Security Practice Guide

Release 12.1.0.0.0

Oracle FLEXCUBE Private Banking

JUN 2015

ORACLE

FINANCIAL SERVICES

Revision History

Version	Modification Date	Details
1.0	Mar 2009	Collection of best practices used in deployment based on FCPB team experience and inputs from Oracle documents
1.1	May 2009	Changes based on review comments by Security Evaluations Group
1.2	Jul 2011	Minor corrections to remove version specific details
1.3	April 2012	Minor corrections to remove version specific details
1.4	Jul 2013	Minor corrections to remove version specific details
1.5	Jan 2014	FCPB Application Security Hardening section updated and Additional Security Hardening section added

Table of Contents

1. Introduction

Oracle FLEXCUBE Private Banking is a web based wealth management application that provides a single platform to plan, record, track and manage the overall wealth of a customer, across a range of asset classes and instruments including Equity, Fixed Income, Mutual funds, Insurance, Structured Products, Real Estate, PMS, Collectibles like Art, Deposits & Loans. The product enables a unified view and analysis of the overall wealth of the customer.

FCPB being an internet and intranet facing application can face security threats from various internal and external sources within the financial institution. While the internet banking channel has always been exposed to the vulnerabilities originating from the internet via traditional threats and attacks, the internal breakdown of controls and measures is also responsible for critical information being available exposed to un-authorized users.

This document aims to serve as a best practices guide for securing the FCPB environment. It covers security of FCPB deployment infrastructure and application security. This document is not a general introduction to environment tuning, and we assume that our readers are experienced IT professionals, with an understanding of FCPB's deployment architecture. To take full advantage of the information covered in this document, we recommend that you have a basic understanding of system administration, internet architecture, relational database concepts, SQL, and an understanding of FCPB deployment.

Structure of This Document

This document provides guidance for setting up security for FCPB system beyond application security. The intent of this document is to provide information about securing the overall infrastructure of a deployed FCPB system.

- Chapter 1 "Introduction": introduces the document.
- Chapter 2 "Glossary" or terms and acronyms used in the document
- Chapter 3 "Security Model": discusses required reading and gives a conceptual overview of security issues. Individuals and groups who may be tasked with setting security policy as well as ensuring compliance and adherence to industry best practices should find this section useful.
- Chapter 4 "Securing Network Infrastructure": discusses different approaches to network infrastructure security. Network and security administrators (or other individuals tasked with network security) will find this section to be a useful guideline to securing the supporting network of an FCPB environment.
- Chapter 5 "Securing FCPB Web Server": gives solutions and configurations for securing the web server environment
- Chapter 6 "Securing Oracle TNS Listener" & Chapter 7 "Securing Oracle Database" cover security related to listener configurations and database setup
- Chapter 8 "Securing the Desktop" identifies best practices in configuring end user desktops
- Chapter 9 "Securing the Operating Environment": this section details guidelines for periodic operational activities on the hardware environment hosting FCPB
- Chapter 10 "FCPB Application Security Hardening": additional practices for application security

2. Glossary

Acronym	Description
Oracle FCPB	Oracle FLEXCUBE Private Banking
JEE	Java Enterprise Edition
HTTP(S)	Hyper Text Transfer Protocol (Secured)
SSL	Secured Socket Layer
TCP	Transmission Control Protocol
IDS	Intrusion Detection System
RPS	Reverse Proxy Server
NFS	Network File System
IE	Internet Explorer
NIS	Network Information Service
JS	JavaScript
JSP	Java Server Pages
DMZ	Demilitarized Zone

3. Security Model

Required Reading

There are a number of books, publications and white papers on security that a security administrator should consult to get a comprehensive understanding of how to secure a site. At a minimum, please download and read *Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices* published by Internet Security Alliance from http://www.isalliance.org.

The document is an excellent starting guide for security administrators to ensure that basic security policies and practices are observed within an organization before any FCPB-specific security is put into place. The document identifies ten of the highest priority and most frequently recommended security practices as a place to start for today's operational systems. These practices address dimensions of information security such as policy, process, people, and technology, all of which are necessary for deployment of a successful security process. It's up to each organization to determine where to position itself on this exponential curve, (a symbolic reference to the full spectrum of "dimensions of information security.") and what amount of security investment they need to make to achieve a satisfactory level of security within the system. A satisfactory level of security also depends on the business goals of the security system. These considerations lead us to the need to create a security model targeted to address security threats and their business impact.

Security Model Overview

While security tools and practices are important for preventing attacks, implementing a security model at the organization level helps react to security situations better. A security model is a formal description of a security policy, which in turn captures the security requirements of an enterprise and describes the steps that must be taken to achieve security. The goal of implementing a security model is to provide information assurance. FCPB security implementation strategy can be based on the financial institution's existing security model or a new one may be created.

The following are a few popular security models that an organization can apply based on suitability.

1) CIA triad: This model focuses on the *Confidentiality*, *Integrity* and *Availability* aspects of security. In addition, it also covers *authentication*, *access control*, and *non-repudiation*. The CIA model is a good way to achieve high security. But some other goals such as risk assessment and the creation of a modified version of a "demilitarized zone" (DMZ) perimeter are not covered.

2) Many security consulting organizations (Big 4 consulting firms and others) have devised an alternative security model that identifies security more as a ***"strategic business process that includes the organization, the processes, and the technologies that enable access to, and protection of, an enterprise's information assets."*** This comprehensive security model illustrates how to identify, create, capture, and sustain the value of security in an organization by managing the inherent trade-offs between enablement and protection of an enterprise's most valuable resource — its information assets. In this model, these primary security activities are driven by business objectives and carried out in alignment with the enterprise's supporting capabilities – its organization (people), firm processes, and technology infrastructure. This type of model centers on how security adds value to an organization. A security model of this nature is specifically designed to function as a roadmap. It helps an organization navigate the process of building a scalable and sustainable security infrastructure that both protects and enables access to critical business and information assets in alignment with strategic business objectives and appropriately balanced and associated costs.

3) Another alternative has been developed by the Burton Group; it's commonly referred to as the *Virtual Extended Network* (VEN) model. The VEN model is an alternative to the traditional DMZ. It consists of four layers that represent different techniques for different zones of use:

- Resource – network, servers, data.
- Control – employees and security systems.
- Perimeter – partners.
- Extended Perimeter – suppliers and customers.

Specifically, the VEN model defines four logical layers: the resource layer, which houses clients, servers, applications and data; the control layer, where authentication services reside, as do controls for security policies across layers; the perimeter layer, which defines an organization's physical boundaries and contains firewalls, proxies and gateways; and the extended perimeter, where companies engage technologies or services to secure resources physically located outside the perimeter. The result is a model that builds on the existing infrastructure, but plans for a distributed perimeter.

4) *Defense-in-depth* is a strategy for achieving information assurance. It addresses security vulnerabilities in personnel, technology and operations for the duration of the system's lifecycle. The defense-in-depth approach builds mutually supporting layers of defense to reduce vulnerabilities, and to assist an organization in its efforts to protect against, detect, and react to as many attacks as possible. The construction of mutually supporting layers of defense inhibits the ability of an adversary who penetrates or breaks down one defensive layer to promptly encounter another, and another, until the attack is ultimately thwarted.

The purpose of this document is not a lengthy discussion about security models and how to develop and implement them, but it is critical to understand that the securing of your FCPB environment should be done in alignment with your enterprise security policies. Those policies should be created from the foundation based upon the security model established. Securing your FCPB environment should not be a one-off solution, but rather a comprehensive approach taken in concert with overall corporate security policies, guidelines and business requirements.

While it is impossible to anticipate every contingency, developing a well-rounded information security plan can help to dissuade all but the most determined attackers. With proper auditing systems such as audit logs, intrusion detection systems (IDS), and other mechanisms, incident response staff will have the right tools to determine what happened should a successful attack take place. Finally, maintaining confidentiality, integrity, and availability of information is a continuous process. Security is not something that can be dropped in place and forgotten.

Security Threats

In order to secure a site or organization, the first thing to know is where the security threats exist, how these threats are exploited, and what the financial ramifications are for each of these threats. The primary step in addressing security threats is to conduct and periodically repeat an information security risk evaluation that identifies your critical information assets (e.g., systems, networks, and data), threats to critical assets, asset vulnerabilities, and risks.

A critical part of addressing security threats is to identify and properly secure the systems deployed within your infrastructure and organization. This security assessment enables you to create a list of security vulnerabilities for the deployed software and hardware.

Create a list of all vendors who have supplied software and hardware for the deployed system. Then for each vendor and their hardware/software create a list of known vulnerabilities. This list provides a list of “known” issues and security concerns, and at a minimum these should be addressed. This might include applying patches, identifying workarounds and implementing them during deployment.

The list of known vulnerabilities and the results of the security assessment will provide your organization with a remediation roadmap for improving the security posture of your FCPB environment. It is crucial to actually implement the fixes, patches, and recommended security infrastructure improvements.

4. Securing Network Infrastructure

This chapter discusses various network components used for secure systems. The choice of these components and their configuration is finalized for each implementation in consultation with the bank implementing FCPB. The bank's internet standards and policies as well as FCPB team recommendations drive the final configuration.

Network Components

The various security components to consider in the system are:

Routers – Most routers also have certain firewall capability, such as packet filtering, port blocking, and so on. These features should be enabled for added security whenever possible.

Firewalls – The firewall is one of the most common network devices used to secure a network environment. It acts as a primary defense mechanism against unauthorized access. A firewall device can be special software running on the hardware or it can be a dedicated hardware device.

Multiple DMZ may be created with the Web Server, Application Server and Database Server residing in different DMZs.

Note: Best practices suggest the use of firewalls from different vendors for the internet facing firewall and the internal firewalls. This makes the intrusion difficult via multiple levels of different firewalls. The final decision of the firewall deployment should be performed by the bank based on their internal security guidelines.

Load Balancers – Load balancers are a highly recommended device for achieving high scalability and fault tolerance at a reasonable cost. Most units can be configured to replace a firewall and provide hardware SSL acceleration. This provides some amount of security and scalability at a reasonable cost.

Reverse Proxy Servers – RPS are most often used as part of a security infrastructure. Most sites deploy them to prevent internet IP packets from reaching production web servers directly. This is a security device for inbound HTTP(S) traffic. A RPS provides protection from attacks that are launched to take advantage of vulnerability such as buffer overflow, malformed packets, and so on. It also adds another tier to the security architecture.

Forward Proxy Servers – Forward Proxy Servers or Proxy Servers in short are mostly used as part of a client security and caching infrastructure. Most sites deploy them to prevent users from connecting to the Internet directly. This is security device for outbound HTTP(S) traffic. The user's browser connects to a proxy server that is either configured in the browser or transparently routed to via a router. The proxy does the actual communication with the web server on behalf of the user.

In the case where a site deploys FCPB which communicate to servers outside the production environment a forward proxy server should be used. The production firewall should be configured to allow only the proxy server to connect outside the firewall. The proxy is therefore the only means of communicating to the outside world from within the production environment. All HTTP(S) requests originating from FCPB servers should be routed via the proxy server.

Servers – Servers have a number of security setting and vulnerability issues associated with them. At a minimum, all vendor-provided OS security patches should be applied to the servers. Additionally, all unused services should be disabled on the servers.

Disaster Recovery Plans – All installations regardless of size must create a disaster recovery plan. The disaster recovery plan must include unavailability due to security failures, standard power failures, physical disasters, and other outages. For highly secure installations, this should include creation of a second data center that is also part

of a separate physical security zone. This means separate network security policies, access codes/badges, and security administrators.

Virtual IPs (VIPs) – VIPs are not physical devices. These are IP addresses where users point their browsers to access a services. These IP addresses could point to a real web server in the simplest case. In most cases, they will point to a logical service implemented using firewalls, load balancers, proxy servers, and real servers. A VIP is also the IP address that the site's DNS name maps to.

Secure Setups

This section discusses some common FCPB system layouts. The system layouts will have varying degree of scalability, availability, and security. Since every site is unique with unique requirements, different parts of the layout will require modification. FCPB infrastructure team can provide that support on a case-by-case basis. The following items are basic design assumptions and policies that should be addressed.

- The deployment should not have any single point of security failure in the architecture
- Static routes are used within the system whenever possible
- The application has been placed on the DMZ network
- The architecture assumes the external/internet as well as internal/intranet network to be non-trusted, so protection from both the internet and the intranet is needed
- Each tier in the FCPB Pure Internet Architecture has been leveraged to provide an additional security tier between the outside network and the protected data

5. Securing Web Server

Once the infrastructure is secure, FCPB web server should be secured. The various layers to secure for a production system are described below followed by individual sections describing how to configure each item.

- Apply vendor recommended security hardening procedure to web server
- Use HTTPS as a minimum level of security for FCPB Internet Architecture
- Disable HTTP access to FCPB Internet Architecture
- Disable browser caching
- Use only HTTPS and mutual authentication for integration

Oracle FCPB uses the Web Server as the entry point for all transactional requests. The following configurations are valid for the Apache Web Server as well as any variants like Oracle HTTP Server or IBM HTTP Server based on the same

Note: The Apache / IBM HTTP / Oracle HTTP Server documentation should be referred for the details of the server directives used within this section for the various configurations

Remove Default user

To protect the apache server, the default apache user login accounts should be disabled, after creating the appropriate operative accounts with administrative privileges. Attackers first try to control the system with then default user credentials.

Remove Server Banner

To avoid exposing Apache version and enabled modules, turn off the banner in httpd.conf:

```
Set ServerSignature off
Set ServerTokens Prod
```

Turn Off Directory Indexing

There are two goals when protecting a web server:

- Reduce the amount of information available
- Reduce access to non-application related areas

Directory indexes display the contents of a directory if there is not an index.htm or similar file available. Disabling this entry prevents an intruder from viewing the files in a directory, potentially finding a file that may be of use in their quest to access the system.

This can be done by modifying the following configuration files and commenting out the line indicated below:

```
${IAS_ORACLE_HOME}/Apache/Apache/conf/httpd.conf and
${IAS_ORACLE_HOME}/Apache/Apache/conf/httpd_pls.conf


# IndexOptions FancyIndexing
```

The Apache AUTOINDEX module automatically generates directory indexes. To disable the module in httpd.conf, comment these lines as follows.

```
#LoadModule autoindex_module libexec/mod_autoindex.so
#AddModule mod_autoindex.c
```

Remove Server Manuals

The server manuals from the manuals directory on the server should be removed or protected with appropriate access control to be not allowed from the internet.

Prevent Search Engine Indexing

For internet facing web servers, enable robot exclusion. This may be done either with a robots.txt file or using a META tag. See http://www.robotstxt.org/wc/robots.html for more information.

The following would indicate that no robots are allows to access the site.

```
User-Agent: *
Disallow: /
```

The following META tag can also be added in the static HTML files to indicate to the robots to not index the content of the page or scan it for further links. The META tag should be placed in the head section of the HTML page.

```
<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW" />
```

Protect Administrative Web Pages

The Web Server provides a number of web pages provide administrative and testing functionality. These pages offer information about various services, the server's state and its configuration. While useful for debugging, these pages must be restricted or disabled in a production system. Use the configuration file httpd.conf to limit web page access to a list of trusted hosts. To do this, create a file trusted.conf and include it in the httpd.conf file. This new file contains the following content.

```
<Location "URI-to-protect">
    Order deny,allow
   Deny from all
   Allow from localhost <list of TRUSTED IPs>
</Location>
```

Replace "URI-to-protect" with the path of the page you wish to protect.

Replace *<list of TRUSTED IPs>* with host machines from which administrators may connect.

Disable Test Pages

Add the following directives in httpd.conf to prevent access fast-cgi test pages:

```
<Location ~ "^/fcgi-bin/echo.*$">
   Order deny,allow
   Deny from all
</Location>
```

Or better yet - unconfigure fast-cgi.

Configure TLS Cipher Versions

The protocols supported for secure communication can be included TLS V1.1 or TLS V1.2. The use of only TLS V1.1 or TLS V1.2 is recommended to be setup within httpd.conf file in the webserver.

Please refer the below link for more details.

https://gps.oracle.com/ossa/farm/standards/doku.php?id=ats:implementation_details

Block TRACE access

Prevent the TRACE HTTP method for being invoked from the internet. The following configuration should be added to the httpd.conf file.

```
###Added to prevent HTTP TRACE
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* -[F]
```

Audit

Apache's logging parameters, when activated, as is done by default, the server logs data about all web access to the system.

More Information

WebLogic: If you have deployed a WebLogic JEE server, take the following steps to harden the installation:

Follow Oracle recommendations for hardening WebLogic Server. For e.g. details of security for Oracle ® WebLogic Server 11g can be found at:

http://docs.oracle.com/cd/E23943_01/web.1111/e13707/toc.htm

WebSphere: If you have deployed a WebSphere JEE server, follow IBM's recommendations to security harden the installation, located at the IBM website at

http://publib-b.boulder.ibm.com/Redbooks.nsf/9445fa5b416f6e32852569ae006bb65f/d630ec33fde5486785256b5f007ecac5?OpenDocument

6. Securing Oracle TNS Listener

Oracle clients communicate with the database using the Transparent Network Substrate (TNS) protocol. When the Listener receives a connection request (TCP port 1521, by default), it starts up a new database process and establishes a connection between the client and the database.

This section contains security recommendations for the TNS Listener.

Network

Add IP Restrictions or Enable Valid Node Checking

Valid Node Checking allows or denies access from specified IP addresses to Oracle services. To enable Valid Node Checking for 9*i* and above, set the following parameters in $TNS_ADMIN/sqlnet.ora:

```
tcp.validnode_checking = YES
tcp.invited_nodes = (X.X.X.X, hostname,...)
tcp.excluded_nodes = (hostname, X.X.X.X,..)
```

The first parameter turns on Valid Node Checking. The latter two parameters respectively specify the IP addresses or hostnames that are permitted to make or are denied from making network connections to Oracle services. Replace X.X.X.X with the middle-tiers' IP addresses. Middle-tier applications include web servers and any remote monitoring tool that uses SQLNet.

Note, use of SQLNet clients such as sqlplus, toad, ADI from Windows desktop is not recommended. If implemented, that desktop cannot use DHCP. Use a static IP address.

Specify Connection Timeout

In $TNS_ADMIN/listener.ora, set the following parameter:

```
CONNECT_TIMEOUT_$ORACLE_SID = 10
```

Use the parameter CONNECT_TIMEOUT to specify the amounts of time, in seconds, for the Oracle Listener to wait for the connection from a client to complete.

Configure Listener on a Non Default Port Number

By default, the TNS Listener receives service requests on TCP port 1521. Configure it to listen on another port number. Although not foolproof, this makes attacks more difficult.

Authentication

Enable TNS Listener Password

Setting a password for the Listener is one of the most important hardening procedures. These instructions assume that the listener name is WM11. The default for oracle databases in general is “LISTENER” while for FCPB databases it is set to the SID of the database.

Start the Listener control program and set the current Listener in case you have more than one listener defined, then change the password.

```
$ lsnrctl
LSNRCTL> set current_listener WM11
Current Listener is WM11
LSNRCTL> change_password
Old password: -- just hit return
New password: -- new, secure password
Reenter new password: -- new, secure password
Connecting to (DESCRIPTION = (ADDRESS = (PROTOCOL=TCP) (HOST=X.X.X.X) (PORT=1521)))
Password changed for WM11
The command completed successfully
LSNRCTL> set password
Password:
The command completed successfully
LSNRCTL> save_config
```

With the Listener password protected, ensure that file and directory settings can only be changed by editing the listener.ora file (not via set commands in lsnrctl). Enable ADMIN_RESTRICTIONS by adding the following line to listener.ora and reload the configuration file into the Listener:

```
$ echo "ADMIN_RESTRICTIONS_WM11 = ON" >> listener.ora

LSNRCTL> set current_listener WM11
  Current Listener is WM11
LSNRCTL> set password
  Password:
  The command completed successfully
LSNRCTL> reload
  Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=X.X.X.X)(PORT=1521)))
  The command completed successfully
```

With these settings, the Listener configuration file cannot be changed via the tnslsnr process.

To undo these steps:

1. Edit listener.ora and remove the lines PASSWORDS_<listener> and ADMIN_RESTRICTIONS_<listener>
2. Stop the tnslsnr process (using lsnrctl or use ps to find the pid and kill to kill it)
3. Restart the listener (using lsnrctl start)

Note, password protecting the TNS Listener has the following effects:

- Only the oracle user can stop the TNS Listener using lsnrctl without providing the password.
- The Listener process requires a password to list SERVICES or STATUS. This breaks some monitoring and remote administration tools, if they do not expect to provide a password.
- Cannot start, stop, check status or run services on remote machines via lsnctrl. Use Enterprise Manager for remote administration.

Authorization

Enable Admin Restrictions

In $TNS_ADMIN/listener.ora, set the following parameter:

```
ADMIN_RESTRICTIONS_<listener>=ON
```

Note: When ADMIN_RESTRICTIONS is ON, all the set commands in lsnrctl are disabled and the only way to change the configuration is to edit the listener.ora file. Because password restrictions are enabled, some remote administration tools may subsequently fail.

Audit

Enable TNS Listener Logging

To enable logging, in $TNS_ADMIN/listener.ora set the following parameters:

```
LOG_STATUS = ON
LOG_DIRECTORY_$ORACLE_SID = $TNS_ADMIN
LOG_FILE_$ORACLE_SID = $ORACLE_SID
```

7. Securing Oracle Database

This section contains security recommendations for the Database.

Hardening

Disable XDB

To support XDB, the TNS Listener process listens on two additional TCP ports: 2100 for ftp access and 8080 for http access. FCPB does not require these services; they should be disabled.

To disable XDB, remove or comment out the line in init.ora that reads

```
*.dispatchers='(PROTOCOL=TCP) (SERVICE=sidXDB)'
```

Review Database Links

Review database links in both production and development environments.

Authentication

Middle-tier applications logon to the database through application schemas rather than end-user accounts. Some individuals (IT Administrators) may require direct access to the application database via their own schema.

Remove Operating System Trusted Remote Logon

This setting prevents the database from using an insecure logon protocol. Make sure init.ora contains:

```
REMOTE_OS_AUTHENT=FALSE
```

Implement Two Profiles for Password Management

The database provides parameters to enforce password management policies. However, some of the database password policy parameters could lock-out FCPB. Because of this, we make specific recommendations for or against using certain management features depending upon schema type.

Password Parameters	Application Profile	Administrator Profile
FAILED_LOGIN_ATTEMPTS	UNLIMITED	5
PASSWORD_LIFE_TIME	UNLIMITED	90
PASSWORD_REUSE_TIME	180	180
PASSWORD_REUSE_MAX	UNLIMITED	UNLIMITED
PASSWORD_LOCK_TIME	UNLIMITED	7
PASSWORD_GRACE_TIME	UNLIMITED	14
PASSWORD_VERIFY_FUNCTION	*Recommended*	*Recommended*

Database profiles contain limits on database resources and password policies. Create two database profiles: one for middle-tier application schemas and one for personnel. Assign middle-tier application schemas to the first profile and all accounts used by administrators to the second profile.

For more information on profiles, see CREATE PROFILE in the Oracle SQL Reference documentation.

Change Default Installation Passwords

Following an installation, the application database instance contains default, open schemas with default passwords. These accounts and corresponding passwords are well-known, and they should be changed, especially for a database to be used in a production environment.

Use database command to change a password:

```
SQL> alter user <SCHEMA> identified by <NEW_PASSWORD>;
```

Patch 4926128 contains a SQL script that will list all open accounts with default password in your database.

Complex Password Setup

The password to the default accounts like SYS, SYSTEM etc. should be complex and securely stored by the bank.

Authorization

Restrict Access to SQL Trace Files

The init.ora parameter _TRACE_FILES_PUBLIC grants file system read access to anyone who has activated SQL tracing. Set this to its default value of *False*.

```
_TRACE_FILES_PUBLIC=FALSE
```

Remove Operating System Trusted Remote Roles

Set the init.ora parameter REMOTE_OS_ROLES to *False* to prevent insecure remote roles.

```
REMOTE_OS_ROLES=FALSE
```

Limit File System Access within PL/SQL

The parameter UTL_FILE_DIR limits file system access for all database accounts using the PL/SQL API UTL_FILE. FCPB follows table logging and does not require this parameter to be set. However if used, best practice would be to use

```
UTL_FILE_DIR = <dir1>, <dir2>,<dir3>...
Avoid:
UTL_FILE_DIR = *
```

Limit Dictionary Access

Set O7_DICTIONARY_ACCESSIBILITY to *False* to prevent users with Select ANY privilege from reading data dictionary tables. False is the default for the 10g database.

```
O7_DICTIONARY_ACCESSIBILITY = FALSE
```

Audit

This section describes the auditing capabilities available in Oracle database. These recommendations should not have a measurable performance impact.

Configure the Database for Auditing

In init.ora, set AUDIT_TRAIL to DB, OS or TRUE. Consult with the Applications Database Administrator before setting this value to TRUE. When set to OS, the database stores its audit records on the file system:

```
AUDIT_TRAIL = OS
```

Set parameter AUDIT_FILE_DEST to the directory where the audit records should be stored. When not set, AUDIT_FILE_DEST defaults to $ORACLE_HOME/rdbms/audit. In this example, the database places audit records in directory E:\logs\db\audit.

```
AUDIT_FILE_DEST = E:\logs\db\audit
```

Restart the database for these parameters to take effect.

Note: The database generates some audit records by default, whether or not AUDIT_TRAIL is enabled. For example, Oracle automatically creates an operating system file as an audit record when a user logs in as SYSDBA or as INTERNAL.

Audit Database Connections

Monitoring and auditing database sessions, provides valuable information on database activity and is the only way to identify certain types of attacks (for example, password guessing attacks on an application schema). By auditing database sessions, suspicious connections to highly privileged schemas may be identified.

To audit sessions, login through sqlplus as SYSTEM and issue the following command:

```
SQL> audit session;
```

Audit Database Schema Changes

Audit any changes to the standard FCPB database schema or creation of new schemas. As rare events, these changes may indicate inappropriate or malicious activity.

To audit schema changes, login through sqlplus as SYSTEM and issue the following command:

```
SQL> audit user;
```

Audit Other Activities

To complete the recommended auditing, enable three other audit events: *create database link, alter system* and *system audit*. The remaining audit options generate significant entries of little value. Auditing these other actions provides little meaningful information.

To audit the other events, login through sqlplus as SYSTEM and issue the following commands:

```
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 Administrators and their Actions

Connections to the database as well as SYSDBA and SYSOPER actions (instance startup/shutdown) are always logged to the directory $ORACLE_HOME/rdbms/audit (unless AUDIT_FILE_DEST property is overridden). This file contains the operating system user and terminal ID.

Review Audit Records

If AUDIT_TRAIL is set to OS, review audit records stored in the file name; in AUDIT_FILE_DEST.

If AUDIT_TRAIL is set to DB, retrieve audit records from the SYS.AUD$ table. The contents can be viewed directly or via the following views:

- DBA_AUDIT_EXISTS
- DBA_AUDIT_OBJECT
- DBA_AUDIT_SESSION
- DBA_AUDIT_STATEMENT
- DBA_AUDIT_TRAIL
- DBA_OBJ_AUDIT_OPTS
- DBA_PRIV_AUDIT_OPTS
- DBA_STMT_AUDIT_OPTS
-

The audit trail contains a lot of data; begin by focusing on the following:

- Username: Oracle Username.
- Terminal: Machine from which the user originated.
- Timestamp: Time the action occurred.

- Object Owner: The owner of the object that the user touched.
- Object Name: The name of the object that the user touched.
- Action Name: The action that occurred against the object (INSERT, UPDATE, DELETE, SELECT, EXECUTE).

Maintain Audit Records

Archive and purge the audit trail on a regular basis, at least every 90 days. The database connection entries take up significant space. Backup the audit file before purging.

Secure Audit Records

Audit data may contain confidential or privacy related data. Restrict audit trail access appropriately.

Secure Database Backups

The database backups should be stored for the required period as per the regulations and bank's history retention policies. These backups should be securely stored and access should be controlled to authorized users only.

8. Securing the Desktop

Hardening

Update Browser

- Update browser when new versions are released; they often include new security features
- Check browser for built-in safety features
- The browser used to should meet the minimum security requirements like 128-bit encryption and cipher strength support
- When using Internet Explorer:
  - Upgrade to at least Version 6.0.
  - Check Microsoft website for the latest browser security patches (http://www.microsoft.com)

Update Security Patches

Security patches provided by the desktop operating system provider should be regularly applied. The same is true to patches release by anti-virus software supplier.

Set Policy for Unattended PC Sessions

People may attempt to access unattended workstation while the user is still logged into the system. The user should never leave their workstation unattended while logged into the system because it makes the system accessible to others who may walk up to the computer. Organizations should set a corporate policy for handling unattended PC sessions. Users are recommended to use the password-locked screen savers feature on all PCs.

Browser Security

Turn Off AUTOCOMPLETE in Internet Explorer

Change Internet Explorer's AUTOCOMPLETE settings. IE can automatically show previous values entered in the same form field. Although desirable for frequently accessed pages, for privacy and security reasons this feature should be disabled.

To turn OFF the Auto Complete feature:

- Navigate through *Tools -> Internet Options -> Content*
- From the *Content* tab, click the *AutoComplete* button.
- Uncheck "forms" and "User names and passwords on forms".

Also, do not use the "remember password" function; this is known security vulnerability.

Note: FCPB anyways enforces the Auto Complete Flag from within the pages but the above should be done as a good practice.

Clear Browser Cache and Exit Browser

Whenever a public or shared computer is used, it is essential that the user signs out when the internet session is finished. Once the user has signed out, they should delete the browser's cache and history this deleting any cached copies of the pages, if any, in the browser cache. The browser should be closed after every internet banking session.

9. Securing the Operating Environment

The environment in which Oracle Applications run contributes to or detracts from overall system security. This section contains security recommendations for tightening Oracle file system security along with more general advice for overall system hardening.

Disclaimer :-

The security recommendation provided by oracle is subset of best practices for the operating environment. The explained steps should not be taken as authoritative guide. Oracle recommends referring the Operating system vender's security manual to secure the environment from all the aspects.

Hardening

Cleanup File Ownership and Access

- The directory $ORACLE_HOME/bin contains Oracle executables. Check that the operating system owner of these executables matches the operating system user under which the files have been installed. A typical mistake is to install the executables in user oracle's directory but owned by root.
- Prevent remote login to the Oracle (and root) accounts. Instead, require that legitimate users connect to their own accounts and su to the Oracle account. Better yet, use sudo to restrict access to executables.

Cleanup File Permissions

Refer to the product installation documentation for the complete instructions on setting file permissions.

On UNIX systems:

- Set the permissions on $ORACLE_HOME/bin to 0751 or less. Set all other directories in $ORACLE_HOME to 0750 or less. Note, this limits access to the Oracle user and its groups (probably DBA).
- Set file permissions for listener.ora and sqlnet.ora to 0600.
- Set file permissions for tnsnames.ora to 0644.
- Ensure that the owner, group and modes of the Oracle files created upon installation are set to allow minimum privilege. The following commands make this change. Note, the group and owner are for illustration only, the correct group and owner should be substituted.

```
$chgrp -R    <dba>      $ORACLE_HOME
$chown -R    <oracle>   $ORACLE_HOME
```

- Review owners and groups when cloning a database
- Protect the $ORACLE_HOME/rdbms/admin directory including catalog.sql, catproc.sql and backup scripts.
- Secure scripts containing usernames and passwords
- Verify that set user id (SUID) and set group id (SGID) are not set on binaries. In general, Oracle recommends that the SUID and SGID bits to be removed from binaries shipped by Oracle.

On windows systems, NTFS must be used. The FAT/FAT32 file system provides no security.

Protecting core dumps

UNIX based operating system generate core-dump files, in case of any memory related issues happens and due to that application crashes. The core file contains the state of the memory dump during the time of

program crash. This core dump file contains significant information about the system configuration, file system etc. Hence we need to protect the dump files from easy access.

By default, a core dump file is named core, but the /proc/sys/kernel/core pattern file (since Linux 2.6 and 2.4.21) can be set to define a template that is used to name core dump files. The template can contain % specifies which are substituted by the following values when a core file is created:

%% a single % character

%p PID of dumped process

%u (numeric) real UID of dumped process

%g (numeric) real GID of dumped process

%s number of signal causing dump

%t time of dump, expressed as seconds since the Epoch (00:00h, 1 Jan 1970, UTC)

%h hostname (same as nodename returned by uname(2))

%e executable filename (without path prefix)

%c core file size soft resource limit of crashing process (since Linux 2.6.24)

A single % at the end of the template is dropped from the core filename, as is the combination of a % followed by any character other than those listed above. All other characters in the template become a literal part of the core filename. The template may include '/' characters, which are interpreted as delimiters for directory names. The maximum size of the resulting core filename is 128 bytes (64 bytes in kernels before 2.6.19). The default value in this file is "core". For backward compatibility, if /proc/sys/ker-nel/core_pattern does not include "%p" and /proc/sys/kernel/core_uses_pid (see below) is non-zero, then .PID will be appended to the core filename.

UNIX administrators can define the file path for the core-dump files and those paths can be protected with appropriate priviliages.

Lockdown Operating System Libraries and Programs

The database and applications require that the underlying operating system provide certain services.

- Electronic Mail

  FCPB may require access to a SMTP Mail Transfer Agent (SMTP MTA) typically send mail. This is required for outbound emails, typically notifications from FCPB (if this feature is desired by the financial institution). If possible, restrict access to the operating system users who absolutely need the mail facility from the shell.

- Remote Access

  Use secure shell (ssh) to access middle-tier and database hosts. This replaces telnet, rsh, rlogin, rcp and ftp.

The following services may provide operational convenience:

- NTP (Network Time Protocol) – for synchronizing the clock on the UNIX hosts to provide accurate audit records and simplify trouble-shooting.
- CRON – for operating system cleanup and log file rotation

Network

To secure the network, limit access to services users need and make those services as secure as possible. Disabling unused services reduces securing and monitoring work.

Refer to Chapter 4 for details on the same.

Authentication

Good security requires secure accounts.

Configure Accounts Securely

- Make sure that *all OS accounts* have a non-guessable password. To ensure that the passwords are not guessable, use crack or john-the-ripper (password cracking tools) on a regular basis. Often, people use passwords associated with them: license plate numbers, children's names or a hobby. A password tester may check for these. In addition, change passwords from time to time.
- Automatically disable accounts after several failed login attempts.
- .netrc files weaken security.

Limit Root Access

- The fewer people with root access, the easier it is to track changes.
- The root password must be a strong, non-guessable password. In addition, change the root password every three (3) months and whenever an administrator leaves company. Always logout of root shells; never leave root shells unattended.
- Limit root to console login, only (specified in /etc/security).
- Root, and only root, should have UID 0.
- Check root '.*' files for security holes. The root '.*' files SHOULD have 700 or 600 permissions
- umask for root is 022 (rwxr-xr-x). A umask of 077 (rwx------) is best, but often not practical
- To avoid trojan horse programs, always use full pathnames including aliases. Root should NEVER have "." in path.
- NEVER allow non-root write access to any directories in root's path.
- If possible, do not create root's temporary files in publicly writable directories.

Manage User Accounts

Do not share user accounts. Remove or disable user accounts upon termination. Disable login for well known accounts that do not need direct login access (bin, daemon, sys, uucp, lp, adm). Require strong passwords and, in some cases, a restricted shell.

Do Not Allow Guest Accounts

It is hard to imagine what kind of guests should have access to a production system. For this reason do not allow guest access.

Authorization

Secure NFS

Only run NFS as needed, apply latest patches. When creating the /etc/exports file, use limited access flags when possible (such as readonly or nosuid). By using fully qualified hostnames, only the named host may access the file system.

Secure Operating System Devices

Device files /dev/null, /dev/tty and /dev/console should be world writable but NEVER executable. Most other device files should be unreadable and non-writable by regular users.

Secure Executables

Always get programs from a known source. Use a checksum to verify they have not been altered.

Secure File Access

Create minimal writable file systems (esp. system files/directories). Limit user file writes to their own directories and /tmp. Add directories for specific groups. Limit important file access to authorized personnel. Use setuid/setgid only where absolutely necessary.

Maintenance

Good security practice does not end after installation. Continued maintenance tasks include:

- Install the latest software patches.
- Install latest operating system patches.
- Verify user accounts - delete or lock accounts no longer required.
- Run security software and review output.
- Keep up to date on security issues by subscribing to security mailing lists, reading security news groups and following the latest security procedures.
- Implement trusted file systems like NIS, NIS+ or others such as HP-UX trusted system.
- Test the system with tools like NESSUS (network security) and CRACK (password checker).
- Install Tripwire to detect changes to files
- Monitor log files including btmp, wtmp, syslog, sulog, etc. Consider setting up automatic email or paging to warn system administrators of any suspicious behavior. Also check the snort logs.

10.FCPB Application Security Hardening

FCPB is depended upon to provide application access in a secure, reliable fashion. Data integrity, confidentiality and availability must be maintained. FCPB must be installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Application level access has implemented via the Security Management System (SMS) module.SMS supports “ROLE BASED” access of Screens and different types of operations. FLEXCUBE Private Banking Solutions supports dual control methodology, wherein every operation performed has to be authorized by another user with the requisite rights

The purpose of this chapter is to describe the requirements for installing and operating FCPB in a secure fashion, to maintain the security integrity of FCPB.

Before the application is put into production, you should take reasonable steps to ensure that security has been hardened. The appropriate use of authentication, authorization, and audit functionality in-built to the application, can help mitigate risk to the security infrastructure.

The hardening procedure is a group of tasks that should be completed in order to harden the application. Many of these items are industry standard best practices; others are specific to FCPB. This list is by no means exhaustive; however, it should give a feel for items to check. Some of the general steps included in the FCPB application hardening procedure include:

- Setting security parameters
- Enabling audit logging

Expire Password at First Login

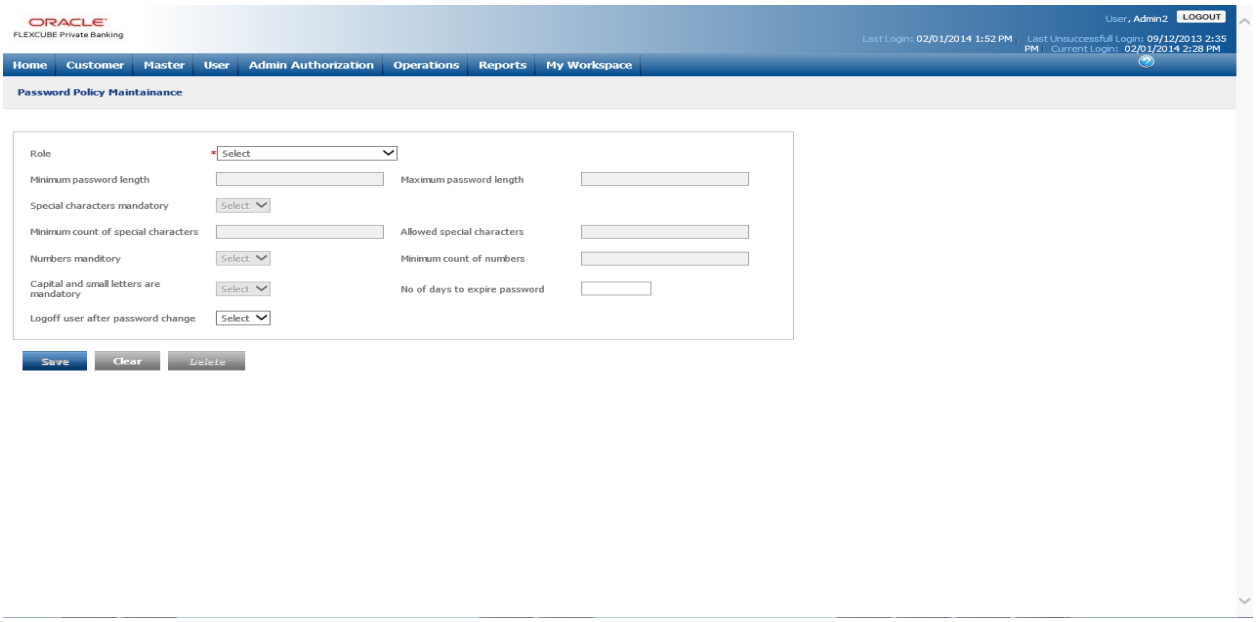
The user should be forced to change their passwords in the following situations:

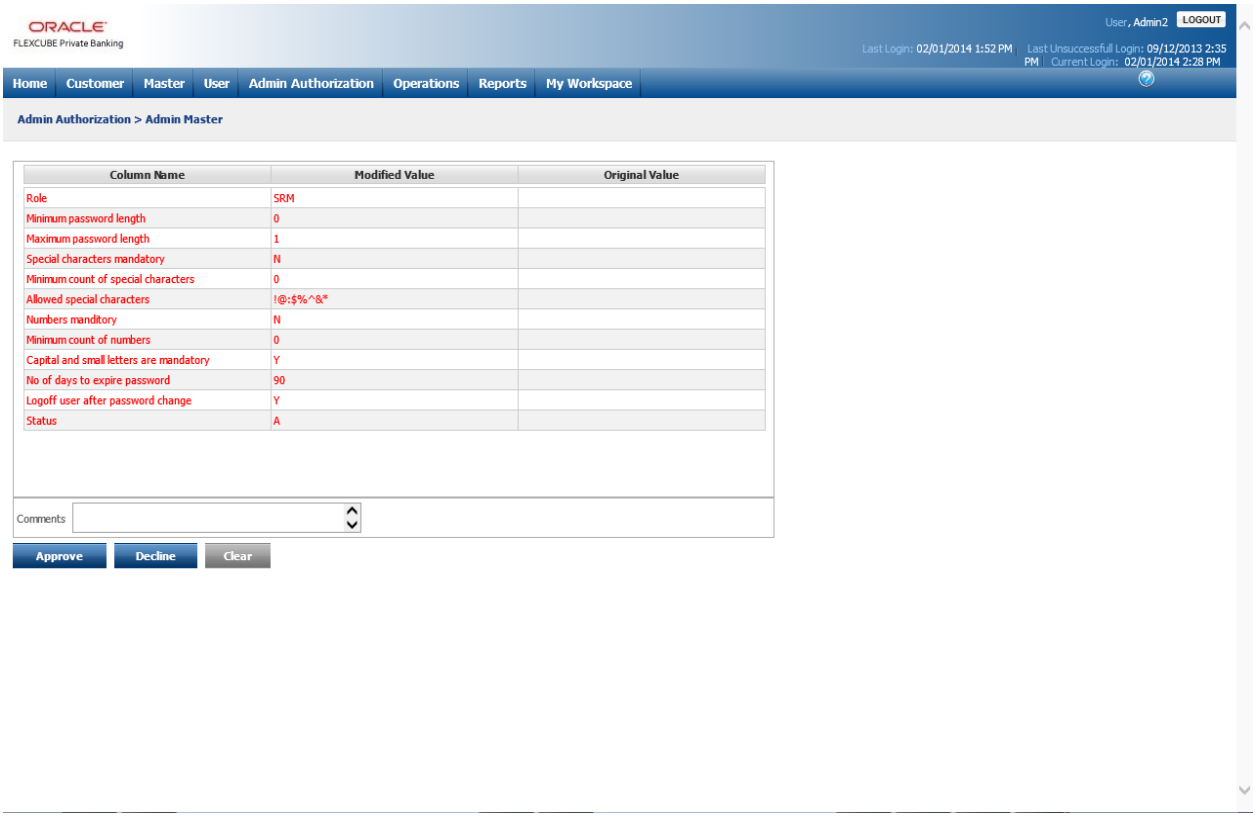
- The first time that a user signs in to FCPB
- The first time that a user signs in after the system has emailed the user a randomly generated password (password reset by application administrator)

Increase Password strength

FCPB 12.0.3 supports facility to increase the password strength. Hence bank can increase the password strength by changing password policy for the specific roles.

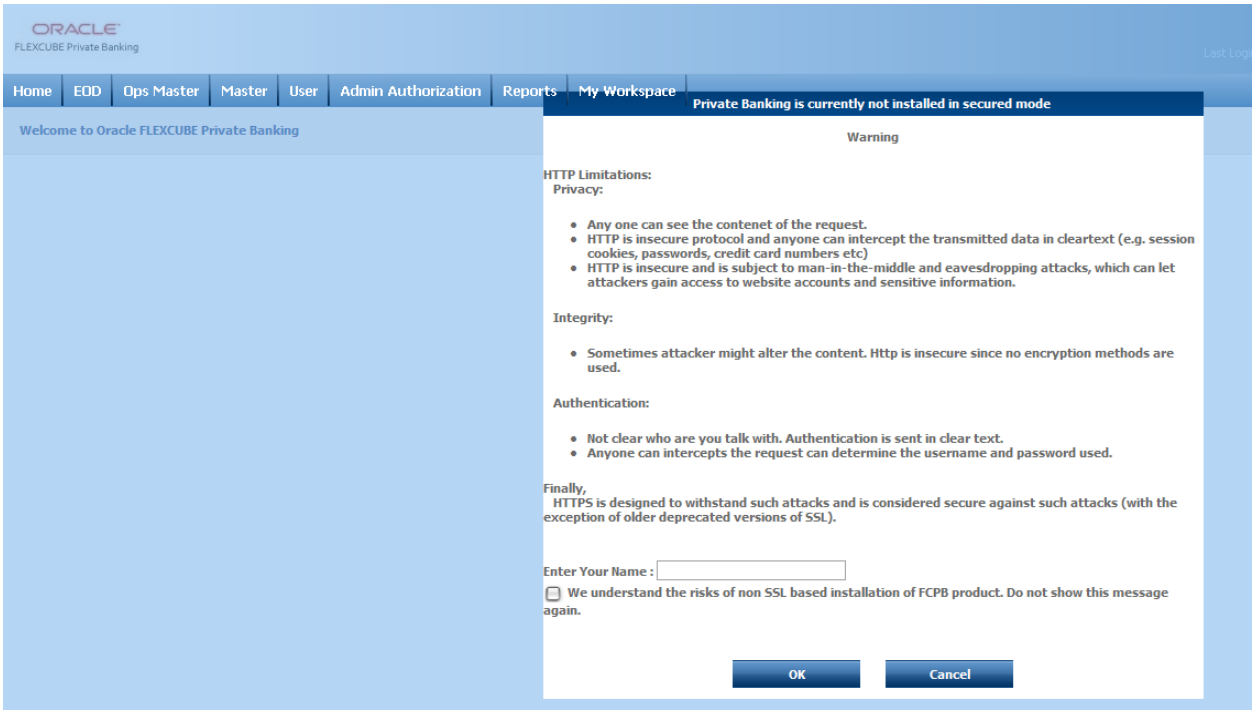
Password policy provides facility to specify Length of the password, minimum capital letters required for a password, minimum number of special characters required for a password and allowed special characters in a password. Hence system forces users to choose stronger password.





Deploying FCPB in Secure Mode

FCPB detects automatically, if the deployment is not done in secure mode (HTTPS) and warns the admin and ops users to deploy in secure. Hence bank can take necessary actions to deploy the application in HTTPS.



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.

- Cookies are set with Http only as true
- Cookie secure flag set to true
- Cookie path to refer to deployed application

<session-descriptor>

<cookies-enabled>**true**</cookies-enabled>

<cookie-http-only>**true**</cookie-http-only>

<url-rewriting-enabled>**false**</url-rewriting-enabled>

</session-descriptor>

Always make sure Cookies are set with always Auth Flag enabled by default for WebLogic server .

Disable Default User

Upon installation, FCPB creates 2 bootstrap user accounts with limited privileges and maker-checker feature (4-eyes) to authorize new user and role creation. Create additional administrative users for operational needs and de-activate the default user accounts.

Remove Unwanted Static Web Content

The WAR file should be cleaned after the Branding exercise for any unwanted static content, JSP files etc. Images, JavaScript files etc that are not required should be removed before the final deployment. However, FCPB does not currently do a cleanup of the WAR file prior to deployment.

Remove Copyrights from Static Web Content like HTML, JS Files

JS and Static HTML files can contain copyrights and modification history information. This should be removed from the static content from within the WAR files. No modification history and copyrights should be maintained in the static content. However, FCPB does not currently do a cleanup of the static content prior to deployment.

Disable Directory Browsing

Directory browsing feature should be disabled in the WAR files if newly built.

Review Sign-in and Timeout Security

A user attempting to sign in to FCPB enters a user ID and a password on the application Sign-on page. If the ID and password are valid, FCPB connects the user to the application, and the system retrieves the appropriate user profile.

After a user signs in, he or she can stay connected as long as the sign-in time allows and as long as the browser doesn't sit idle for longer than the timeout interval. A timeout interval specifies how long the user's machine can remain idle before FCPB automatically disconnects the user from the application.

The timeout settings are maintained in the application web.xml. These settings should be reviewed prior to moving a FCPB application into production.

A timeout setting of 600 seconds (10 min) is recommended as a good practice.

Track Users' Login and Logout Activity

FCPB Security provides two audit logs which tracks users' sign-in and sign-out activity in audit tables. Sign-out activity includes user logout, timeouts and browser closings.

Detect and Prevent Duplicate User Sessions

FCPB prevents multiple session of the same application user from being created. The same is an application Sign-on time authentication.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, etc., especially early on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement.

Following would be useful:

1. Review failed attempts by a user during a day or date range using the login report of FCPB
2. Usage of tools such as Oracle Adaptive Access Manager to review potentially fraudulent login patterns. E.g. login using IP different from usual IP for the same user ID
3. Monitor log files to review unauthorized attempts to functions

11.Additional Security Hardening

File Permissions

File permissions in the server machine is very important, only the root user/file owner should have the full permission on the file system other users should be given permissions on requirement basis. If a user/role need only a read access to a file or directory, the administrators should provide only read access to the file, rather if administrator provides the full permissions, the user may inappropriately access the file and that may harmful to the data and system integrity.

Example, if you allow non-root users to modify files that root either executes or writes on then you open your system to root compromises. For example, someone could replace the web server binary (typically httpd) so that the next time you start it, it will execute some arbitrary code. If the logs directory is writeable (by a non-root user), someone could replace a log file with a symlink to some other system file, and then root might overwrite that file with arbitrary data. If the log files themselves are writeable (by a non-root user), then someone may be able to overwrite the log itself with bogus data.

Disabling WEBDAV

WebDAV (Web-based Distributed Authoring and Versioning) is a set of extensions to HTTP/1.1. It is an open, published standard that allows you to edit documents on a remote web server.

WebDAV supports the following features:

Editing: Create, update, and delete files.

Properties: Store metadata such as titles, author names, and publication dates. You can set, delete, and retrieve these metadata.

Collections: Group resources into collections that are organized like a file system, similar to a directory or desktop folder.

Locking: Prevent others from editing the same content you're working on in WebDAV. The duration of the locks is independent of any individual network connection.

In apache webserver WEBDAV is disabled by default. We suggest ensuring the httpd.conf file WEBDAV is enabled/ disabled.

In httpd.conf file, if you find an entry as

DAV ON

Then WEBDAV is ON. We recommend switching off as below.

DAV OFF

Disabling unused/not required modules in apache

The apache webserver by default enables with modules, which are not all the modules are required for product functioning. Hence disable the unused/not required modules in apache webserver.

Disabling Unnecessary HTTP methods

For FCPB product functioning requires HTTP get and HTTP Post method only. The other HTTP methods TRACE, PUT, DELETE, TRACK, OPTIONS, CONNECT can be disabled in apache webserver.

Disabling SSL Renegotiation

SSL Renegotiation feature of the web server should be switched-off to prevent man in middle attack. By default apache webserver switched off with the SSL Renegotiation. We suggest ensuring the httpd.conf file SSL Negotiation enabled/disabled.

In httpd.conf file, if you find an entry as

SSLInsecureRenegotiation ON

We recommend switching off as below.

SSLInsecureRenegotiation OFF

Security Practice Guide 12.0.2.0.0

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/