indicate it is a customization. The file name can be valid for your operating system and site preferences and must be suffixed with ".xml". Uncomment any section you want to set.
- Create a custom `spl.properties` template or use the templating function to set the following parameter with the filename and location of the custom whitelist.
`com.oracle.ouaf.customer.whitelist.file=<filename>`
- Execute the `initialSetup[.sh]` to implement the new setting.

13.3 SQL Whitelist

Note:

Custom SQL Whitelists are not supported at this time.

Sites not wanting to use this SQL function whitelist should ensure that the `spl.runtime.customSQLSecurity` is set to false in the `spl.properties` file.

The SQL used in query zones and in Groovy scripts can be limited in terms of what SQL functions are supported to prevent performance issues or inappropriate access to the database via functions.

The product provided whitelist is implemented as a Managed Content object named `F1-SQLFunctionWhiteList`. This whitelist is not changeable and lists the supported functions that are whitelisted for use. Any function used that is not used in this whitelist, if the facility is enabled, will generate a runtime error when the SQL is executed.

13.4 HTML WhiteList

The HTML used in UI Maps can be limited using a HTML whitelist. This product managed whitelist lists the valid HTML tags that can be used in the HTML objects. The whitelist is implemented as a Managed Content whitelist named `F1-HTMLWhiteList`.

Any attempt to run a UI Map with a tag that is not listed in the `F1-HTMLWhiteList` will be ignored (as comments) which may lead to unexpected behavior.

13.5 Implementing a Custom HTML Whitelist

It is possible to replace the inbuilt HTML whitelist by creating a custom HTML whitelist to extend the tags supported at runtime in UI Maps.

To implement a custom HTML whitelist, copy the `F1-HTMLWhiteList` Managed Content to `CM-HTMLWhiteList` Managed Content and extend the whitelist.

Note:

Do not remove any tags that exist within `F1-HTMLWhiteList` in your custom whitelist. This may cause unexpected behavior across base UI Maps.

Any upgrades to `F1-HTMLWhiteList` must be also manually reflected in `CM-HTMLWhiteList` for any subsequent upgrade.

13.6 Groovy Whitelist

Note: The current implementation of the Groovy Whitelist is dynamically generated and cannot be altered.

The Groovy language has been added as an alternative language used for scripting. As the Groovy language can access low level API's it has been whitelisted to exclude parts of the language not appropriate for cloud implementations. The whitelist confirms to the Oracle Cloud SDK Supported Groovy Classes and Methods. ADF extensions to Groovy are not supported. Refer to the online documentation for additional advice and examples.

14. Custom Authentication Service Provider

In the Oracle Utilities Application Framework, a custom Oracle WebLogic Authentication Service Provider has been provided to support complex domain security configurations.

14.1 What does this Security Provider do?

The Oracle Utilities Application Framework Service Provider allows Oracle WebLogic domains to be extended with the following additional checks:

- The provider will check that the authentication user has been defined as a User object within the product. If the user does not exist, then the provider will issue an error to be processed according to the rules in the domain security setup (including using the Oracle WebLogic Adjudicator Providers to implement access rules).
- If the user exists as a User object within the product, the user record is checked that the user is enabled for use. It is possible to disable a user at the authorization level as well as the authentication level. This provider performs the authorization level check. If the user is disabled, the provider will issue an error to be processed according to the rules in the domain security setup (including using the Oracle WebLogic Adjudicator Providers to implement access rules).

14.2 Where would I use this Security Provider?

This provider is designed to be used in a number of security scenarios:

- If the domain security realm uses a number of authentication sources then the Security Provider can be used to decide the order where the checks provided by this provider are executed. By default, the login even performs the same checks after all providers are called, the security provider allows that event to be done earlier in the chain.
- If the implementation is using single sign on (SSO) or federated security, this security provider can be used to decide when the checks performed are done in relation to these configurations.

By default, the checks performed by this provider are done automatically by the product login process. Use of the provider allows implementations to perform these checks earlier in the security checking process.

14.3 Implementing the Security Provider

Note:

Before using the provider ensure a data source has been created to connect to the product database to access the SC_USER table.

Each Plugin Properties must exist on a separate line.

The Oracle Utilities Application Framework security provider is provided in the \$SPLBASE/tools/bin/auth subdirectory as ouaf-dbmsauth-<version>.jar. This jar file must be copied to the \$DOMAIN_HOME/lib directory. After restarting the Admin server the following must be configured to use this security provider:

- Login to the Oracle WebLogic Administration console using the appropriate administrator account.
- Navigate to the Security Realms → myrealm → Providers tab from the console.
- Select New to add a new Provider.
- Assign an appropriate name for the provider according to your site standards.
- Use the CustomDBMSAuthenticator for the Provider type.
- Use the Ok button to save the authenticator definition.
- Select the Name you assigned the provider to complete the configuration.
- Select the appropriate Control Flag for your site standards to determine the how the provider fits into the login sequence.
- Select the Provider Specific tab to configure the provider using the following settings:
 - Specify the data source created to connect to the database created earlier in the Data Source Name attribute.
 - Specify com.oracle.ouaf.fed.OuafDBMSAuthenticator for the Plugin Class Name.
 - Specify the userGroup=<usergroupname> where <usergroupname> is the realm group created for the product (set by WEB_APPVIEWER_ROLE_NAME) in the Plugin Properties. By default, this is set to cisusers if parameter not present. For example:
userGroup=cisusers
 - Optionally, specify the users you wish to bypass from this Security provider by specifying the excludeUser=<listofusers> where <listofusers> is a list of authentication users delimited by "," to be excluded. For example:
excludeUsers=system,weblogic,OracleSystemUser
- Save the Provider configuration.
- Optionally, use Reorder to set the order of check.
- Optionally, configure the Adjudicator Provider for additional rules.