

Security Guide  
Oracle Banking Liquidity Management  
Release 14.1.0.0.0  
[May] [2018]



# Table of Contents

<b>1. ABOUT THIS MANUAL.....</b>	<b>1-1</b>
1.1 INTRODUCTION.....	1-1
1.2 SCOPE.....	1-2
1.2.1 <i>Read Sections Completely</i> .....	1-2
1.2.2 <i>Understand the Purpose of this Guidance</i> .....	1-2
1.2.3 <i>Limitations</i> .....	1-2
1.2.4 <i>Test in Non-Production Environment</i> .....	1-2
<b>2. PREREQUISITE.....</b>	<b>2-3</b>
2.1 OPERATING ENVIRONMENT SECURITY.....	2-3
2.2 NETWORK SECURITY.....	2-3
2.3 ORACLE DATABASE SECURITY.....	2-3
2.3.1 <i>Oracle Banking Liquidity Management Recommended configuration</i> .....	2-3
2.4 APPLICATION SERVER SECURITY.....	2-5
2.5 THIRD-PARTY APPLICATIONS.....	2-6
2.6 CHOICE OF THE SSL CIPHER SUITE.....	2-6
2.7 CONFIGURING ORACLE BANKING LIQUIDITY MANAGEMENT.....	2-7
2.8 SECURING THE ORACLE BANKING LIQUIDITY MANAGEMENT APPLICATION.....	2-7
2.8.1 <i>Setting up Secure Flag for Cookies</i> .....	2-7
2.8.2 <i>Session time out and Token Management</i> .....	2-7
2.8.3 <i>Two-way SSL Connection</i> .....	2-7
2.8.4 <i>Securely store the credentials in CSF</i> .....	2-8
<b>3. SECURING ORACLE BANKING LIQUIDITY MANAGEMENT.....</b>	<b>3-9</b>
3.1 DESKTOP SECURITY.....	3-9
3.2 ORACLE BANKING LIQUIDITY MANAGEMENT CONTROLS.....	3-9
3.2.1 <i>Overview</i> .....	3-9
3.2.2 <i>Disable Logging</i> .....	3-9
3.2.3 <i>Audit Trail Report</i> .....	3-9
3.2.4 <i>Security Violation Report</i> .....	3-9
3.2.5 <i>Display/Print User Profile</i> .....	3-10
3.2.6 <i>Clear User Profile</i> .....	3-10
3.2.7 <i>Change User Password</i> .....	3-10
3.2.8 <i>List of Logged-in Users</i> .....	3-10
3.2.9 <i>Authentication &amp; Authorization</i> .....	3-11
3.2.10 <i>Role Based Access Controls</i> .....	3-11
3.2.11 <i>Maker – Checker</i> .....	3-11
3.2.12 <i>User Management</i> .....	3-11
3.2.13 <i>Access Enforcement</i> .....	3-11
3.2.14 <i>Privacy controls</i> .....	3-12
3.2.15 <i>Password Management</i> .....	3-12
<b>4. GENERAL INFORMATION.....</b>	<b>4-15</b>
4.1 CRYPTOGRAPHY.....	4-15
4.2 SECURITY PATCH.....	4-15
4.3 ORACLE DATABASE SECURITY SUGGESTIONS.....	4-15
4.4 ORACLE SOFTWARE SECURITY ASSURANCE - STANDARDS.....	4-16
4.5 REFERENCES.....	4-16
4.5.1 <i>Datacenter Security considerations</i> .....	4-16
4.5.2 <i>Database Security considerations</i> .....	4-16

4.5.3 *Security recommendations / practices followed for Database Environment* ..... 4-16  
4.5.4 *Common security considerations* ..... 4-16

---

# 1. About this Manual

## 1.1 Introduction

### Purpose:

This document provides security-related usage and configuration recommendations for Oracle Banking Liquidity Management. This guide may outline procedures required to implement or secure certain features, but it is also not a general-purpose configuration manual.

### Audience:

This guide is primarily intended for IT department or administrators deploying Oracle Banking Liquidity Management and third party or vendor software's. Some information may be relevant to IT decision makers and users of the application are also included. Readers are assumed to possess basic operating system, network, and system administration skills with awareness of vendor/third-party software's and knowledge of Oracle Banking Liquidity Management application.

## **1.2 Scope**

### **1.2.1 Read Sections Completely**

Each section should be read and understood completely. Instructions should never be blindly applied. Relevant discussion may occur immediately after instructions for an action, so be sure to read whole sections before beginning implementation.

### **1.2.2 Understand the Purpose of this Guidance**

The purpose of the guidance is to provide security-relevant configuration recommendations. It does not imply the suitability or unsuitability of any product for any particular situation, which entails a risk decision.

### **1.2.3 Limitations**

This guide is limited in its scope to security-related issues. This guide does not claim to offer comprehensive configuration guidance. For general configuration and implementation guidance refer to other sources such as Vendor specific sites.

### **1.2.4 Test in Non-Production Environment**

To the extent possible, guidance should be tested in a non-production environment before deployment.

Ensure that any test environment simulates the configuration in which the application will be deployed as closely as possible.

---

## 2. Prerequisite

### 2.1 Operating Environment Security

Please refer the vendor specific documentation for making the environment more safe and secured.

### 2.2 Network Security

Please refer the vendor specific documentation for making the environment more safe and secured.

### 2.3 Oracle Database Security

Please refer the Oracle Database Security specification document for making the environment more safe and secured.

#### 2.3.1 Oracle Banking Liquidity Management Recommended configuration

This section contains security recommendations for the Database used for Oracle Banking Liquidity Management Application.

Init.ora	REMOTE_OS_AUTHENT=FALSE	Authentication
Init.ora	_TRACE_FILES_PUBLIC=FALSE	Authorization
Init.ora	REMOTE_OS_ROLES=FALSE	Authorization
Init.ora	O7_DICTIONARY_ACCESSIBILITY = FALSE	Authorization
Init.ora	AUDIT_TRAIL = OS	Audit
Init.ora	AUDIT_FILE_DEST = E:\logs\db\audit	Audit

To audit sessions	SQL> audit session;	Audit
To audit schema changes	SQL> audit user;	Audit
To audit other events	SQL> AUDIT DATABASE LINK; -- Audit create or drop database links SQL> AUDIT PUBLIC DATABASE LINK; -- Audit create or drop public database links SQL> AUDIT SYSTEM AUDIT; -- Audit statements themselves SQL> AUDIT ALTER ANY ROLE by ACCESS; -- Audit alter any role statements SQL> AUDIT ALTER DATABASE by ACCESS; -- Audit alter database statements SQL> AUDIT ALTER SYSTEM by ACCESS; -- Audit alter system statements SQL> AUDIT CREATE ROLE by ACCESS; -- Audit create role statements SQL> AUDIT DROP ANY ROLE by ACCESS; -- Audit drop any role statements SQL> AUDIT PROFILE by ACCESS; -- Audit changes to profiles SQL> AUDIT PUBLIC SYNONYM by ACCESS; -- Audit public synonyms statements SQL> AUDIT SYSDBA by ACCESS; -- Audit SYSDBA privileges SQL> AUDIT SYSOPER by ACCESS; -- Audit SYSOPER privileges SQL> AUDIT SYSTEM GRANT by ACCESS; -- Audit System grant privileges	Audit

To audit the events, login through sqlplus as SYSTEM and issue the commands.

## 2.4 **Application Server Security**

Please refer the Oracle Weblogic Security specification document for making the environment more safe and secured.

Apart from the Oracle Weblogic Security specification, Oracle Banking Liquidity Management Application recommends to implement the below security specifications.

### **Support for Single Sign on (SSO)**

Oracle Banking Liquidity Management Solution supports Single sign-on capability. Ensure that the LDAP used for Oracle Banking Liquidity Management Single Sign-on deployment is certified to work with Oracle Access Manager.

Oracle Access Manager consists of the Access System and the Identity System. The Access System secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control across enterprise resources. The Identity System manages information about individuals, groups and organizations. It enables delegated administration of users, as well as self-registration interfaces with approval workflows. These systems integrate seamlessly.

*For details on configuration, refer to the document*

[https://docs.oracle.com/cd/E86317\\_01/PDF/Installation/Oracle\\_Banking\\_Liquidity\\_Management\\_SSO\\_Setup.pdf](https://docs.oracle.com/cd/E86317_01/PDF/Installation/Oracle_Banking_Liquidity_Management_SSO_Setup.pdf)

### **Support for LDAP (External Password Authentication)**

Oracle Banking Liquidity Management Solution also supports authentication through LDAP/MSAD without the use of SSO.

Depending on the value PASSWORD\_EXTERNAL in system setup parameter screen, the password will be validated with LDAP/MSAD or OBLM Application.

### **Support for SSL (Secure Transformation of Data)**

Oracle Banking Liquidity Management can be configured to enable support for SSL.

In other words, all HTTP traffic in the clear will be prohibited; only HTTPS traffic will be allowed. It is highly recommended to enable this option in a production environment, especially when WebLogic Server acts as the SSL terminator.



## 2.5 Third-party Applications

### Support for OWSM (Securing Web services)

Oracle Banking Liquidity Management supports WebLogic Server WS-Policies for enforcing security for Web/REST services. Customer can implement any Oracle WSM WS-Security policies and use them with WebLogic Web services.

The Oracle WSM policies are documented in the [Oracle Fusion Middleware Security and Administrator's Guide for Web Services](http://docs.oracle.com/cd/E21764_01/web.1111/b32511/toc.htm) <  
[http://docs.oracle.com/cd/E21764\\_01/web.1111/b32511/toc.htm](http://docs.oracle.com/cd/E21764_01/web.1111/b32511/toc.htm)>

## 2.6 Choice of the SSL cipher suite

Oracle WebLogic Server allows for SSL clients to initiate a SSL connection with a null cipher suite. The null cipher suite does not employ any bulk encryption algorithm thus resulting in transmission of all data in clear text, over the wire.

The default configuration of Oracle WebLogic Server is to disable the null cipher suite. Ensure that the usage of the null cipher suite is disabled, preventing any client from negotiating an insecure SSL connection.

Furthermore, for installations having regulatory requirements requiring the use of only 'high' cipher suites, Oracle WebLogic Server can be configured to support only certain cipher suites. The restriction can be done in config.xml of the WebLogic domain. Provided below is an example config.xml restricting the cipher suites to those supporting 128-bit symmetric keys or higher, and using RSA for key exchange.

```
....  
<ssl>  
    <enabled>true</enabled>  
    <ciphersuite>TLS_RSA_WITH_AES_256_CBC_SHA</ciphersuite>  
    <ciphersuite>TLS_RSA_WITH_AES_128_CBC_SHA</ciphersuite>  
</ssl>  
....
```

- 
- Configuration of WebLogic Server to support the above defined cipher suites might also require an additional command line argument to be passed to WebLogic Server, so that a FIPS 140-2 compliant crypto module is utilized. This is done by adding **-Dweblogic.security.SSL.nojce=true** as a JVM argument.
- The restriction on cipher suites needs to be performed for every managed server.
- The order of cipher suites is important – Oracle WebLogic Server chooses the first available cipher suite in the list, that is also supported by the client.
- Cipher suites with RC4 are enabled despite it being second best to AES. This is primarily for older clients that do not support AES (for instance, Microsoft Internet Explorer 6, 7 and 8 on Windows XP).

## 2.7 Configuring Oracle Banking Liquidity Management

This section explains the various configurations required for securing the various components of Oracle Banking Liquidity Management.

## 2.8 Securing the Oracle Banking Liquidity Management Application

The following guidelines serve to secure the Oracle Banking Liquidity Management application deployed on Oracle WebLogic Server.

### 2.8.1 Setting up Secure Flag for Cookies

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic.

Below configuration has to be ensured in weblogic.xml within the deployed application ear.

1. Cookie secure flag set to true

```
<wls:session-descriptor>  
  
    <wls:cookie-secure>true</wls:cookie-secure>  
  
    <wls:url-rewriting-enabled>>false</wls:url-rewriting-enabled>  
  
</wls:session-descriptor>
```

Always make sure Cookies are set with always Auth Flag enabled by default for WebLogic server and also recommended to apply the weblogic patch 10.3.5 for versions using below weblogic 10.3.5 to reflect the above changes.

### 2.8.2 Session time out and Token Management

Session timeout represents the event occurring when a user do not perform any action on a web site during a interval (defined in application). The event, on server side, change the status of the user session to 'invalid' (ie. "not used anymore") and instruct the Application/web server to destroy it (deleting all data contained into it). Application allows defining the session time out.

The default value for session time out is 30 minutes.

The entire subsequent request within the session will be having the Authenticated and Cross-site request forgery tokens .Every request send to the application from the browser is validated against the IsAuthenticated attribute and Cross-site request forgery token.

### 2.8.3 Two-way SSL Connection

A two-way SSL is used when the server needs to authenticate the client. In a two-way SSL connection the client verifies the identity of the server and then passes its identity certificate to the server. The server then validates the identity certificate of the client before completing the SSL handshake.

In order to establish a two-way SSL connection, need to have two certificates, one for the server and the other for client.

For Oracle Banking Liquidity Management solution, need to configure a single connector. This connector is related to SSL/TLS communication between host or browser and the branch which uses two-way authentication.

*For details on implementation of Two-way SSL process, refer to the document available for [https://docs.oracle.com/cd/E86317\\_01/PDF/Installation/Oracle\\_Banking\\_Liquidity\\_Management\\_SSL\\_Configuration.pdf](https://docs.oracle.com/cd/E86317_01/PDF/Installation/Oracle_Banking_Liquidity_Management_SSL_Configuration.pdf)*

#### **2.8.4 Securely store the credentials in CSF:**

Oracle Banking Liquidity Management application use CSF to securely store the credentials (encryption key / symmetric key) in a credentials store and the additional benefits of CSF, such as the ability to manage / operations use Oracle Fusion Middleware user interfaces / em console.

*For details on implementation of OPSS CSF, refer to the document installation / configuration documents in user manuals.*

---

## 3. Securing Oracle Banking Liquidity Management

### 3.1 Desktop Security

Please refer the vendor specific relevant sections for securing the Desktops Operating system. Also do refer the Browser specific security settings mentioned in the vendor specific docs.

Refer the client browser setting required for OBLM.

### 3.2 Oracle Banking Liquidity Management Controls

#### 3.2.1 Overview

This chapter describes the various programs available within Oracle Banking Liquidity Management, to help in the maintenance of security.

Access to the system is possible only if the user logs in with a valid ID and the correct password. The activities of the users can be reviewed by the Security Officer in the Event Log and the Violation Log reports.

#### 3.2.2 Disable Logging

It is recommended that the debug logging facility of the application be turned off, once the system is in production. This is achieved by updating the logging parameters in system setup screen.

The above described practice does not disable logging performed by the application in the database tier. This can be disabled by running the lockdown scripts provided. The lockdown scripts will disable logging across all modules and across all users in the system.

#### 3.2.3 Audit Trail Report

A detailed Audit Trail is maintained by the system on all the activities performed by the user from the moment of login. This audit trail lists all the functions invoked by the user, along with the date and time. The program reports the activities, beginning with the last one. It can be displayed or printed. The records can be optionally purged once a printout is taken. This program should be allotted only to the Security Officer.

#### 3.2.4 Security Violation Report

This program can be used to display or print the Violation Report. The report gives details of exceptional activities performed by a user during the day. The difference between the Violation Report and the Audit Trail is that the former gives details of all the activities performed by the users during the day, and the latter gives details of exceptional activities, for e.g. forced password change, unsuccessful logins, User already logged in, etc. The details given include:

- Time
- The name of the operator
- The name of the function
- The ID of the terminal

- A message giving the reason for the login

The system gives the Security reports a numerical sequence. The Security Report includes the following messages:

### 3.2.4.1 Sign-on Messages

Message	Explanation
User Already Logged In	The user has already logged into the system and is attempting a login through a different terminal.
User ID/Password is wrong	An incorrect user ID or password was entered.
User Status is Locked. Please contact your System Administrator	The user profile has been disabled due to an excessive number of attempts to login, using an incorrect user ID or password. The number of attempts could have matched either the successive or cumulative number of login failures (configured for the system).

### 3.2.5 Display/Print User Profile

This function provides an on-line display / print of user profiles and their access rights. The information includes:

- The type (customer / staff)
- The status of the profile - enabled or disabled or on-hold
- The time of the last login
- The date of the last password /status change
- The number of invalid login attempts
- The language code / home branch of the user

### 3.2.6 Clear User Profile

A user ID can get locked into the system due to various reasons like an improper logout or a system failure. The Clear User Profile function can be run by another user to reset the status of the user who got locked in. This program should be used carefully and conditionally.

### 3.2.7 Change User Password

Users can use this function to change their passwords. A user password should contain a minimum of six characters and a maximum of twelve characters (both parameterizable). It should be different from the current and two previous passwords. The program will prompt the user to confirm the new password when the user will have to sign-on again with the new password.

### 3.2.8 List of Logged-in Users

The user can run this program to see which users are in use within Oracle Banking Liquidity Management at the time the program is being run. The information includes the following:

- The ID of the terminal
- The ID of the user

- The login time

### **3.2.9 Authentication & Authorization**

First, only authorized users can access the system with the help of a unique User ID and a password. Secondly, a user should have access rights to execute a function.

The user profile of a user contains the User ID, the password and the functions to which the user has access. Oracle Banking Liquidity Management operation such as new, query etc will be enabled based on function rights available for the user. The function rights will be checked for each operation performed by the user.

Administrator can define the maximum number of unsuccessful attempts after which a User ID should be disabled. When a User ID has been disabled, the Administrator should enable it. The password of a user can be made applicable only for a fixed period. This forces the user to change the password at regular intervals thus reducing security risks.

### **3.2.10 Role Based Access Controls**

Application level access has implemented via the Security Management System (SMS) module. SMS supports “ROLE BASED” access of Screens and different types of operations.

Oracle Banking Liquidity Management Banking Solutions supports dual control methodology, wherein every operation performed has to be authorized by another user with the requisite rights.

### **3.2.11 Maker – Checker**

Application supports dual control methodology, wherein every operation performed has to be authorized by another user with the requisite rights.

### **3.2.12 User Management**

Oracle Banking Liquidity Management enables creation of users through user creation screen.

The password supplied is hashed iteratively after being appended with a randomly generated salt value. Hashing algorithm used is of SHA-2 family and above.

User privileges are maintained by Roles. Roles definition is captured via another UI Basing on these user- roles mapping the user will have access to different modules in Oracle Banking Liquidity Management.

### **3.2.13 Access Enforcement**

Access management in Oracle Banking Liquidity Management can be done in four steps.

1. Roles wise—as described above basing on the user-roles mapping, the user can access different modules in OBLM. For an example, a bank clerk will have access to customer creation, account opening, structure creation screens, but he will not have access to screen, which is for user creation.
2. Function-ID wise—here, the user can be restricted to launch even the UI on clicking on the menu list.

### **3.2.14 Privacy controls**

Tokenization mechanism is implemented in OBLM, where the token is created for every request that hit server for avoiding forgery attacks. Also, to avoid Clickjacking and frame spoofing attack OBLM have respective header and code configuration. Proper privacy control and content type has been placed.

### **3.2.15 Password Management**

Certain user password related parameters should be defined at the bank level. These parameters will apply to all the users of the system. Examples of such parameters are the number of invalid login attempts after which a user-id should be disabled, the maximum and minimum length for a password, the number of previous passwords that should not be used, the interval at which the password should be changed by every user, etc.

#### **3.2.15.1 Invalid Logins**

In Oracle Banking Liquidity Management user should specify the allowable number of times an invalid login attempt is made by a user. Each user accesses the system through a unique User ID and password. While logging on to the system, if either the User Id or the Password is wrong, it amounts to an invalid login attempt.

By default, the allowable number of cumulative invalid attempts is six, and the allowable number of consecutive invalid attempts is three. These default values can be changed and specify the allowable number of attempts in each case. An allowable number for cumulative attempts are between 6 and 99, and for consecutive (successive) attempts are between 3 and 5.

When authentication of credentials is unsuccessful due to an incorrect user ID, then the user id will not be logged in the audit logs. In case the user id is correct and the password is wrong, the attempt is logged in the audit log and the successive and cumulative failure count is incremented. When the user id and password are correct, this is logged into the audit logs.

#### **3.2.15.2 Specifying Parameter**

##### **Dormancy Days**

Oracle Banking Liquidity Management allows you to automatically disable the profile of all the users who have not logged into the system for a pre-defined period of time. A user ID is considered dormant if the difference between the last login date and the current date is equal to or greater than the number of 'Dormancy Days' that has been specified. This is reckoned in calendar days i.e. inclusive of holidays. All dormant users (whose home branch is same as the current branch) are disabled during the end of day run at the current branch.

#### **3.2.15.3 Specifying Parameters for User Passwords**

##### **Password Length (characters)**

The range of length (in terms of number of characters) of a user password can be set. The number of characters in a user password is not allowed to exceed the maximum length, or fall below the minimum length that has been specified.

The minimum length defaults to 8, and the maximum length to 15. The defaults values can be changed and specify the required range. The length can specify a minimum length between 6 and 15 characters, and a maximum length between 10 and 15 characters. The minimum length that specified must not exceed the maximum length that have specified.

### **Force Password Change after**

The password of a user can be made valid for a fixed period after which a password change should be forced. After the specified number of days has elapsed for the user's password, it is no longer valid and a password change is forced. The number of calendar days defined will be applicable for a password change of any nature - either through the 'Change Password' function initiated by the user or a forced change initiated by the system. The system defaults to a value of 30, which can be changed. The number of days can be between 15 and 180 days,

### **Password Repetitions**

The number of previous passwords that cannot be set as the new current password can be configured, when a password change occurs. The system defaults to a value of three (i.e., when a user changes the user password, the user's previous three passwords cannot be set as the new password). The default value can be changed and it can specify a number between one and five.

### **Minimum Days between Password Changes**

The minimum number of calendar days that must elapse between two password changes can be configured. After a user has changed the user password, it cannot be changed again until the minimum numbers of days you specify here have elapsed.

### **Intimate Users (before password expiry)**

The number of working days before password expiry can be configured, which is used to display a warning message to the user. When the user logs into the system (the stipulated number of days before the expiry date of the password), a warning message will continue to be displayed till the password expires or till the user changes it. By default, the value for this parameter is two (i.e., two days before password expiry).

## **3.2.15.4 Placing Restrictions on User Passwords**

Application allows placing restrictions on the number of alpha and numeric characters that can be specified for a user password.

### **Maximum Consecutive Repetitive Characters**

The maximum number of allowable repetitive characters occurring consecutively, in a user password can be specified. This specification is validated whenever a user changes the user password, and is applicable for a password change of any nature - either through the 'Change Password' function initiated by the user or a forced change initiated by the system.

### **Minimum Number of Special Characters in Password**

Application allows defining minimum number of special characters allowed in a user password. The system validates these specifications only when a user chooses to change the password. Following is the default value application used:

Minimum No of Special Characters = 1



### **Minimum Number of Numeric Characters in Password**

Likewise, application allows defining the minimum number of numeric characters allowed in a user password. The system validates the password only when a user chooses to change his password. Following is the default value used:

Minimum No of Numeric Characters = 1

### **Minimum Number of Lower Case Characters in Password**

The minimum number of lowercase characters allowed in a user password also can be configured. The allowed lower case characters are from the US-ASCII character set only. The system validates these specifications only when a user chooses to change the password

Following is the default value used:

Minimum No of Lower Case Characters = 1

### **Minimum Number of Upper Case Characters in Password**

The minimum number of upper case characters allowed in a user password can be configured. The allowed upper case characters are from the US-ASCII character set only. The system validates these specifications only when a user chooses to change the password.

Following is the default values used:

Minimum No of Upper Case Characters = 1

---

## 4. General Information

### 4.1 Cryptography

Oracle Banking Liquidity Management uses cryptography to protect the sensitive data.. It uses Hashing algorithm while storing user passwords. SHA-2 family hashing algorithm is used for the purpose. SHA-256 algorithm produces 32 bytes hash value.

For encryption, AES, which is considered to be of gold standard, is used. It produces a key size of 256 bits when it comes to symmetric key encryption.

### 4.2 Security patch

Security patches needs to be applied whenever it's available for the applicable product version.

### 4.3 Oracle Database Security Suggestions

#### Access Control

Database Vault (DV) Provides enterprises with protection from the insider threats and in advantage leakage of sensitive application data. Access to application data by users and administrators is controlled using DV realms, command rules and multi factor authorization. DV also address Access privilege by separating responsibilities.

#### Data Protection

Advance Security provides the most advance encryption capabilities for protecting sensitive information without requiring any change to the application. TDE is native database solution that is completely transparent to the existing applications.

Advance Security also provides strong protection for data in transit by using network encryption capabilities. Features like Easy to deploy, Ensure secure by default to accept communication from client using encryption, Network encryption using SSL/TLS.

#### Oracle Secure Backup (OSB)

OSB is tightly integrated with the Oracle database, hence provides optimal security and performance, eliminating backup of any associated database UNDO data. Supports Comprehensive tape backup solutions for Oracle database and file systems. Provides single point of control for enterprise-wide tape backup and associated encryption key.

#### Monitoring and Compliance

Audit Vault (AV) transparently collects and consolidate audit data from multiple databases across the enterprise, does provide valuable insight into who did what with which data & when including privilege users. The integrity of the audit data is ensured using controls including DV, Advance Security. Access to AV data is strictly controlled. It also does provide graphical summaries of activity causing alerts, in addition database audit setting are centrally managed and monitored.

## **4.4 Oracle Software Security Assurance - Standards**

Every acquired organization must complete the Mergers and Acquisitions (M&A) Security Integration process. The issues identified during this review must be addressed according to the agreed upon M&A remediation plan. The acquired organization must complete SPOC assignments and plan integration of O SSA methodologies and processes into its SDLC.

## **4.5 References**

### **4.5.1 Datacenter Security considerations**

Please refer to the following links to understand Datacenter Security considerations

[http://docs.oracle.com/cd/B14099\\_19/core.1012/b13999/rectop.htm](http://docs.oracle.com/cd/B14099_19/core.1012/b13999/rectop.htm)

### **4.5.2 Database Security considerations**

Please refer the below links to understand more on Database Security considerations recommended to be followed

<http://www.oracle.com/us/products/database/security/overview/index.html>

<http://www.oracle.com/technetwork/database/security/twp-security-checklist-database-1-132870.pdf>

### **4.5.3 Security recommendations / practices followed for Database Environment**

Please refer the below mentioned links to understand more on Security recommendations / practices followed for Database Environment

[http://docs.oracle.com/cd/B28359\\_01/network.111/b28531/guidelines.htm](http://docs.oracle.com/cd/B28359_01/network.111/b28531/guidelines.htm)

### **4.5.4 Common security considerations**

Please refer below links to understand some of the common security considerations to be followed

[http://docs.oracle.com/cd/B14099\\_19/core.1012/b28654.pdf](http://docs.oracle.com/cd/B14099_19/core.1012/b28654.pdf)

[http://docs.oracle.com/cd/E14899\\_01/doc.9102/e14761/tuningforappserver.htm](http://docs.oracle.com/cd/E14899_01/doc.9102/e14761/tuningforappserver.htm)

[http://docs.oracle.com/cd/E13222\\_01/wls/docs81b/lockdown/practices.html](http://docs.oracle.com/cd/E13222_01/wls/docs81b/lockdown/practices.html)

[http://docs.oracle.com/cd/E23943\\_01/web.1111/e14529/security.htm](http://docs.oracle.com/cd/E23943_01/web.1111/e14529/security.htm)

<http://www.oracle.com/us/solutions/oos/weblogic-server/overview/index.html>



Security Guide  
[May] [2018]  
Version 14.1.0.0.0  
Oracle Financial Services Software Limited  
Oracle Park  
Off Western Express Highway  
Goregaon (East)  
Mumbai, Maharashtra 400 063  
India

Worldwide Inquiries:  
Phone: +91 22 6718 3000  
Fax:+91 22 6718 3001  
[www.oracle.com/financialservices/](http://www.oracle.com/financialservices/)

Copyright © 2017, 2018, Oracle and/or its affiliates. All rights reserved.

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

**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.

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.

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.