

Oracle® Banking Platform Collections

Security Guide

Release 2.6.2.0.0

E95189-01

May 2018

Oracle Banking Platform Collections Security Guide, Release 2.6.2.0.0

E95189-01

Copyright © 2011, 2018, Oracle and/or its affiliates. All rights reserved.

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 decompilation of this software, unless required by law for interoperability, is prohibited.

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.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" 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, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

This software or hardware 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. 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.

Contents

Preface	9
Audience	9
Documentation Accessibility	9
Organization of the Guide	9
Conventions	10
1 Introduction	12
1.1 Security Features	12
2 Authentication	14
2.1 Online Authentication	14
2.2 Web Service Authentication	14
3 Authorization	16
3.1 Authorization Model	16
4 Managing Security	18
4.1 Managing Online Users	18
4.1.1 Managing Users	19
4.1.2 Template Users	20
4.1.3 Assigning To Do Types	21
4.1.4 Assigning User Portal Preferences	22
4.1.5 Assign Favorite Links	23
4.1.6 Assign Favorite Scripts	24
4.1.7 Assign User Characteristics	24
4.1.8 Defining Users to User Groups	25
4.1.9 Defining User Groups to Application Services	26
4.1.9.1 Using the Application Services Portal	27

4.1.9.2 Using User Group Maintenance	30
4.1.10 Define Users to Data Access Groups	33
4.1.11 User Enable and Disable	35
4.2 Managing Batch Users	35
4.3 Managing Web Services Users	36
5 Advanced Security	38
5.1 J2EE Authentication Group	38
5.2 Logon Configuration	39
5.3 Data Ownership Rules	39
5.4 Configuring JMX Security	40
5.4.1 Default Simple File Based security	40
5.4.2 SSL based Security	41
5.4.3 Using Other Security Sources	42
5.5 Menu Security Guidelines	42
5.6 Security Types	43
5.7 Default Generic Application Services	44
5.8 Password Encryption	44
5.9 Administration Delegation	45
5.10 Secure Communications (SSL)	46
5.11 Password Management	46
5.12 Securing Online Debug Mode	47
5.13 Securing Online Cache Management	47
6 Audit Facilities	48
6.1 About Audit	48
6.2 Audit Configuration	48
6.3 Audit Query By User	50

6.4 Read Auditing	51
7 Database Security	52
7.1 About Database Security	52
7.2 Database Users	52
7.3 Database Roles	53
7.4 Database Permissions	53
8 Security Integration	54
8.1 About Security Integration	54
8.2 LDAP Integration	54
8.3 Single Sign On Integration	54
8.4 Oracle Identity Management Suite Integration	55

List of Figures

Figure 3–1 Security Authorization Model	16
Figure 4–1 Managing Online Users Process	18
Figure 4–2 Managing User - Main Tab	19
Figure 4–3 Defining To Do Roles for the User	21
Figure 4–4 Portal Preferences	22
Figure 4–5 Maintain Preference for a Specific Portal	22
Figure 4–6 Assign Favorite Links	23
Figure 4–7 Assigning Favorite Scripts	24
Figure 4–8 Assign User Characteristics	24
Figure 4–9 Defining User to User Groups	26
Figure 4–10 Application Services Portal	27
Figure 4–11 Application Service Details	28
Figure 4–12 User Groups with Access	28
Figure 4–13 User Groups Without Access	29
Figure 4–14 Application Services Tab	29
Figure 4–15 Using User Group Maintenance	30
Figure 4–16 Application Service and an Individual User Group Association	31
Figure 4–17 Maintain Association	31
Figure 4–18 User Group Maintenance	32
Figure 4–19 Object Relationship	34
Figure 4–20 Maintaining Data Access Roles and Access Groups	34
Figure 5–1 Web Descriptor	38
Figure 5–2 Specifying Application Service	43
Figure 5–3 Defining Security Types	43

Figure 6–1 Maintaining Audit Information	49
Figure 6–2 Querying Audit Information	49
Figure 6–3 Audit Query by User	50

List of Tables

Table 4–1 Managing Users	19
Table 4–2 Enable or Disable the User	35
Table 5–1 Default Group Configuration Settings	38
Table 5–2 Configuration Settings	39
Table 5–3 ouaf.jmx.access.file	41
Table 5–4 ouaf.jmx.password.file	41
Table 5–5 Additional System Properties	42
Table 5–6 Password Management	47
Table 7–1 Configuration Settings to Create Variations	52

Preface

This document describes how to configure security using the default security features. To use this document, you need to have a basic understanding on how the product works, and basic familiarity with the security aspects of the Oracle WebLogic and Oracle Database.

What's New in Security?

The Security chapter lists and describes the new and enhanced security features, which provide superior access control, privacy, and accountability.

This preface contains the following topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Organization of the Guide](#)
- [Conventions](#)

Audience

This document is intended for the following audience:

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/us/corporate/accessibility/index.html>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/us/corporate/accessibility/support/index.html#info> or visit <http://www.oracle.com/us/corporate/accessibility/support/index.html#trs> if you are hearing impaired.

Organization of the Guide

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

[Chapter 1 Introduction](#)

This chapter explains how the security features protect access to the product, its functionality and the underlying data stored and managed through the product.

[Chapter 2 Authentication](#)

This chapter explains how online, batch, and web service authentication is handled.

[Chapter 3 Authorization](#)

This chapter 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.

[Chapter 4 Managing Security](#)

This chapter describes how to manage the security definitions from the product, security infrastructure and security repositories.

[Chapter 5 Advanced Security](#)

This chapter lists and describes the advanced security settings that can be configured to support various security requirements.

[Chapter 6 Audit Facilities](#)

This chapter explains how to configure the audit facility to track changes made to the key data.

[Chapter 7 Database Security](#)

This chapter 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.

[Chapter 8 Security Integration](#)

This chapter lists and describes the additional security features or security products that can be integrated with the product to augment the security setup.

Conventions

The following text conventions are used in this document:

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

1 Introduction

Security is one of the key aspects of the product which not only confirms the identity of an individual user but, after the identity is confirmed, it also confirms what kind of data and functions the user can access within the product.

1.1 Security Features

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 through 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 J2EE Web Application Server security:** The supported J2EE 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 J2EE Web Application Server, to authenticate users for online and Web Services based 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 the 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 J2EE Web Application Server. A wide range of security policies are available.
- **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.

2 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 J2EE Web Application Server supports a number of industry standard security repositories and authentication methods. These can be native to the J2EE 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.

2.1 Online Authentication

The product delegates the responsibility of authentication of the online users to the J2EE Web Application Server. This means that any integration that the J2EE 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 J2EE Web Application Server itself.

Typically the J2EE Web Application Server support one or more of the following:

- **Inbuilt Security:** The J2EE 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 and Microsoft Active Directory). LDAP support may be direct or indirect via Identity Management software like Oracle Virtual Directory or Oracle Identity Federation.
- **DBMS Based Security:** The J2EE Web Application Server can store, manage and retrieve security information directly from a database.

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

See the *Security Guides* supplied with your J2EE Web Application Server for details of the security configuration process.

2.2 Web Service Authentication

The Web Service component of the product is housed in the J2EE 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 J2EE Web Application Server.
- The J2EE 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 J2EE Web Application Server can be used.
- Web Service management products such as Oracle Web Services Manager can be used to augment security for Web Services.

3 Authorization

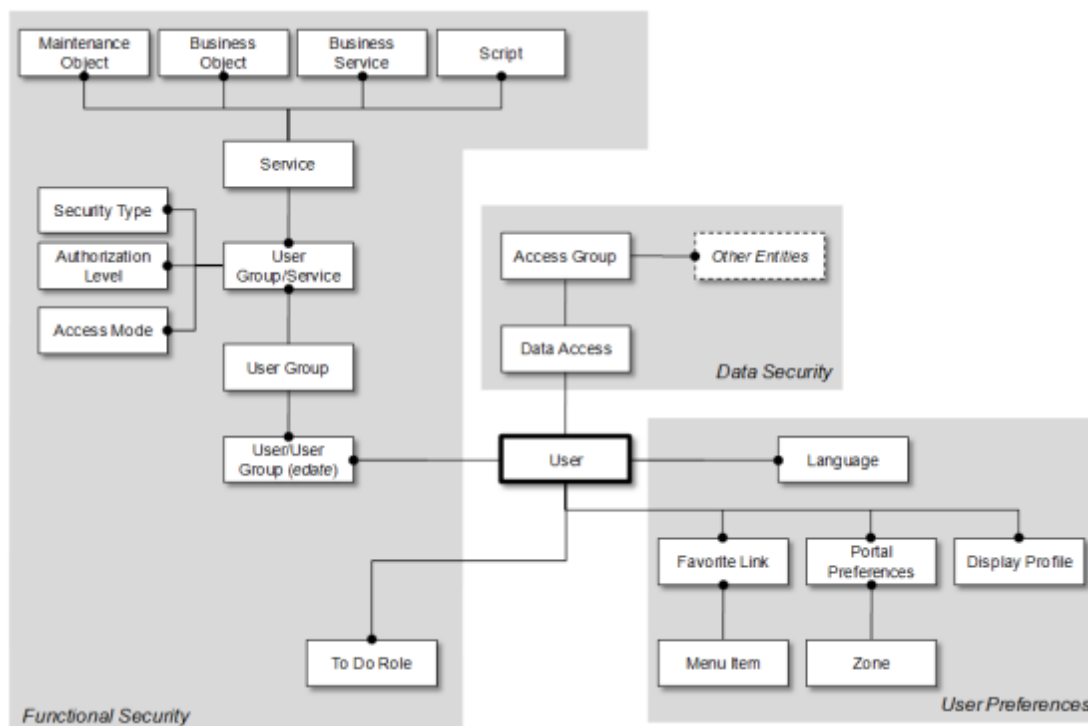
Once users are identified, they must be authorized to specific functions and data within the product.

The 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.

3.1 Authorization Model

The following data model describes the security authorization model.

Figure 3–1 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), 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 active date period of this relationship is defined by effective date. 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 the product. They correspond to each of the screens accessible in the 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 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.

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

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. The 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.

4 Managing Security

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

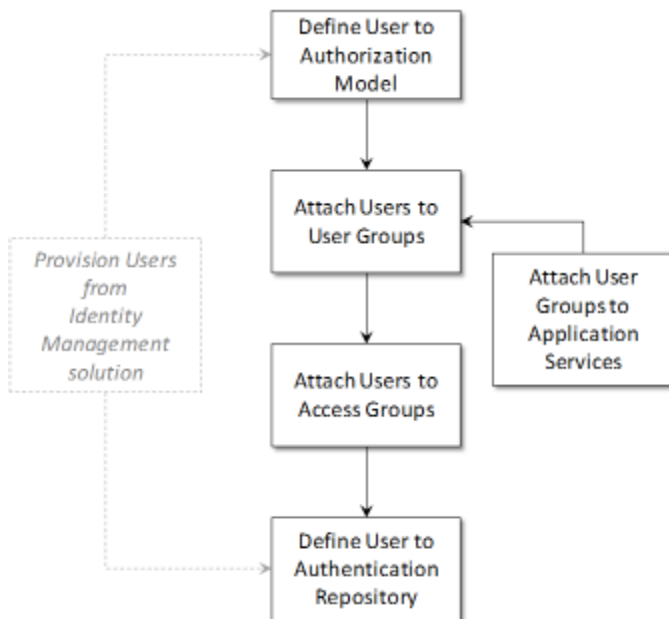
4.1 Managing Online Users

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

- The security repository and rules must be configured in the J2EE Web Application Server to enable authentication. See the *J2EE Web Application Server Administration Guides* for more information.
- The product group used to connect users to J2EE resources should be created in the security repository and configured in the product configuration. The default value for this setting is `cisusers`.
- Users need to be connected to the product group within the security repository to indicate that they can access the J2EE resources.

Following is the outline of the process for managing online users:

Figure 4–1 Managing Online Users Process



- Users should be defined to the authorization model to define their profile and permissions within the product. See [Chapter 4.1.1 Managing Users](#) 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. See [Chapter 4.1.9 Defining User Groups to Application Services](#) 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. See [Chapter 4.1.10 Define Users to Data Access Groups](#) for more details of this process.
- Attach users to the appropriate user groups to define the subset services and valid actions the user can perform within the product. See [Chapter 4.1.8 Defining Users to User Groups](#) for more details of this process.

4.1.1 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. The following process is performed to maintain the users:

- Navigate to the Administration Menu->U->User menu option. Using the Add option on the menu allows navigation to the add function.
- Navigate to the Administration Menu->U->User menu option. Using the Search option on the menu allows navigation to search existing users.
- The User maintenance object is displayed which maintains the security information for the user.
- A screen similar to the one shown in [Figure 4–2](#) is displayed.

Figure 4–2 Managing User - Main Tab

User Group	Expiration Date	Owner
+ ALL_SERVICES	01-01-2100	Base
+ C1_CLSERVICES	01-01-2100	Base

Table 4–1 Managing Users

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.

Field	Comments
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. See Chapter 4.1.11 User Enable and Disable 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 ID associated with the user. This controls the display of currency and dates.
Time Zone	Time Zone allocated to user account. This feature is only applicable to specific products. Check your product online documentation for more information. Changes to the profile user are automatically inherited to any users where the profile user is attached to.
E-mail Address	Optional E-mail address associated with user. This is used by utilities and can be used for interfaces requiring e-mail 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. See Chapter 4.1.2 Template Users for more information.
Favorites Profile User Id	The user id used to inherit favorite definitions from. See Chapter 4.1.2 Template Users for more information.
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. See Chapter 4.1.8 Defining Users to User Groups to User Groups for more information.

- Using the Save function on the top of the screen, you can save the additions or changes.

4.1.2 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.
 - Favorites - Use the Favorites Profile User Id to indicate which Template user can be used to inherit the favorites and favorite scripts.
- 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.

4.1.3 Assigning To Do Types

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.

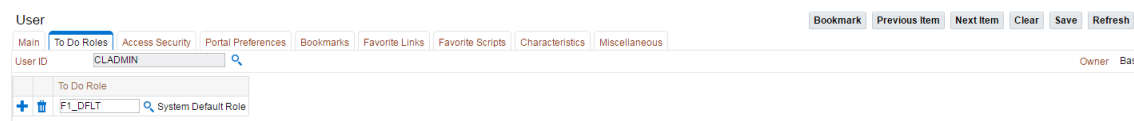
Note

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.

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

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 the user, navigate to the To Do Roles tab of user maintenance function. The following screen appears:

Figure 4–3 Defining To Do Roles for the User



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

Icon	Description
	Use this icon to add a new To Do Role.
	Use this icon to remove an existing To Do Role from the list.
	Use this icon to find the existing To Do Role or it can be typed in.

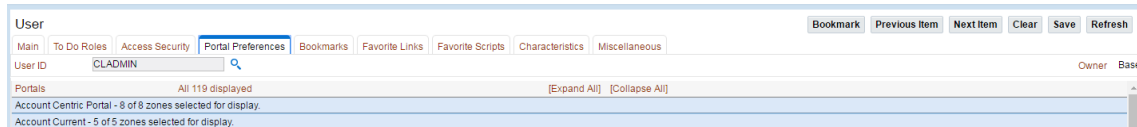
Once the users have been attached to the To Do Roles then they can access the associated To Do types assigned to that role or any To Do directly assigned to them.

4.1.4 Assigning User Portal Preferences

The product user interface is made up of portals containing individual zones. Each of the portals and zones should be associated with an application service for security purpose. 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 the user, navigate to the Portal Preferences tab of user maintenance function. It will display a screen as mentioned below with a list of the portals the user has access to, via the user groups they are attached to:

Figure 4–4 Portal Preferences



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:

Figure 4–5 Maintain Preference for a Specific Portal

Zone	Display	Initially Collapsed	Sequence	Refresh Seconds	Security Access
Add Fact Record	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	Yes
Display Fact Characteristics	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	Yes
Fact General Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	Yes
Fact Log	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	Yes

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. See 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 not. See the online documentation for more information.

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

Note

See 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 the Template users are used. In this case the ability to set for portal preferences for users attached to a template user is disabled.

4.1.5 Assign Favorite Links

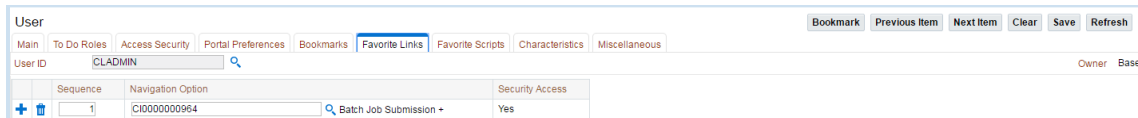
Each individual user can set a number of favorite functions or menu items that they can access using keyboard shortcuts or via the Favorites zone on the Dashboard.

The definition of the users Favorite Links can be configured by navigating to the Favorite Links tab of user maintenance function. The following screen appears:

Note

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




Figure 4–6 Assign Favorite Links



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 the user, the following must be performed:

Icon	Description
	Use this icon 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 this icon to remove an existing Navigation Option from the list.
	Use this icon to find the existing Navigation Option or it can be typed in.

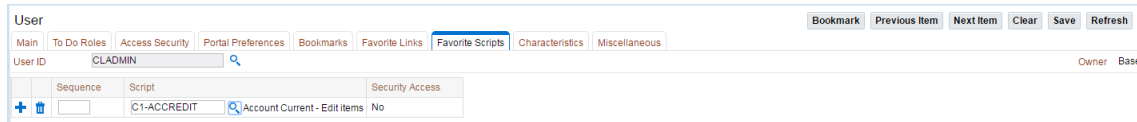
Favorites are then available to be displayed in the Favorites portal on the Dashboard.

4.1.6 Assign Favorite Scripts

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:

Figure 4–7 Assigning Favorite Scripts






Note

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

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 the user, the following must be performed:

Icon	Description
	Use this icon 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 this icon to remove an existing Script from the list.
	Use this icon to find the existing Script or it can be typed in.

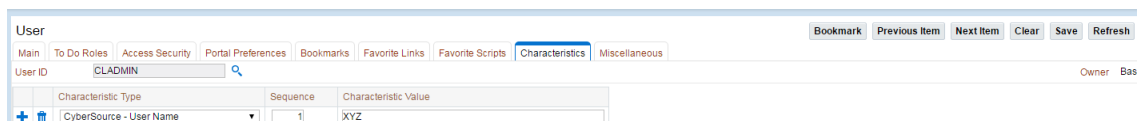
Favorites are then available to be displayed in the Favorite Scripts portal on the Dashboard.

4.1.7 Assign User Characteristics

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. The following screen appears:

Figure 4–8 Assign User Characteristics



Note



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

The product ships with a predefined set of characteristic types.

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 the user, the following must be performed:

Icon	Description
	Use this icon 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 this icon to remove an existing Characteristic from the list.

4.1.8 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 the user and user group is owned and subjected to the 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.
- The 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, the highest valid permission is used.

This can be achieved by navigating to the Main of User Maintenance function. The following screen appears with zones at the bottom of the screen:

Figure 4–9 Defining User to User Groups

		User Group	Expiration Date	Owner	
		 ALL_SERVICES	 System User Group	 01-01-2100	 Base
		 C1_CLSERVICES	 All Services(C1- Collection Admin)	 01-01-2100	 Base

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

Icon	Description
	Use this icon to add a new User Group indicating the User Group Name with the appropriate expiry date to indicate relevance of the connection.
	Use this icon to remove an existing User Group from the list.
	Use this icon to find the existing User Group or it can be typed in.

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

4.1.9 Defining User Groups to Application Services

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 the 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. See [Chapter 5.6 Security Types](#) for more details of this facility.

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.

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.

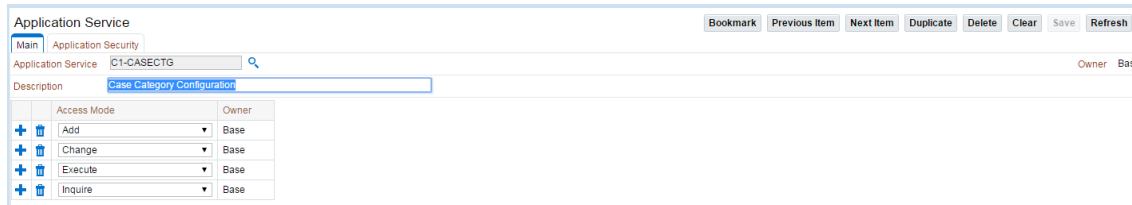
Both methods are valid for most sites and can be used to manage the same information from different prospective.

4.1.9.1 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 Administration Menu->A->Application Service option. The following screen appears:

Figure 4–10 Application Services Portal



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. 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:

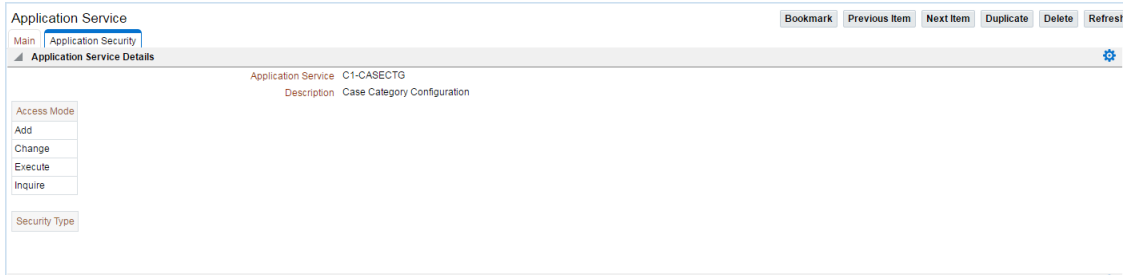
Icon	Description
	Use this icon to add a new Access mode from the drop down list of valid actions. An individual Access Mode can only be defined once for an individual Application Service.
	Use this icon to remove an existing Access Mode from the list.

The Access Mode link to the Application Service is ownership controlled. By default, all created links are owned as Customer Modifications. See [Chapter 5.3 Data Ownership Rules](#) 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:

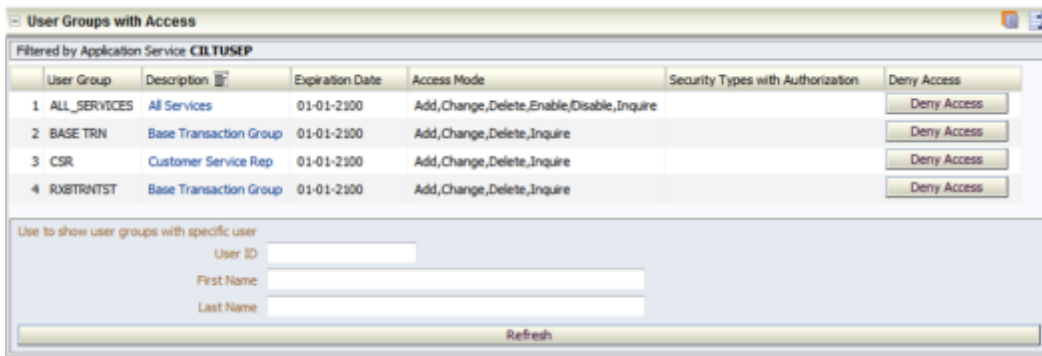
- **Application Service Details:** This zone summarizes the access modes and security types defined for an application service. For example:

Figure 4–11 Application Service Details



- 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:

Figure 4–12 User Groups with Access




- User Groups Without Access:** This zone lists 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:

Figure 4–13 User Groups Without Access

▲ User Groups without Access

Filtered by Application Service C1-DEFAULTPP

	User Group	Description 	Grant Access
1	*PORTAL*	Portal System Default	Grant Access
2	BASE DEV	Base Development Tools	Grant Access
3	BASE TRN	Base Transaction Group	Grant Access
4	C1_ADD_TIER	All Services(C1- Banking Admin)	Grant Access
5	C1_BKSERVICE	All Services(C1- Banking User Admin)	Grant Access
6	C1_BSERVICES	All Services(C1- Banking Admin)	Grant Access
7	C1_CLSERVICES	All Services(C1- Collection Admin)	Grant Access
8	C1_COLLCTRL	User Group for Collection Control	Grant Access
9	C1_COLLDEMO	C1 Collection Demo Service	Grant Access
10	C1_GETTIER	All Services	Grant Access

Use to show user groups with specific user

User ID

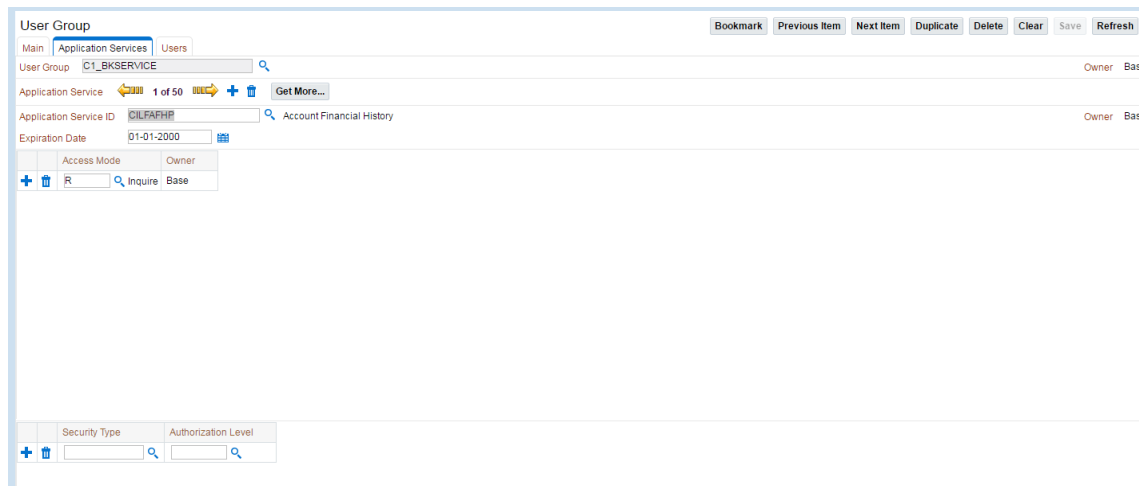
First Name

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:




Figure 4–14 Application Services Tab






- **Expiry Date:** Date on which the access will expire.

Icon	Description
	Use this icon to use the Date selection widget.


- **Access Mode:** Valid Access mode as defined on Application Service definition.

Icon	Description
	Use this icon to add a new Access Mode.
	Use this icon to remove an existing Access Mode from the list.
	Use this icon to find the existing Access Mode or it can be typed in.

- **Owner:** Ownership of link (see [Chapter 5.3 Data Ownership Rules](#)).
- **Security Type:** Security Type code associated with Application Service.

Icon	Description
	Use this icon to add a new Security Type.
	Use this icon to remove an existing Security Type from the list.
	Use this icon to find the existing Security Type or it can be typed in.

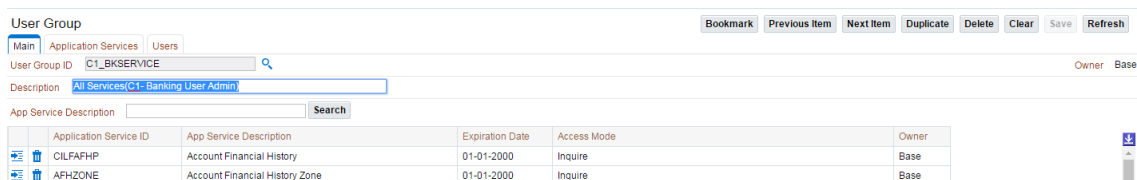
- **Authorization Level:** The Authorization Level assigned to this User Group when executing this Application Service for the Security Type.

Icon	Description
	This icon can be used to find the existing Authorization Level or it can be typed in.

4.1.9.2 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 Administration Menu->U->User Group menu option. The following screen appears:

Figure 4–15 Using User Group Maintenance



Application Service ID	App Service Description	Expiration Date	Access Mode	Owner
CILFAFHP	Account Financial History	01-01-2000	Inquire	Base
AFHZONE	Account Financial History Zone	01-01-2000	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:



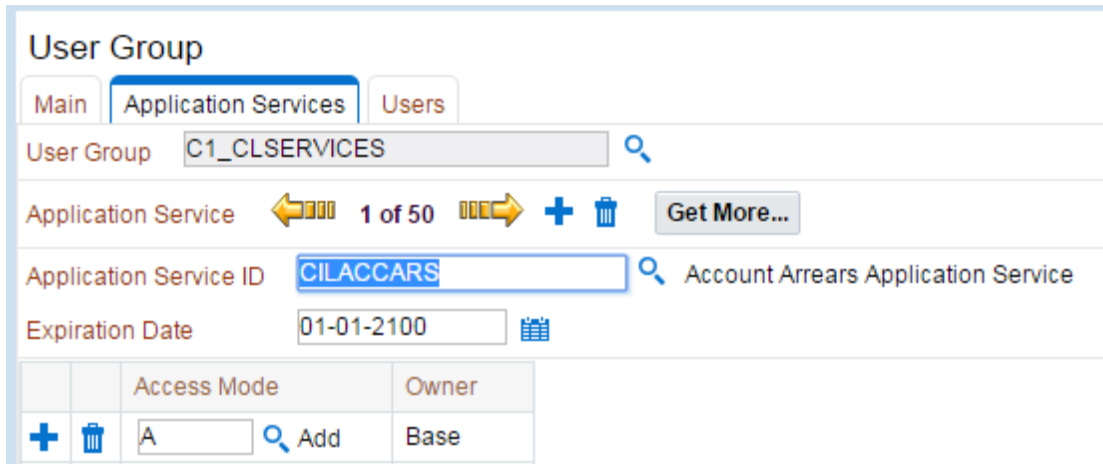
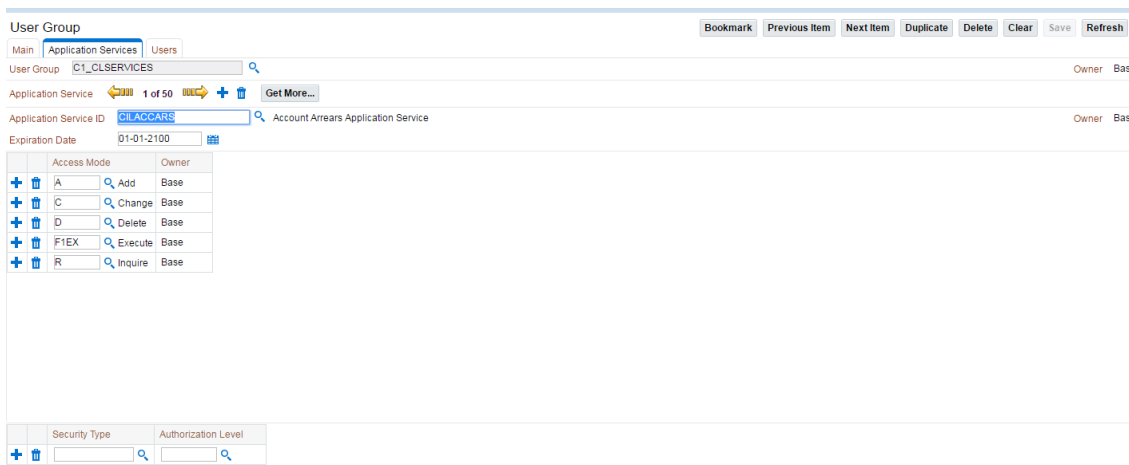
Icon	Description
	Use this icon to remove an associate between the user group and an application service.
	Use this icon to edit an existing permission.

Figure 4–16 Application Service and an Individual User Group Association




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:

Figure 4–17 Maintain Association






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




- **Expiry Date:** Date on which this Access will expire.

Icon	Description
	Use this icon to use the Date selection widget.


- **Access Mode:** Valid Access mode as defined on Application Service definition.

Icon	Description
	Use this icon to add a new Access Mode.
	Use this icon to remove an existing Access Mode from the list.
	Use this icon to find the existing Access Mode or it can be typed in.

- **Owner:** Ownership of link (see [Chapter 5.3 Data Ownership Rules](#)).
- **Security Type:** Security Type code associated with Application Service.

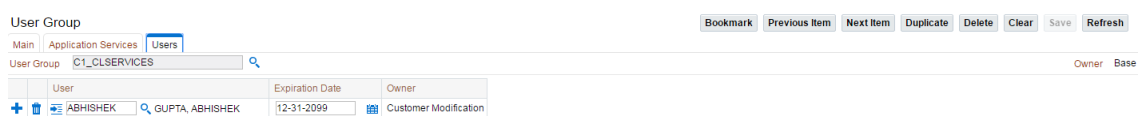
Icon	Description
	Use this icon to add a new Security Type.
	Use this icon to remove an existing Security Type from the list.
	Use this icon to find the existing Security Type or it can be typed in.





- **Authorization Level:** The Authorization Level assigned to this User Group when executing this Application Service for the Security Type.

Icon	Description
	This 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:

Figure 4–18 User Group Maintenance




User	Expiration Date	Owner
  ABHISHEK  GUPTA, ABHISHEK	12-31-2099	 Customer Modification



- **User:** This is the authorization user identifier to be connected to the user group.

Icon	Description
	This 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.

Icon	Description
	Use this icon to use the Date selection widget.

- **Owner:** Ownership of link (see [Chapter 5.3 Data Ownership Rules](#)).

Icon	Description
	Use this icon to add a new user.
	Use this icon to remove an individual user from the list.

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

4.1.10 Define Users to Data Access Groups

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 (also known as, Access Groups).
- **Data Access Groups:** Data Access Groups are tags that are attached to entities in the product to implement data security. Data Access Groups are maintained using Access Group maintenance. See the *Oracle Revenue Management and Billing Online Help* for more information about this facility.

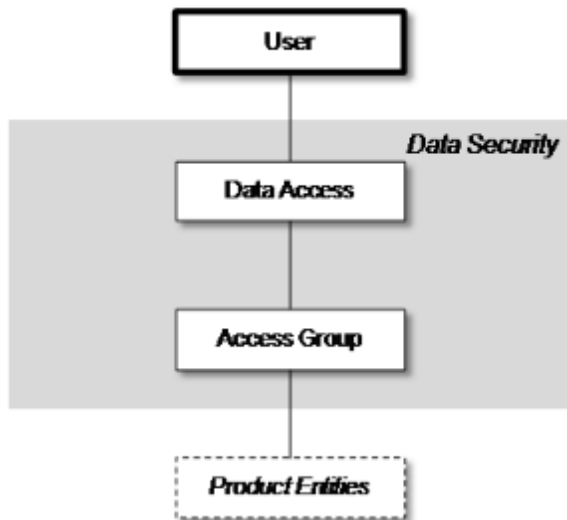
Attaching a Data Access Group to a product entity it does not automatically implement data security. Queries for that object must be altered to take into account the Data Access Group. See *Oracle Utilities SDK* for more details.

Note

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

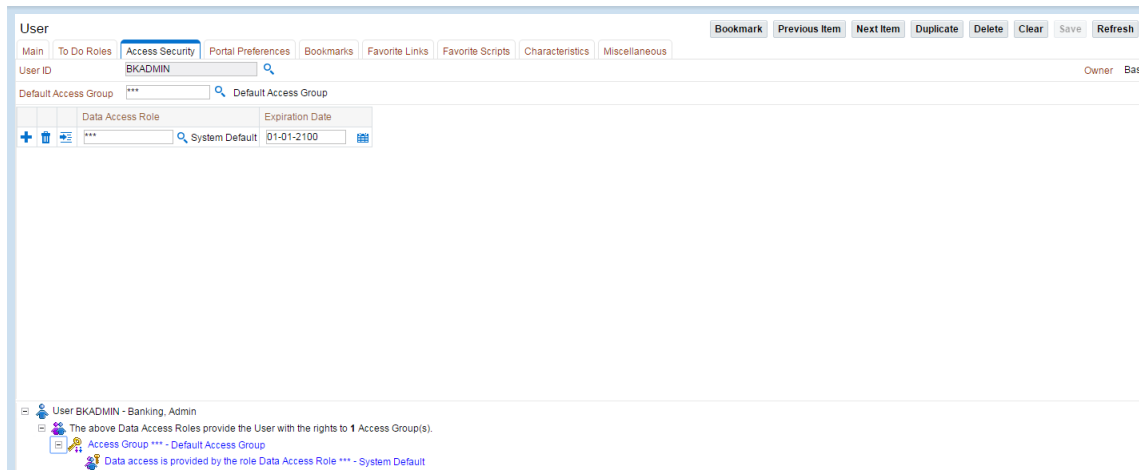
The relationships between these objects are illustrated in the figure below:

Figure 4–19 Object Relationship




To maintain the Data Access Roles and Access Groups the user has access to; navigate to the Access Security tab of the user maintenance function. The following screen appears [Figure 4–20](#).

Figure 4–20 Maintaining Data Access Roles and Access Groups






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.

Icon	Description
	This 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.

Icon	Description
	Use this icon to use the Date selection widget.

Icon	Description
	Use this icon to add a new Data Access Role.
	Use this icon to remove a Data Access Role from the list.

4.1.11 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 financial, and some are configurable). When the 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 the user by setting the appropriate value for User Enable on the User object. It has the following implications:

Table 4–2 Enable or Disable the User

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 yet keep the user data intact in database.
- **Logical deletion:** If the user needs to be deleted for any reason then setting Disable.
- **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 the user is disabled, it will apply when the user next attempts to login or when the security cache is refreshed.

4.2 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.

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. See the product functional documentation on the objects used in each of the product batch processes.

4.3 Managing Web Services Users

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 J2EE 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

Native Security support is only supported for XAI Inbound Services using the Business Adapter.

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 J2EE 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 J2EE 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. See the *Oracle Fusion Middle ware 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.

5 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 chapter outlines the various security settings available and the configurations supported.

5.1 J2EE Authentication Group

The default installation of the product includes a default authentication group (role-name) defined within the J2EE Web Application web descriptor (web.xml). This role name is used by the J2EE Web Application to link the authorized users within the product to the associated J2EE physical resources (that is, pages, configuration files) within the J2EE Web Application Server. The specification of the group in the web descriptor is in the security section. The security role is used in a number of sections of the web application descriptor. For example:

Figure 5–1 Web Descriptor

```
<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 J2EE 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. The group name should have no embedded blanks.

Table 5–1 Default Group Configuration Settings

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

- If the J2EE 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 J2EE administration group is changed after installation time,

users will need to be migrated to the new J2EE administrations group either manually, using tools provided with the security repository or J2EE Web Application Server.

5.2 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 the 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 J2EE 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 screens by setting the following configuration settings appropriately for each web component as outlined in the Server Administration Guide:

Table 5–2 Configuration Settings

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

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

- **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-CERT:** This is an advanced configuration to allow for certificated (one way or two way) to be used. See the documentation supplied with the J2EE Web Application Server for more details of the additional configuration required.

Note

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

5.3 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.
- **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.

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

5.4 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.

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

5.4.1 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 %SPLEBASE%\scripts in Windows):

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

Table 5–3 *ouaf.jmx.access.file*

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:

Table 5–4 *ouaf.jmx.password.file*

Field	Comments
User Id	Authentication user to access JMX.
Permission	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.

5.4.2 SSL based Security

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

Note

For a full description of SSL setup, see *Monitoring and Management Using JMX Technology*. See the documents at (<http://docs.oracle.com/javase/6/docs/technotes/guides/management/agent.html> .)

- Security has to be setup using the [Chapter 5.4.1 Default Simple File Based security](#) or [Chapter 5.4.3 Using Other Security Sources](#).
- A key pair and certificate need to be setup on your server. See *Monitoring and Management Using JMX Technology*. See the documents at <http://docs.oracle.com/javase/6/docs/technotes/guides/management/agent.html> or J2EE 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. The following additional system properties must be set:

Table 5–5 Additional System Properties

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

Note

Additional options are also supported as documented in Monitoring and Management Using JMX Technology. See the documents at <http://docs.oracle.com/javase/6/docs/technotes/guides/management/agent.html>

Specification of system properties for java is as per the Java Command Line. See the documents at <http://docs.oracle.com/javase/7/docs/technotes/tools/windows/java.html>

For sites using Oracle WebLogic in native mode, configuration of SSL requires configuring Oracle WebLogic to use SSL. See the documents at http://docs.oracle.com/cd/E25054_01/core.1111/e10105/sslconfig.htm and altering the startup scripts for Oracle WebLogic to include the above options.

5.4.3 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 \$SPLEBASE/splapp/config directory (or %SPLEBASE%\splapp\config directory on Windows).

In the JAAS configuration file there is a default jmxrealm that contains the default JMX Login Module. This can be changed, using custom templates, to support an alternative source for authentication. See, *Ldap Login Module* see the documents at <http://docs.oracle.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html> for information and examples of login configurations.

5.5 Menu Security Guidelines

By default, a menu option is displayed whenever the 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

5.6 Security Types

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:

Figure 5–2 Specifying Application Service

The screenshot shows the 'Menu' administration page with the 'Menu Items' tab selected. The 'Application Service' field is highlighted with a red box. The 'Access Mode' dropdown is also visible below it.

5.6 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.

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

Figure 5–3 Defining Security Types



The screenshot shows the 'Security Type' administration page. The 'Security Type' field is set to 'ADJAMT' and the 'Description' is 'Adjustment Amount'. A table lists five authorization levels with their descriptions.

Authorization Level	Description
1	Amt <= 500
2	Amt <= 5,000
3	Amt <= 10,000
4	any amount
5	frfr




At the bottom, the 'Application Service ID' is set to 'CILAADUP' with the description 'Adjustment'.

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. The Authorization Level values are free format but should be representative of the desired function. The Description is used to explain the value.

Icon	Description
	Use this icon to add a new Authorization Level.
	Use this icon to remove an existing Authorization Level from the list.

- Application Service Id - A list of associated Application Services to use this Security Code.

Icon	Description
	Use this icon to add a new Application Service.
	Use this icon to remove an existing Application Service from the list.
	Use this icon 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.

5.7 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-DFLTTS - 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.

5.8 Password Encryption

Administration passwords in the product are encrypted when used in configuration files. The utilities shipped with the product automatically encrypt passwords at configuration time. It is recommended to use these utilities to maintain passwords.

If manual intervention is required for configuration of passwords there is a manual process for generating passwords for use in configuration files.

To generate an encrypted password the following process is used:

- Use the splenviron utility to set the environment variables for the product environment.
- Set the CLASSPATH to point to the required jar files for this utility.

Windows:

```
set CLASSPATH=%CLASSPATH%;%SPLEBASE%\splapp\standalone\lib\spl-shared-4.3.0.1.0.jar;%SPLEBASE%\splapp\standalone\lib\commons-cli-1.4.jar;%SPLEBASE%\splapp\standalone\lib\log4j-1.2.17.jar;%SPLEBASE%\splapp\standalone\lib\commons-codec-1.4.jar
```

Unix/Linux:

```
export CLASSPATH==$CLASSPATH;$SPLEBASE/splapp/standalone/lib/spl-shared-4.3.0.1.0.jar; $SPLEBASE/splapp/standalone/lib/commons-cli-1.4.jar; $SPLEBASE/splapp/standalone/lib/log4j-1.2.17.jar; $SPLEBASE/splapp/standalone/lib/commons-codec-1.4.jar
```

- Execute the Cryptography class, manually providing the password to the utility. This will generate an encrypted password to the screen which can be used in the relevant configuration files. For example:

```
$ java com.splwg.shared.common.Cryptography

Enter the password to encrypt (or hit ENTER to quit):

Re-enter the password:

The encrypted password is:

ENC (+...=)
```

5.9 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 spl utility to manage the startup and shutdown of the product then the utility permissions must be altered to set the sticky bit, 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.

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

- 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.

5.10 Secure Communications (SSL)

By default, the product uses HTTP 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, configure the J2EE Web Application Server to use the SSL protocol. For Oracle WebLogic customers see *Configuring SSL* see the documents at https://docs.oracle.com/cd/E23943_01/web.1111/e13707/ssl.htm#SECMG384 in Oracle Fusion Middleware Securing Oracle Weblogic Server (see the documents at https://docs.oracle.com/cd/E23943_01/web.1111/e13707/toc.htm).

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

5.11 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.

Table 5–6 Password Management

Password Owner	Location	Comments
Online User	J2EE Authentication Source	No configuration changes. User changes password in security repository directly or indirectly using security products. Security repository is configured in J2EE Web Application Server. 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. See the <i>Server Administration Guide</i> for more details.
Web Service User	J2EE Authentication Source	No configuration changes. User changes password in security repository directly or indirectly using security products. Security repository is configured in J2EE 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. See the <i>Server Administration Guide</i> on process to change values. New Passwords need to be re-encrypted. See, Chapter 5.8 Password Encryption .
JMX Users	BSN_JMX_ SYSPASS	The default JMX user is stored in ENVIRON.INI. See the <i>Server Administration Guide</i> on process to change values. New Passwords need to be re-encrypted. See, Chapter 5.8 Password Encryption .
J2EE Administration Account	WLS_WEB_ WLSYSPASS WEB_ WLSYSPASS	The default administration users are stored in ENVIRON.INI. See the <i>Server Administration Guide</i> on process to change values. New Passwords need to be re-encrypted. See, Chapter 5.8 Password Encryption .

5.12 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.

5.13 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.

6 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.

6.1 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.

6.2 Audit Configuration

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:

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. See *Oracle Utilities SDK* and online Administration documentation for a description of programmatic implementation of Auditing.

- **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.
 - `CIPZADTA` - For backward compatibility purposes, products which use COBOL based extensions can use a COBOL version of the `DefaultTableAuditor`. It is recommended for customers to use the java version in preference to the COBOL version.

Note

It is possible to implement custom Audit handlers using the base classes as parent classes. See *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:

Figure 6–1 Maintaining Audit Information

The screenshot shows the 'Table' configuration page for table 'CI_ACCT'. The 'Audit Table' field is highlighted with a red box. Below the main configuration area, there is a table with columns for 'Field', 'Label', 'Override Label', 'Audit Delete Switch', 'Audit Insert Switch', 'Audit Update Switch', and 'Allow Custom'. The 'Audit Switch' columns are highlighted with a red box.

Field	Label	Override Label	Audit Delete Switch	Audit Insert Switch	Audit Update Switch	Allow Custom
ACCESS_GRP_CD			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ACCT_DATA_AREA			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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:

Figure 6–2 Querying Audit Information

The screenshot shows the 'Audit Query by Table/Field/Key' page. It includes search filters for 'Audited Table Name', 'Audited Field Name', and 'Creation Start Date/Time' and 'Creation End Date/Time'. Below the filters 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'.

Create Date/Time	User Name	Primary Key	Audited Field Name	Audit Action	Value Before Update	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 when 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 (that is, 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.

6.3 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:

Figure 6–3 Audit Query by User

Audit Query by User

Bookmark Clear Save Refresh

User ID Search

Audit Table Audit

Creation Start Date/Time / Creation End Date/Time /

Row Creation Date Audited Table Name Primary Key Audited Field Name Audit Action Field Value Before Update Field Value After Update

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 when 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 (that is, 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.

6.4 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 zones. 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.

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.

The information audited can be programmatically determined and which information is logged according to your requirements. See 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. See the product documentation for details of these samples.

7 Database Security

This chapter describes the details of Database Security.

7.1 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, see the *Oracle Database Security Guide*.

7.2 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.

Table 7–1 Configuration Settings to Create Variations

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 product.

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

- **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 during installation time. See the *Oracle Banking Collections Installation Guide* and *Oracle Banking Collections Database Administrator's Guide* for more information.

7.3 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.

7.4 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 Security Integration

This chapter describes the details of Security Integration.

8.1 About Security Integration

Whilst the product provides a set of security facilities natively or via the J2EE Web Application Server, it is possible to augment the security with additional security features or security products.

8.2 LDAP Integration

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

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

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

- The J2EE Web Application Server must be configured to use the external LDAP security source for authentication. See the documentation provided with the J2EE Web Application Server for more details. For Oracle WebLogic customers, see the *Configuring LDAP Authentication Providers* see the documents at http://docs.oracle.com/cd/E23943_01/web.1111/e13707/atn.htm#1216261 section of the Oracle Fusion Middleware Securing Oracle WebLogic Server Guide, see the documents at http://docs.oracle.com/cd/E23943_01/web.1111/e13707/atn.htm
- 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 at <https://support.oracle.com/>

Note

Whilst LDAP sources are the most common security repository, it is possible to use alternative security authentication sources as supported by the J2EE Web Application Server. See the documentation provided with the J2EE Web Application Server for more details.

8.3 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 J2EE Web Application Server can be configured to support Single Sign On. For more details, see *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 at <https://support.oracle.com/>.

8.4 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.

See *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 at <https://support.oracle.com/>.