Oracle® Banking Treasury Management

Security Guide

Release 14.7.6.0.0
G32240-01
April 2025

Oracle Banking Treasury Management Security Guide, Release 14.7.6.0.0

G32240-01

Contents

Preface

This topic contains the following sub-topics:

Purpose

This document provides security-related usage and configuration recommendations for Oracle Banking Treasury 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 Treasury 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 Treasury Management.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to make sure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

For more information, see these Oracle Banking Treasury Management resources:

- *Oracle Banking Treasury Management Release Notes*
- *Oracle Banking Treasury Management Installer Index*
- *Oracle Banking Treasury Management Installer Prerequisite*

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

The acronyms and abbreviations are listed in this below table:

Table Acronyms and Abbreviations

Abbreviations or Acronyms	Definition
DV	Derivatives
ETD	Exchange Traded Derivatives
FX	Foreign Exchange
MM	Money Market

Table (Cont.) Acronyms and Abbreviations

Abbreviations or Acronyms	Definition
OBTR	Oracle Banking Treasury Management
ODT	Open Development Tool
OT	Over the Counter Options
SE	Securities
SR	Securities Repo

1
Prerequisite

This topic contains following sub-topics:

1.1 Operating Environment Security

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

1.2 Network Security

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

1.3 Oracle Database Security

Please refer the *Oracle Database Security specification* document for making the environment more safe and secured.
This topic contains following sub-topics:

1.3.1 Recommended configuration

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

Table 1-1 Recommended Configuration

Configuration	Configuration	Configuration
Init.ora	REMOTE_OS_AUTHENT=FALSE	Authentication
Init.ora	_TRACE_FILES_PUBLIC=FALSE	Authorization
Init.ora	REMOTE_OS_ROLES=FALSE	Authorization

Table 1-1 (Cont.) Recommended Configuration

Configuration	Configuration	Configuration
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.

1.4 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, Application recommends to implement the below security specifications.

1. **Support for Single Sign on (SSO)**
   Oracle Banking Treasury Management Solution supports Single sign-on capability with SAML (Security Assertion Markup Language) authentication. Ensure that the LDAP used for Oracle Banking Single Sign-on deployment with SAML (if SAML validation opted) 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 the document *FCUBS_V.UM_OAM_Integration_Enabling_SSO.zip*.

2. **Support for LDAP (External Password Authentication)**
   Also supports authentication through LDAP/MSAD without the use of SSO.

   Depending on the value of the property EXT_USERLOGIN in fcubs.properties file the length of userid field in login screen changes. If the value is **Y** then user is able to input up to 30 characters in userid field. Otherwise userid field allows only 12 characters.

   Depending on the value PASSWORD_EXTERNAL in fcubs.properties file, the password is validated with LDAP/MSAD or FCUBS Application.

   For details on configuration of LDAP, refer the *Universal Banking Installation Guide document (Sec 1.4).*

3. **Support for SSL (Secure Transformation of Data)**
   The Installer allows a deployer to configure the application such that all HTTP connections to the application are over SSL/TLS. In other words, all HTTP traffic in the clear is prohibited; only HTTPS traffic is allowed. It is highly recommended to enable this option is a production environment, especially when WebLogic Server acts as the SSL terminator.

   For details on configuration of SSL, refer the *Installation Guide documents - Weblogic Configuration.pdf* for Weblogic and *Websphere_Configurations.pdf* for WebSphere)

4. **Support for SMTPS (Mail communication)**
   Also mail session configuration required in Application server. Sample details for creating a mail session are listed below:

   - Name: FCUBSMailSession
   - JNDI Name: mail/FCUBSMail (The same need to be maintained in property file creation.)
   - Java Mail Properties for SMTPS protocol:
   - mail.host=<HOST_MAIL_SERVER>
   - mail.smtps.port=<SMTPS_SERVER_PORT>
   - mail.transport.protocol=smtps

- mail.smtps.auth=true
- mail.smtps.host==<HOST_SMTPS_MAIL_SERVER>

For details on configuration of Mail Session process, refer the document < *Resource_Creation_WL.doc for weblogic or Resource_Creation_WAS.doc for websphere* >.

5. **Support for Securely store the credentials in CSF**
   Product supports to store encryption key (Symmetric key) store in secure credential storage area.

   To support CSF, OPSS component should be available in the application server domain.

   Installer allows administrator to enable CSF component to the application. If CSF component enabled, then the application look into encryption key in CSF framework and get the value.

   The default CSF option is enabled for the application.

1.5 Third-party Applications

Support for OWSM (Securing Web services)

Oracle Banking Treasury Management supports the WebLogic Server WS-Policies for enforcing security for Web 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 https://docs.oracle.com/cd/E21764_01/web.1111/b32511/toc.htm

1.6 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_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 old clients that do not support AES.

1.7 Securing the Application

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

1. **Setting up Secure Flag for Cookies**:
   If the secure flag is set on a cookie, then browsers do not submit the cookie in any requests that use an unencrypted HTTP connection, there-by 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.

   a. 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. **Credential Over mail**:
   To enable this feature mail server details needs to be provided at the time of property file creation. Below are the required parameters:

   - Host Server
   - User ID
   - User Password
   - JNDI Name

3. **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** (that is, **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 has 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.

4. **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 solutions, 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 *FLEXCUBE < SSL_OR_TLS_ Configuration.doc>*.

5. **Securely store the credentials in CSF**:
Application uses 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.

1.8 Securing the Gateway Services

This topic contains following sub-topics:

1.8.1 Overview

Different applications deployed on disparate platforms and using different infrastructure need to be able to communicate and integrate seamlessly with Oracle Banking Treasury Management in order to exchange data. The Oracle Banking Treasury Management Integration Gateway caters to these integration needs.

The integration needs supported by the Gateway can be broadly categorized from the perspective of the Gateway as follows:

- Inbound application integration – used when any external system needs to add, modify or query information within application.
- Outbound application integration – used when any external system needs to be notified of the various events that occur within application.

1.8.2 External System Maintenance

An external system needs to be defined that communicates with the Integration Gateway. Below are the details requiring inputting while creating the external system.

Table 1-2 External System Maintenance

Field	Description
External System	Specify a name for the external system. This should be the same as the Source in an incoming message.
Description	Specify a brief description for the External System.

Table 1-2 (Cont.) External System Maintenance

Field	Description
Request	A way needs to be defined in which the external system should correlate its request message with the response message. Message ID can be chosen of a request message as the Correlation ID in the response message. Alternatively, user can choose Correlation ID of a request message and maintain it as the Correlation ID of the corresponding response message.
Request Message	User can choose the Request message to be **Full Screen** or **Input Only**. If you select **Full Screen** as the request message, the response message also displays **Full Screen**.
Response Message	User can choose the Response message to be **Full Screen** or **Record Identification Msg**.
Default Response Queue	You can define a response queue for each of the In Queue's through which the External System communicates with application. Define a valid queue name as the Default Response Queue.
Dead Letter Queue	If the messages received are non-readable, such messages are directed to Dead Letter Queue defined for the external system.
XSD Validation Required	Select this box to indicate if the request message should be validated against its corresponding XSD.
Register Response Queue Message ID	Select this box to indicate if the message ID provided by the Response Queue should be logged when a response message is posted into the queue.

1.8.3 Accessing Services and Operations

In a message it is mandatory to maintain a list of Service Names and Operation Codes. This information is called Gateway Operations.

A combination of every such Service Name and Operation Code is mapped to a combination of Function ID and Action. Every screen in Oracle Banking Treasury Management is linked with a function ID. This information is called Gateway Functions.

User can gain access to an external system using the Gateway Functions. The Function IDs mapped in Gateway Functions should be valid Function IDs. Hence, for every new Service or Operation being introduced, it is important that you provide data in Gateway Operations and Gateway Functions.

1.8.4 Gateway Password Generation Logic for External System Authentication

As a secure configuration password authentication should be enabled for the external system maintained. The same can be verifying in External system detail screen level.

Once these features enable, system validates for Encrypted password as part of every request sent by the External System.

The Message ID which is present as part of the header in Request XML, is considered as hash. External System generates an unique Message ID, which is functional mandatory field in the header. Create a Message Digest with SHA-512 algorithm.

The hash created from the previous step and the password in clear text together is encrypted in DESede encryption method. Apply Base64 encoding to encrypted value and send to the gateway.

2

Securing Oracle Banking Treasury Management

This topic contains following sub-topics:

2.1 Desktop Security

Please refer the *vendor specific relevant sections for securing the DeskTops Operating system*. In addition, do refer the *Browser specific security settings mentioned in the vendor specific docs.*
Refer the *client browser setting required* for FCUBS.

2.2 Oracle Banking Treasury Management Controls

This topic contains following sub-topics:

- Password Management

2.2.1 Overview

This topic describes the various programs available within application, 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.

2.2.2 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 property file of the application using the Installer.

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 disable the logging across all modules and across all users in the system.

2.2.3 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.

2.2.4 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 example, forced password change, unsuccessful logins, User already logged in, and so on. 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:

Sign-on Messages

Table 2-1 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).

2.2.5 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

2.2.6 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.

2.2.7 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 prompts the user to confirm the new password when the user has to sign-on again with the new password.

2.2.8 List of Logged-in Users

The user can run this program to see which users are in use within application 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

2.2.9 Change Time Level

Time levels have to be set for both the system and the users. Ten time levels are available, 0 to 9. Restricted Access can be used to set the Users time level. The Change Time Level function can be used to do the same for the branch. A user is allowed to sign-on to the system only if his/her time level is equal to or higher than the system time level.

This concept is useful because timings for system access for a user can be manipulated by increasing the system time level. For example, the End of Day operators could be allotted a time level of 1, and the users could be allotted a time level of 0. If the application time-level is set at 1 during End of Day operations, only the End of Day operators are granted with access to the application. Access is denied to the other users.

2.2.10 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. Operations such as new, copy, query, unlock, and so on are enabled based on function rights available for the user. The function rights are 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. Further, Administrator can define passwords that could be commonly used by a user as Restrictive Passwords at the user, user role and bank level. A user cannot use any password that is listed as a Restrictive Password at any of these levels.

2.2.11 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.

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

2.2.12 Masking

Masking Personally Identifiable Information (PII) in scoped function ID's are enhanced to display masked or unmask values depending on the user definition. Masking personally identifiable information is based on the policies created in database. In FLEXCUBE Enterprise Limits & Collateral Management System masking can be achieved through following steps:

1. Factory shipped personal identifiable information (PII) of FLEXCUBE Enterprise Limits & Collateral Management provided and by default these are available in data store.
2. Masking Maintenance
    a. Bank User can maintain the Masking details using Masking Maintenance.
    b. Alternatively, Data controller can execute below given sample script to apply default masking maintenance for factory shipped PII. Bank user can modify / remove masking maintenance using step 2a for PII fields.

Please refer the below sample script for Mask Maintenance:

```
DECLARE
P_ERRCODE VARCHAR2(200);
BEGIN
     P_ERRCODE:=NULL;
     SMPKS_MASK_TBLCOL.PR_PROCESS_PII_FIELDS(P_ERRCODE);
END;
/
```

3. Policy Creation
   a. FLEXCUBE Universal Banking Solutions used DBMS_REDACT package to apply masking on PII fields.
   b. Data controller can execute below sample script to create REDACTION policies on PII fields. Please refer the below sample script for Policy Creation.

```
DECLARE
P_ERRCODE VARCHAR2(200);
P_BRANCH VARCHAR2(10) :='000'; -- Initialize to proper branch
BEGIN
     GLOBAL.PR_INIT(P_BRANCH);
     P_ERRCODE := NULL; SMPKS_MASK_TBLCOL.PR_PROCESS_JOB
(P_ERRCODE => P_ERRCODE );
END;
```

> **Note:**
>
> Masking / Redaction is part of Oracle Advanced Security, which is a separately licensed Enterprise Edition option.

2.2.13 Granular Access

Customer and Customer Account maintenance, transaction restricted to users based on the access group restriction attached at user level for the scoped function IDs. User is not able to query, view, create or amend data based on access group restriction.

2.2.14 Right to be forgotten

Personally Identifiable Information (PII) of both closed Users and Customers are permanently anonymized. Once PII information are anonymized corresponding Users and Customers cannot be queried from application. Right to be forgotten is processed based on the number of days to forget the customer and on the customer’s request.

2.2.15 Access controls like branch level

User can indicate the branches from where a user can operate in the **Restricted Access** screen (function-ID).

2.2.16 Maker – Checker

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

2.2.17 User Management

Application enables creation of users through SMDUSRDF UI. On authorization of the newly created user, the credentials are automatically mailed to the user's email id. This reduces the risk of password been known to the administrator, who creates users for the bank.

User is forced to change the password on first login. 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. These roles are mapped to a user in the SMDUSRDF UI. Basing on these user-roles mapping the user has access to different modules in Application.

2.2.18 Access Enforcement

Access management can be done in four steps.

1. **Branch level** - In such a case the user cannot view even the menu list when he tries to login into the restricted branch. Thus, no transactions could be performed.
2. **Roles wise** - As described above basing on the user-roles mapping, the user can access different modules in the application. For an example, a bank clerk has access to customer creation, account opening, term-deposits opening and liquidation screens, but he do not has access to SMDUSRDF UI, which is for user creation.
3. **Function-ID wise** - Here, the user can be restricted to launch even the UI on clicking on the menu list.
4. **Product/ Account class wise** - Here, the user can be prevented access to certain account classes or products. This disables him from creating any accounts or transactions using those prevented account class and product respectively.

2.2.19 Privacy controls

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

2.2.20 Password Management

Certain user password related parameters should be defined at the bank level. These parameters are applied 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, and so on.

This topic contains following sub-topics:

- Invalid Logins

- Specifying Parameter
- Specifying Parameters for User Passwords
- Placing Restrictions on User Passwords
- Password Restrictions

2.2.20.1 Invalid Logins

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 is not 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.

2.2.20.2 Specifying Parameter

Dormancy Days

Application 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.

2.2.20.3 Specifying Parameters for User Passwords

Table 2-2 Parameters

Parameters	Description
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.

Table 2-2 (Cont.) Parameters

Parameters	Description
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 are 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 (that is, 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 is continued to display till the password expires or till the user changes it. By default, the value for this parameter is two (that is, two days before password expiry).

2.2.20.4 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.

Table 2-3 Placing Restrictions on Passowrds

Restrictions	Description
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.

Table 2-3 (Cont.) Placing Restrictions on Passowrds

Restrictions	Description
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

2.2.20.5 Password Restrictions

Application allows defining a list of passwords that cannot be used by any user of the system in the bank. This list, called the Restrictive Passwords list can be defined at three levels:

- At the bank level (applicable to all the users of the system)
- At the user role level (applicable for all the users assigned the same role)
- At the user level (applicable for the user)

2.3 General Information

This topic contains following sub-topics:

2.3.1 Cryptography

Applcation 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-512 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.

2.3.2 Security patch

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

2.3.3 Oracle Database Security Suggestions

Table 2-4 Oracle Database Security Suggestions

Suggestions	Description
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.

Table 2-4 (Cont.) Oracle Database Security Suggestions

Suggestions	Description
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.

2.3.4 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 OSSA methodologies and processes into its SDLC.

2.3.5 References

Datacenter Security considerations

Please refer to the following links to understand Data center Security considerations:
http://docs.oracle.com/cd/B14099_19/core.1012/b13999/rectop.htm

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

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

Common security considerations

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

- 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/E23943_01/web.1111/e14529/security.htm
- http://www.oracle.com/us/solutions/oos/weblogic-server/overview/index.html