Oracle® Revenue Management and Billing Analytics

Version 2.7.0.0.0

Security Guide

Revision 1.7

E63804-01

January, 2019

ORACLE

Oracle Revenue Management and Billing Analytics Security Guide

E63804-01

Hazardous Applications Notice

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

Third Party Content, Products, and Services Disclaimer

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

Preface

About This Document

This document describes how to configure security for Oracle Revenue Management and Billing Extractors and Schema and for Oracle Revenue Management and Billing Analytics.

Oracle Revenue Management and Billing Extractors and Schema is used to extract data from a source system named Oracle Revenue Management and Billing, and to subsequently populate a set of star schemas that can be used for business intelligence and analytical purposes via Oracle Revenue Management and Billing Analytics.

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

Intended Audience

This document is intended for the following audience:

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

Organization of the Document

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

Section No.	Section Name	Description
Section 1	Introduction	Explains how the security features of Oracle Revenue Management and Billing Analytics protects access to the product, its functionality and the underlying data stored and managed through the product.
Section 2	Authentication	Explains how Administration UI and Dashboard authentication is handled in Oracle Revenue Management and Billing Analytics.
Section 3	Authorization	Describes how the identified users are authorized to use specific functions and data within the product.
Section 4	Managing Security	Describes how to manage the security definitions.
Section 5	Advanced Security	Lists and describes the advanced security settings that can be configured to support various security requirements.

Section No.	Section Name	Description
Section 6	Database Security	Lists a predefined set of database users and roles shipped with the product. It also explains various database security methods that can be used to provide restricted access to the database users.
Section 7	Security Integration	Lists and describes the additional security features or security products that can be integrated with the product to augment the security setup.

Change Log

Revision	Last Update	Updated Section	Comments
1.1	October 2016	3.2, 3.4, 6.1	Changes corresponding to release 2.2.1.0.0.
1.2	February 2017	3.4	Changes corresponding to release 2.3.0.0.0 + Added a new section for Webservice authentication + Updated new roles specific to Insurance
1.3	June 2017		Changes corresponding to release 2.3.1.0.0
1.4	December 2017	3.1.1	Changes corresponding to release 2.6.0.1.0
1.5	February 2018	3.2.1	Removed Modeller for RM
1.6	May 2018	3.2.1	Added new role
1.7	January 2019	3.2.2.1	New section to add details related to Deal roles

Contents

1. Introduction

One of the key aspects of the product is security which not only confirms the identity of an individual user but, once identity is confirmed, what data and what functions that user has access to within the product. Security is one of the key features of the product architecture protecting access to the product, its functionality and the underlying data stored and managed using 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.
- **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.
- **Inbuilt Authorization Model** – Once a user is authenticated then the internal authorization model is used to determine the functions and data the user has access to within the product.

2. Authentication

This section explains the concept of authentication and details how to configure authentication for admin user interface (UI) and dashboard.

2.1 About Authentication

From a security point of view, authentication is about identification of the user. It is the first line of defense in any security solution. In simple terms, it can be as simple as the challenge-response mechanism we know as user ID and password. It can be also as complex as using digital certificates as the identification mechanism and numerous other schemes for user identification.

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

- **Authentication Scheme Support** – The 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 are 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.

2.2 Administration UI 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, Microsoft Active Directory etc). LDAP support may be direct or indirect via Identity Management software like Oracle Virtual Directory or Oracle Identity Federation.
- **SAML Based Security** – Security Assertion Markup Language (SAML) is an XML based data format for exchanging authentication and authorization information between parties.
- **DBMS Based Security** – The J2EE Web Application Server can store, manage and retrieve security information directly from a database.
- **Operating System Based Security** - The J2EE Web Application Server can store, manage and retrieve security information directly from the underlying operating system.

These security configurations can be natively supported or can be augmented with additional products. ORMBA uses the security feature provided by WLS for user authentication. For details on how to create ORMBA users and groups, refer to the Managing Administration UI and Dashboard Users and Groups section.

2.3 Dashboard Authentication

WebLogic provides the default authentication provider for Dashboards. The default authentication provider accesses user and group information stored in the LDAP server embedded in the Oracle Business Intelligence's Oracle WebLogic Server domain. The WebLogic server authenticates the users based on the credentials defined in the embedded WebLogic LDAP server.

WebLogic also supports integration with other identity management products and/or alternate directory (also known as Authentication providers). Users, Groups and related attributes can be managed and administered in WebLogic LDAP server or other external authentication providers and retrieved during the authentication process.

2.4 Webservice Authentication

ORMBA has a set of RESTful web services and while users call these web services, they are authenticated prior to granting them access. ORMBA web services support 'HTTP Basic Authentication' model wherein the caller has to provide their username and password for authentication. Users are authenticated by the WebLogic server based on the credentials available in the embedded WebLogic LDAP server.

3. Authorization

Once the authentication is configured, you need to authorize users to use specific functions and data within the product. This section explains how to authorize users to access admin user interface (UI) and dashboard. It also graphically represents the authorization model for admin UI and dashboard.

3.1 Administration UI Authorization

ORMBA has pre-defined set of application roles against which the accesses to various functions in the Administration UI are defined. These application roles can be assigned to users or enterprise groups, which provide a way to manage groups of users who have similar requirements when accessing the product.

3.1.1 Administration UI Authorization Model

The following figure describes the security authorization model of Administration UI:

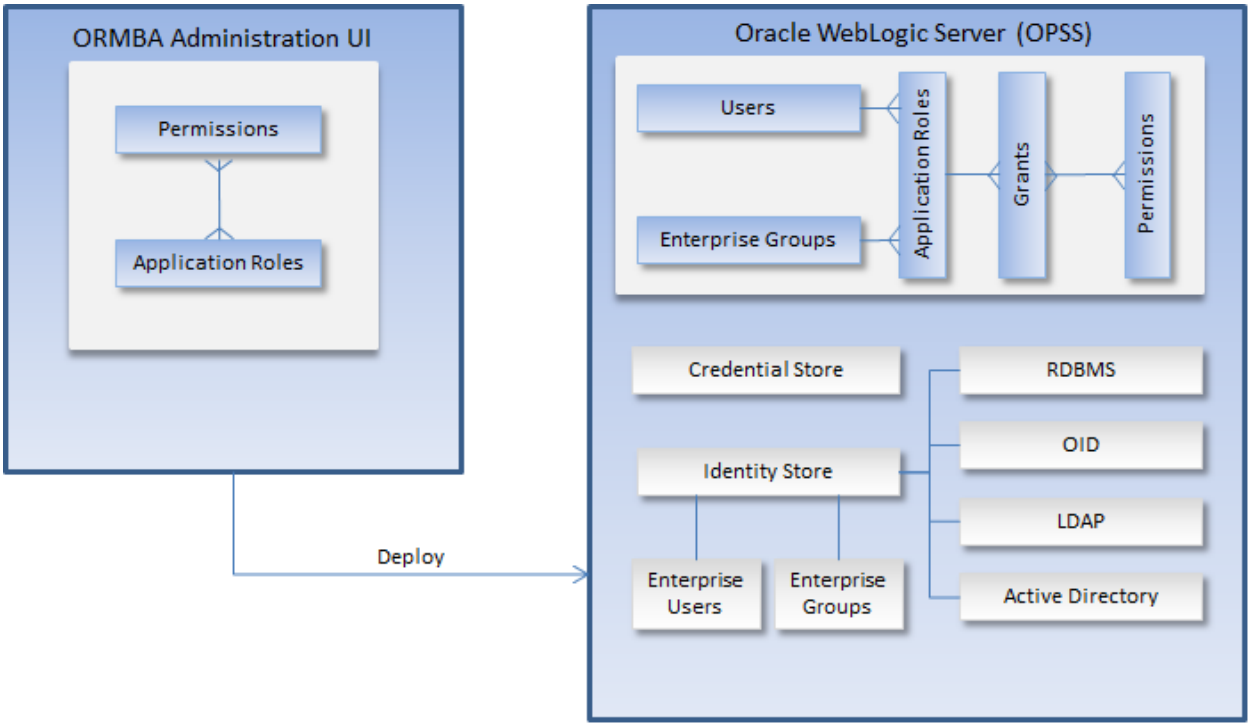

Figure 1: Administration UI Authorization Model

ORMBA Administration UI has a set of pre-defined application roles against which the authorization policies in the product are defined. These application roles need to be created in the WebLogic Administration Console of ORMBA.

3.1.2 Administration UI Application Roles

The application roles and the pages to which they provide access are listed below:

Application Role	Accessible Pages
ReleaseDetailsRole	Release Details
GlobalSettingRole	Global Settings
SourceInstanceRole	Source Instance
SubjectAreaQuestionsRole	Subject Area and Questions
TargetEntityDefinitionRole	Target Entity Definition
JobConfigurationRole	Job Configuration
JobStatusViewRole	Job Status View
DataSecurityRole	Data Security
GGParametersRole	GG Parameters
SourceTableRole	Source Table Definition
UserDefinitionRole *(Not applicable for Insurance)*	User Definition, Role Definition
WorkflowRole *(Not applicable for Insurance)*	Workflow
CharacteristicMapRole	Characteristic Map
BillAmountDistributionRole	Bill Amount Distribution
IndicativeFXRole	Indicative FX
GroupRole *(Applicable only for Insurance)*	Group Definition
TransactionLineRole *(Not applicable for Insurance)*	Transaction Line
ProspUserFieldsRole *(Not applicable for Insurance)*	Prospect User Fields
CostGroupRole *(Not applicable for Insurance)*	Cost Group Definition
CostDefinitionRole *(Not applicable for Insurance)*	Cost Definition
CrvConfigRole *(Not applicable for Insurance)*	CRV Definition

Application Role	Accessible Pages
ORMBA-AdminRole *(Not applicable for Insurance)*	All Screens except Group Definition
RepAdminAppRole	Source Instance GG Parameters Source Table Definition
ETLAdminRole	Target Entity Definition Job Configuration Job Status View
ORMB-AdminRole	Characteristic Map Bill Amount Distribution Indicative FX Transaction Line
ORMBA-HCAdminRole *(Applicable only for Insurance)*	All screens except Role Definition, User Definition, Workflow, Transaction Line, Prospect User Fields, Cost Definition, Cost Group Definition and CRV Definition

Administrators can organize enterprise users into enterprise groups, which provide a way to manage groups of users who have similar requirements when accessing the product. After deploying the product in Web Application Server, the application roles defined in the product can be mapped to the enterprise groups or directly to enterprise users from Oracle Enterprise Manager.

For users within an enterprise group to work within the product, application roles must be granted to the enterprise group. Application roles can also be granted directly to users.

3.2 Dashboard Authorization

Application Roles are the key components for defining authorization for dashboard. Dashboards also come with a pre-configured set of application roles. These application roles can be assigned to users or enterprise groups.

3.2.1 Dashboard Authorization Model

The Dashboard authorization model is similar to the Administration UI authorization model. The following figure describes the security authorization model of dashboard:

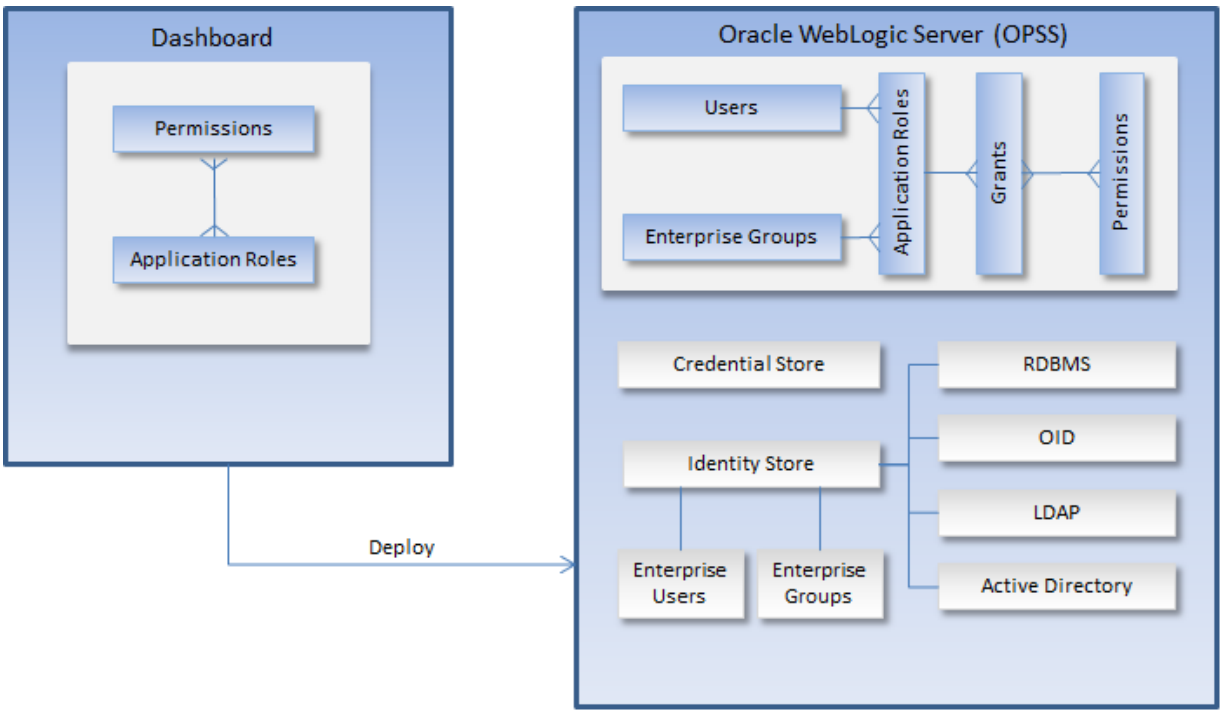

Figure 2: Dashboard Authorization Model

3.2.2 Dashboard Application Roles

ORMBA has a set of application roles (for Financial Services and Insurance domains) against which authorization policies for the dashboards are defined. The application roles for each domain and the dashboards to which they provide access are listed below:

In case of Financial Services domain:

- **ORMBAAdmin:** Can access all dashboards and Mobile App
- **ORMBARM**: Can access Relationship Manager and Deal Management dashboards
- **ORMBAITOperations**: Can access Transaction Feeds, To-Do, Billing, Contracts, and Contacts dashboards
- **ORMBAManagement**: Can access Financial Transactions and Executive Summary dashboards and Mobile App
- **ORMBAPM**: Can access Billable Charges, Product Pricing, and Modeller dashboards
- **ORMBAApprover**: Can access only Deal Management dashboard

In case of Insurance domain:

- **ORMBAAdmin:** Can access all dashboards
- **ORMBARM** (Customer Relationship Manager): Can access Broker, Customer, and Membership dashboards
- **ORMBAITOperations**: Can access Billing, Payments & Collections, Customer Contact and To-Do dashboards
- **ORMBAManagement**: Can access Financial Transactions and Executive Summary dashboards
- **ORMBAPM**: Can access Products & Charges and Broker dashboards

Note: In addition to the pre-defined Application Roles in the above list, you can also create custom roles and configure security for them. To know more about this, see the ORMBA Admin Guide.

You can map these application roles to Enterprise Groups, or directly to Enterprise Users through Oracle Enterprise Manager. To configure accessibility for dashboard users having the above-listed application roles, follow the steps below:

1. Create a user in the WebLogic Administration Console of OBIEE. For more information on how to create a user, see section 4.1.1 of this document.
2. Assign the required application role(s) to the user. For more information on how to assign a role to a user, see section 4.1.6 of this document.

3.2.2.1 Deal Management and Relationship Manager Dashboards

In case of Deal Management dashboard and Relationship Manager Dashboard, it is mandatory to create custom roles and users through ORMBA Administration UI. After creating users and assigning roles in Weblogic, follow the procedure below:

1. Log on to the ORMBA Administration UI and navigate to the Role Definition page.
2. Create role definitions by selecting each one of the following role types:
    - Administrator
    - Relationship Manager
    - Deal Approver

Note: To know more about each of the role types, and what it entitles the corresponding users, see ORMBA Deal Management User Guide.

3. Navigate to the User Definition page and create custom users with the same name as the OBIEE Weblogic username. While creating the user, select one of the custom roles created in the previous step.
4. Save the definition.

3.3 Data Level Security

ORMBA handles data from different source systems, as well as different divisions. It is imperative to restrict the data access to relevant sources or divisions, at a user level. You can restrict a user's data access at following levels:

- All data pertaining to one or more divisions
- All data pertaining to one or more source systems
- All data pertaining to a combination of division(s) and source system(s)

To enable access to data from multiple source systems or divisions, you need to add multiple entries against the same user. If you do not specify division or source system against a user, they will not have access to any data. The data level access is granted for a period, at the end of which the access is automatically revoked.

Note: By default, data level security is disabled. If needed, you can enable data level security using Global Settings page of ORMBA Administration UI.

To know more details on how to configure data level security, see ORMBA Admin UI Online Help.

4. Managing Security

This section explains how to create users and groups and how to add users to groups. It also explains how to assign application roles to users and groups.

4.1 Managing Administration UI and Dashboard Users and Groups

To manage users:

- The security repository and rules must be configured in the J2EE Web Application Server to enable authentication. Refer to *J2EE Web Application Server Administration Guide* for more information.
- Users and Enterprise Groups for the users must be defined in the security repository.
- After deployment, the application roles can be mapped to enterprise groups or enterprise users from the Oracle Enterprise Manager.

When default basic security store is used (embedded LDAP server) for WebLogic server, the users and groups can be created and managed from the WebLogic Server Administration Console. To create users and groups in other identity stores — for example, any external LDAP server — you must use the tools available with those stores.

4.1.1 Creating a User in WebLogic

To create a user:

1. Log on to the WebLogic Server Administration Console using the administrator's credentials. The **Home** page appears.
2. Click the **Security Realms** link in the **Domain Structure** section. The **Summary of Security Realms** page appears in the right pane.
3. Click the **myrealm** link in the **Name** column. The **Settings for myrealm** page appears.
4. Click the **Users and Groups** tab. The **Users and Groups** tab appears.
5. In the **Users** tab, click **New**. The **Create a New User** page appears. It contains the following fields:

- **Name**: Used to specify the user name. Note: The user name must be unique and must not include the following characters: , < > # | & ? ( ) { }. The user names are case sensitive.
- **Description**: Used to specify the description for the user.
- **Provider**: Used to indicate the authentication provider for the user. **Note:** The list will have more than one value if multiple authentication providers are configured in the security realm. You need to select the authentication provider that corresponds to the database in which you want to store the information of the user.
- **Password**: Used to specify the password for the user. Note: The password must be at least eight characters in length. Oracle recommends you to configure the Password Validation provider in the security realm after you create a domain. The Password Validation provider is configured to impose additional password composition rules.
- **Confirm Password**: Used to confirm the password that you have specified for the user.

6. Enter the name and description for the user in the respective fields.
7. Ensure that the DefaultAuthenticator option is selected from the **Provider** list.
8. Enter the password for the user in the **Password** and **Confirm Password** fields.
9. Click **OK**. The user is created and appears in the list of users.

4.1.2 Creating a Group in WebLogic

To create a group:

1. Log on to the WebLogic Server Administration Console using the administrator's credentials. The **Home** page appears.
2. Click the **Security Realms** link in the **Domain Structure** section. The **Summary of Security Realms** page appears in the right pane.
3. Click the **myrealm** link in the **Name** column. The **Settings for myrealm** page appears.
4. Click the **Users and Groups** tab. The **Users and Groups** tab appears.
5. Click the **Groups** tab. The **Groups** tab appears.
6. Click **New**. The **Create a New Group** page appears. It contains the following fields:

- Name: Used to specify the group name. Note: The group name must be unique and must not include any of the following characters: , \t < > # | & ? ( ) { }. The group names are case sensitive.
- Description: Used to specify the description for the group.
- Provider: Used to indicate the authentication provider for the group. Note: The list will have more than one value if multiple authentication providers are configured in the security realm. You need to select the authentication provider that corresponds to the database in which you want to store the information of the group.

7. Enter the name and description for the group in the respective fields.
8. Ensure that the DefaultAuthenticator option is selected from the **Provider** list.
9. Click **OK**. The group is created.

4.1.3 Adding a User to a Group

To add a user to one or more groups:

1. Log on to the WebLogic Server Administration Console using the administrator's credentials. The **Home** page appears.
2. Click the **Security Realms** link in the **Domain Structure** section. The **Summary of Security Realms** page appears in the right pane.
3. Click the **myrealm** link in the **Name** column. The **Settings for myrealm** page appears.
4. Click the **Users and Groups** tab. The **Users and Groups** tab appears.
5. In the **Users** tab, click the **<USER_NAME>** link in the **Name** column to add the user to a group. The **Settings for <USER_NAME>**page appears. It contains multiple tabs, such as General, Passwords, Attributes, and Groups. By default, the **General** tab appears.
6. Click the **Groups** tab. The **Groups** tab appears.
7. Select the check box corresponding to the group (in which you want to the user) in the **Available** list, and then click the **Move** button. The group is moved to the **Chosen** list.

8. Click **Save**. The user is added to the group.

Note: You can also add user to any other default groups of the domain to ensure that the appropriate access is available.

9. Restart the administration server to reflect the changes.

4.1.4 Adding a Group to Another Group

To add a group to one or more parent groups:

1. Log on to the WebLogic Server Administration Console using the administrator's credentials. The **Home** page appears.
2. Click the **Security Realms** link in the **Domain Structure** section. The **Summary of Security Realms** page appears in the right pane.
3. Click the **myrealm** link in the **Name** column. The **Settings for myrealm** page appears.
4. Click the **Users and Groups** tab. The **Users and Groups** tab appears.
5. Click the **Groups** tab. The **Groups** tab appears.
6. In the **Groups** tab, click the **<GROUP_NAME>** link in the **Name** column to add the group to another group. The **Settings for <GROUP_NAME>** page appears. It contains multiple tabs, such as General and Membership. By default, the **General** tab appears.
7. Click the **Membership** tab. The **Membership** tab appears.
8. Select the check box corresponding to the group (in which you want to a group) in the **Available** list, and then click the **Move** button. The group is moved to the **Chosen** list.
9. Click **Save**. The group is added to the parent group.
10. Restart the administration server to reflect the changes.

4.1.5 Deleting a User in WebLogic

To delete a user:

1. Log on to the WebLogic Server Administration Console using the administrator's credentials. The **Home** page appears.
2. Click the **Security Realms** link in the **Domain Structure** section. The **Summary of Security Realms** page appears in the right pane.
3. Click the **myrealm** link in the **Name** column. The **Settings for myrealm** page appears.
4. Click the **Users and Groups** tab. The **Users and Groups** tab appears.
5. In the **Users** tab, click the check box corresponding to **<USER_NAME>** that you want to delete. The **Delete** button is enabled.
6. Click **Delete**. The user is deleted from WebLogic Server Administration Console.

4.1.6 Assigning an Application Role to a Group or User

As already seen above, the groups and users are created in the WebLogic application server. There is a pre-defined set of roles available in the application. Once the application is deployed, you can assign application roles to groups and/or users using Oracle Enterprise Manager. To assign an application role to a group and/or user:

1. Log on to Oracle Enterprise Manager using the administrator's credentials. The Home page appears.
2. Right-click on the <WEBLOGIC_DOMAIN> link in the Target Navigation section and select Security > Application Roles from the shortcut menu. The Application Roles page appears.
3. In the Search section, select the application name (whose roles you want to assign) from the Application Stripe list.
4. Click the Search icon corresponding to the Role Name field. All roles defined in the application are listed in the grid.
5. Select the application role that you want to assign to a group and/or user and then click the Edit button. The Edit Application Role : <ROLE_NAME> page appears.
6. Click the Add button. The Add Principal dialog box appears.
7. Do either of the following:
   - To assign the application role to a Group, select **Group** from the Type list and then click the Search icon. The groups appear in the Searched Principals grid.
   - To assign the application role to a User, select **User** from the Type list and then click the Search icon. The users appear in the Searched Principals grid.
8. Select the group or user to which you want to assign the application role and then click OK. The application role is assigned to the selected group or user.

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 section outlines the various security settings available and the configurations supported.

5.1 Menu Security Guidelines

The permissions to the menu items in the product are granted to the specific application roles. A menu option is displayed for a user whenever a user is added to the application role or when the user is a member of the enterprise group which is attached to the application role.

5.2 Setting User Lockout Attributes in WebLogic

WebLogic provides a set of attributes to protect user accounts from intruders. By default, these attributes are set for maximum protection. As a system administrator, you have the option of turning off all the attributes, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked.

To set the user lockout attributes:

1. Log on to Oracle Enterprise Manager using the administrator's credentials. The Home page appears.
2. In the Change Center section, select the Lock & Edit option from the Changes drop-down list. This helps to lock a domain configuration so that you can make changes to the configuration while preventing other accounts from making changes during your edit session.
3. In WebLogic Server Administration Console, click the Security Realms link in the Domain Structure section. The Summary of Security Realms page appears in the right pane.
4. Click on the myrealm link in the Name column. The 'Settings for myrealm' page appears.
5. Ensure that the Configuration tab is selected.
6. Click the User Lockout tab. The User Lockout tab appears.
7. Modify the default values, if required.
8. Click Save. The changes are saved.
9. In Oracle Enterprise Manager, select the Activate Changes option from the Changes drop-down list. The changes are reflected on all server instances in the domain.
10. Restart the administration server to reflect the changes.

5.3 Unlocking User Accounts in WebLogic

A user account is locked when the number of consecutive invalid login attempts exceeds the threshold limit. To unlock a user account:

1. Log on to Oracle Enterprise Manager using the administrator's credentials. The Home page appears.
2. In the Change Center section, select the Lock & Edit option from the Changes drop-down list.

3. Right-click on the <DOMAIN_NAME> link in the Target Navigation section and select Security > Unlock User from the shortcut menu. A page appears.
4. Enter the name of the user whose account you want to unlock.
5. Click Save. The changes are saved.
6. Select the Activate Changes option from the Changes drop-down list. The changes are reflected on all server instances in the domain.

5.4 Configuring the Password Validation Provider in WebLogic

The Password Validation provider is automatically invoked by a supported authentication provider whenever a password is created or updated for a user. The Password Validation provider determines whether the password meets the criteria established by the composition rules, and accordingly accepts or rejects the password.

The password composition rules you can configure for the Password Validation provider include the following:

- User name policies, such as whether the password can be the same as the username
- Password length policies, such as a minimum or maximum length
- Character policies, such as the minimum or maximum number of alphabetic, numeric, or non-alphanumeric characters required in each password

To configure the Password Validation provider:

1. Log on to Oracle Enterprise Manager using the administrator's credentials. The **Home** page appears.
2. In the **Change Center** section, select the **Lock & Edit** option from the **Changes** drop-down list. This helps to lock a domain configuration so that you can make changes to the configuration while preventing other accounts from making changes during your edit session.
3. In WebLogic Server Administration Console, click the **Security Realms** link in the **Domain Structure** section. The **Summary of Security Realms** page appears in the right pane.
4. Click the **myrealm** link in the **Name** column. The **Settings for myrealm** page appears.
5. Click the **Providers** tab. The **Providers** tab appears. It contains multiple tabs, such as Authentication, Password Validation, Authorization, Adjudication, Role Mapping, Auditing, Credential Mapping, Certification Path, and Keystores. By default, the **Authentication** tab appears.
6. Click the **Password Validation** tab. The **Password Validation** tab appears.
7. Click **New**. The **Create a New Password Validation Provider** page appears.
8. Enter the name of the Password Validation provider in the respective field.
9. Select the **SystemPasswordValidator** option from the **Type** list.
10. Click **OK**. The Password Validation provider is created and appears in the **Password Validation Providers** list.
11. Click the **<Password_Validation_Provider>** link in the **Name** column. The **Settings for <Password_Validation_Provider>** page appears.
12. Click the **Provider Specific** tab. The **Provider Specific** tab appears.

13. Set the attributes in the **User Name Policies**, **Password Length Policies**, and **Character Policies** sections, as required.
14. Click **Save**. The changes are saved.
15. In Oracle Enterprise Manager, select the **Activate Changes** option from the **Changes** drop-down list. The changes are reflected on all server instances in the domain.
16. Restart the administration server to reflect the changes.

5.5 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 passwords used in the product and guidelines for changing the password values used by the product are:

- Administration UI User password: Change in J2EE Authentication Source **Note:** There are no configuration changes. User changes password in security repository directly or indirectly using security products. Security repository is configured in J2EE Web Application Server.
- Dashboard User: Change in J2EE Authentication Source **Note:** No configuration changes. User changes password in security repository directly or indirectly using security products. Security repository is configured in J2EE Web Application Server.

6. Database Security

Oracle Database supports a wide range of security configurations natively or via additional options available.

6.1 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:

- **DWADM**: This is the target schema having the data objects that contain the data warehouse data. This schema contains the star schema objects, such as facts and dimensions that contain all the data of the data warehouse.
- **MDADM**: This is the metadata schema that consists of database objects used for storing metadata of the product. For example, ETL job execution status, target tables for ETL, Oracle GoldenGate configuration details, etc.
- **MODELADM** (Optional): This is the schema used for storing the simulated models. Not required for Insurance type of installation.
- **MAPADM** (Optional): This is the schema used for ORMBA Spatial Metadata.
- **DWSTAGE**: This is the work schema used by ODI to store intermediate results.
- **Replication Schema**: This schema holds the replicated data from source system.
- **Golden Gate Schema**: This schema is used, internally, by Golden Gate for keeping the required objects for replication.

6.2 Database Permissions

Database permissions for the product need to be allocated at the role level with the role setting permissions to the schema objects. 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.

6.3 Using Transparent Data Encryption

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

Note: To implement Transparent Data Encryption, DBAs will have to execute appropriate alter statements on product tables to indicate the level of encryption. For product tables with large amounts of data, it is recommended to use the NOMAC feature to save disk space.

For more information on implementing Transparent Data Encryption, refer to *Oracle Database Security Guide.*

7. 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.

7.1 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.

To use an alternative source as a security, configure the J2EE Web Application Server to use that security source for authentication. Refer the documentation provided with the J2EE Web Application Server for more details. For Oracle WebLogic customers, refer the Configuring LDAP Authentication Providers section of *Oracle Fusion Middleware Securing Oracle WebLogic Server Guide*.

7.2 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.