Security Practices Guide

Oracle FLEXCUBE Enterprise Limits and Collateral Management

Release 12.0.0.0.0

[October] [2013]

Oracle Part Number E51544-01

Table of Contents

1. About this Manual

1.1 Introduction

This document describes the various measures and practices to be adopted with a deployment of Oracle FLEXCUBE Enterprise Limits and Collateral Management, to aid in securing the day-to-day operations of the system. The document also describes in detail the security and audit features of Oracle FLEXCUBE Enterprise Limits and Collateral Management.

1.2 Audience

The document is a prescriptive guide for application implementers, system administrators and related IT personnel.

1.3 Organization of the Document

The document addresses the areas of installation, configuration, deployment and operation of Oracle FLEXCUBE Enterprise Limits and Collateral Management, in the below described manner:

Chapter 1	*About this Manual* gives information on the intended audience. It also lists the various chapters covered in this User Manual.
Chapter 2	*Data Center Practices* prescribes generally accepted practices for installing, configuring and operating the software components of Oracle FLEXCUBE Enterprise Limits and Collateral Management in a data center.
Chapter 3	*Oracle Database Security* describes the measures to be undertaken to harden and secure the Oracle Database Server in the Oracle FLEXCUBE ELCM installation.
Chapter 4	*Application Server Security* describes the measures to be undertaken to harden and secure the Oracle WebLogic Server in the Oracle FLEXCUBE ELCM installation.
Chapter 5	*Desktop Security* provides information about practices to be employed for client workstations.
Chapter 6	*Oracle FLEXCUBE Enterprise Limits and Collateral Management Controls* provides information about controls within the product.

2. Data Center Practices

2.1 Overview

The following guidelines are recommended to secure the host servers (Application Server, Database Server and others) in an installation of Oracle FLEXCUBE ELCM.

2.2 Physical System Security

It is highly recommended to operate servers in a secured data center to prevent unauthorized users or operating personnel from tampering with the machines.

2.3 Minimize the Server Footprint

Each logical software component (Application Server, Database Server etc.) in the installation should preferably operate in a dedicated server. It is not recommended to operate multiple services like mail, FTP, LDAP etc. on the same server, unless absolutely necessary.

It is preferable to customize the operating system installation so that only the minimum set of software components is installed.

Development tools should not be installed on the production servers. In cases where a software package should be compiled and built before installation, it is advisable to perform the build process on a separate machine, following which installation of the binary can be performed on the server.

Samples and demos should not be deployed on a production server, since they are bound to be developed without considering security. Any bugs in such software can be exploited by an attacker resulting in a security incident.

2.4 Operating System Users and Groups

It is recommended to minimize the number of user accounts on the host, for easier auditing and management. Besides, it reduces the risk of unauthorized personnel accessing the server.

It is recommended to create user accounts with names that are not easily guessable. There should be at least two system administrator accounts for a server, to ensure backup in the eventuality of one account being locked.

Passwords for all accounts should be strong passwords – this should be enforced by the operating system, for instance, via the ***pam*** configuration in UNIX. Passwords should not be easy to guess, and neither should they be stored in an insecure media, or written down for easy remembrance.

Passwords should be set to expire periodically; 60-90 days is the recommended period. Passwords for privileged accounts may have a shorter lifecycle.

2.5 Restrict File System Access

It is recommended to use a file system that allows maintenance of access rights.

In Windows, NTFS allows for ACLs to be maintained at the most granular level; however, due care should be exercised when granting file system privileges to the “Everyone” group. Similarly, in UNIX like operating systems, privileges should not be granted to the “Nobody” user and group, unless absolutely required.

2.6 Network Perimeter Protection

Firewall rules should be established to ensure that only a required set of services is accessible to machines outside the data center. Network access can be further restricted to ensure that only certain subnets with trusted machines, and not all machines, can access machines in the data center.

Oracle Financial Services does not recommend exposing the application server hosting Oracle FLEXCUBE ELCM to the Internet.

2.7 Network Service Protection

Network services installed on the server should be enabled only to serve the primary business function(s) that the server must provide. Disable all services that are not needed to serve a justified business need.

Review the network services (like mail and directory services) running on the servers to ensure that they are adequately protected from abuse by an attacker.

Also review and limit the network file shares on the servers, to reduce the risk of an attack on the file system. It is recommended to share files and directories on servers only to trusted machines in the network.

2.8 Usage of Protected Ports

It is not recommended to execute long processes like application servers and database servers under the root account, since a compromise of such processes will result in an attacker gaining elevated privileges.

Therefore, limit the use of protected ports (port numbers less than 1024 on UNIX like operating systems), since they require the use of a privileged user account (in most cases, this is only the root account). Consider the use of NAT to map protected ports to unprotected ones.

2.9 Installation of Software in Production Mode

It is highly recommended to install production builds of any software on production servers. For example, Oracle WebLogic Server should be installed in the production mode, as opposed to the default of development mode. The Oracle Database Server should be installed with options required for production usage (for instance, do not install the sample schemas).

Moreover, it is highly recommended to refer to the manuals and documentation provided by the software supplier, for installing and operating such software securely in a production environment.

2.10 Software Updates and Patches

It is recommended to subscribe to security bulletins and advisories published by software vendors to ensure that critical servers are always up to date.

Oracle Financial Services recommends that patches be tested to ensure that they do not conflict with the normal operation of the system.

2.11 Usage of Security Appliances and Software

Consider the usage of security appliances and software to monitor and ensure that the production environment continues to be secure after the process of server preparation.

Intrusion Detection Systems can be employed to monitor for security sensitive changes in the system and alert personnel. Antivirus scanners can be used to prevent the server(s) from being compromised. Note that, although UNIX like operating systems may have better defenses against viruses (and other malware), consider running antivirus scanners on servers regardless of the OS.

2.12 Configure Security Auditing

Most server operating systems (Linux OS with kernel version 2.6 onwards, IBM AIX, Microsoft Windows Server 2003 etc.) allow for auditing file and directory access. Oracle Financial Services recommends enabling this feature in order to track file system access violations. It is not recommended to enable audit for normal file access operations; audits should preferably contain records of violations to reduce the amount of noise in the logs.

Administrators should ensure sufficient disk space for the audit log. Additionally, administrators should factor the increase on server load due to auditing being enabled.

2.13 Separation of Concerns

It is not recommended to perform development of any kind on a production machine. The standard practice is to establish a separate development environment for developers, isolated from the testing/staging and production environments. Additional environments can be created for other purposes (for instance, a post-production support environment).

2.14 Backup Controls

Back-ups should be taken regularly. This will minimize downtime if there is an emergency. Access to the application areas should not be at the operating system level. On-line archival of redologs should be set up from the date of going live. It is recommended that:

- Backup of all database related files viz., data files, control files, redologs, archived files, init.ora, config.ora etc should be taken at the end of the day.
- The tape can be recycled every week by having day-specific tapes.
- On-line backup of archived redo-log files onto a media to achieve to the point recovery in case of crash, shutdown etc.(recycled every day)
- Complete export of database and softbase should be done atleast once in a week and this can be stored off-site (media can be recycled in odd and even numbers).
- Complete backup of the Oracle directory (excluding the database related files) to be taken once in a month. This media can be recycled bimonthly.
- When the database is huge, incremental exports and on-line tablespace backups are recommended.

The above strategy may be improvised by the Oracle DBA, depending on the local needs. The backup operations are to be logged and tapes to be archived in fireproof storages.

3. Oracle Database Security

3.1 Overview

This section contains security recommendations for the Database.

3.2 Hardening

Review database links in both production and development environments. Unwanted links need to be dropped.

3.3 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.

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

REMOTE_OS_AUTHENT=FALSE

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> PASSWORD or SQL>PASSWORD USERNAME

Always password command should be used because the password is sent unencrypted over the net (without Advanced Security Option) if the alter user syntax is used.

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

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

3.4 Authorization

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

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

REMOTE_OS_ROLES=FALSE

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

3.5 Audit

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

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.

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 any changes to the standard FCELCM 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;
```

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
```

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.

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).

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.

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

It must be noted that auditing features can impose a significant performance overhead. Auditing should thus be limited to the set of items outlined above. Auditing application schema objects should be strictly avoided.

3.6 Secure Database Backups

RMAN secure backup should be used to ensure that the backups stolen from your system cannot be restored in another remote system. Additionally, data masking - a feature offered by Oracle Enterprise Manager – can be used to move data from your production environment to a test environment. Both these are very crucial steps towards securing confidential customer data.

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.

3.7 Separation of Roles

It is vital to ensure that roles and responsibilities of database administrators and application users/administrators are clearly segregated. Database administrators should not be allowed to view or access customer data. Oracle Database vault helps to achieve this separation of duty by creating different realms, factors and rule sets. It can enforce policies that prevent a DBA from accessing an application realm. The product has a set of configuration policies that can be directly implemented with database vault. Implementation specific requirements can be imposed over and above these.

3.8 Securing Audit Information

Oracle Audit vault is an audit solution that consolidates, detects, monitors, alerts and reports n audit data for security auditing an compliance. Oracle Audit vault provides mechanisms to collect audit data from various oracle database. It helps to consolidate audit data from multiple systems into a single centralized repository. Thus, DBA's of individual systems will not be able to tamper with audit information of their respective databases.

3.9 Advanced Security

Oracle Advanced Security provides industry standards-based data privacy, integrity, authentication, single sign-on, and access authorization in a variety of ways. Sensitive information that is stored in your database or that travels over enterprise networks and the Internet can be protected by encryption algorithms. An encryption algorithm transforms information into a form that cannot be deciphered without a decryption key. Oracle Advanced Security supports multiple industry standard encryption algorithms such as RC4, DES3 and Triple-DES. To ensure the integrity of data packets during transmission, Oracle Advanced Security can generate a cryptographically secure message digest using MD5 or SHA-1 hashing algorithms and include it with each message sent across a network.

4. Database Operating Environment Security

4.1 Overview

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.

4.2 Hardening

- 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.

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.

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

- Electronic Mail

FCELCM may require access to a SMTP Mail Transfer Agent (SMTP MTA) typically send mail. This is required for outbound emails, typically notifications from FCELCM (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

4.3 Authentication

Good security requires secure accounts.

- 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.
- 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.

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.

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

4.4 Authorization

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.

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.

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

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.

4.5 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 behaviour. Also check the snort logs.

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.

5. Application Server Security

5.1 Overview

This section describes how to secure the Oracle WebLogic Server production environment that hosts the Oracle FLEXCUBE Enterprise Limits and Collateral Management environment.

5.2 Installation of Oracle WebLogic Server

By default, Oracle WebLogic Server is installed with a JDK and several development utilities. These are not required in a production environment.

The installation footprint of Oracle WebLogic Server can be reduced via the following measures:

- During installation of Oracle WebLogic Server, customize the components to be installed. The following components are not required by Oracle FLEXCUBE Enterprise Limits and Collateral Management in a production environment:
- Oracle WebLogic Workshop
- Web 2.0 HTTP Pub-Sub Server
- Third Party JDBC Drivers (for MySQL and Sybase)
- WebLogic Server examples
- Delete the Pointbase database which is not required for production usage.

5.3 Securing the WebLogic Server installation

Once installed, the measures listed below can be employed to secure the WebLogic Server installation.

5.3.1 Network perimeter protection

It is highly recommended to employ the use of a firewall (as hardware or software) to lockdown the network access to the WebLogic cluster.

For additional information on planning the firewall configuration for a WebLogic Cluster, refer to the section “Security Options for Cluster Architectures” in the “Using Clusters” guide of the Oracle WebLogic Server documentation.

5.3.2 Operating System Users and Groups

It is highly recommended to run the WebLogic Server as a limited user process. The root user account in Unix/Linux and the Administrator account in Windows should not be used to run WebLogic Server since they are privileged user accounts. Other privileged accounts should also not be used to run the WebLogic server.

Hence, it is preferable to create a limited user account say “WebLogic Owner” for running the application server. Additional user accounts are not recommended; in the eventuality, that an additional account is required (say, if the WebLogic owner account is locked out), one of the system administrator accounts can be used to remedy the situation. Having two system administrator accounts is recommended, as it always ensures backup.

5.3.3 File System Access to OS Users

Access rights to the Oracle Home, WebLogic Server product directory, and the WebLogic domain directories should be provided only to the “WebLogic Owner” user. Privileged users will anyway have access to the WebLogic Server installation, by default.

Users in the “Others” category can be restricted from reading the afore-mentioned directories.

Ensure that the following files in the WebLogic installation are available only to the WebLogic owner:

- The security LDAP database which is usually located in the WL_HOME\user_projects\domains\ DOMAIN_NAME\servers\SERVER_NAME\data\ldap\ldapfiles directory
- The keystore used in the keystore configuration of the server(s)
- The Root Certificate Authority keystore

Oracle WebLogic Server provides persistent stores for several subsystems, some of which are utilized by Oracle FLEXCUBE ELCM. Ensure that access to the persistent file stores based on files is restricted to the WebLogic owner OS user. The default persistent file store is located in the *data**store**default* directory under the *servername* subdirectory under the WebLogic domain’s root directory. If custom (user-defined) persistence stores have been created, the same restrictions should be applied on the files and directories used by such stores.

5.3.4 Usage of Protected Ports

In the case of Oracle WebLogic Server

- Operate WebLogic Server using an unprivileged account, bind to unprotected ports, and use NAT to map protected ports to the unprotected ports.
- Configure WebLogic Server to start with a privileged account, bind to protected ports, and then change the user account to an unprivileged user account. For this purpose, Oracle WebLogic Server on UNIX needs to be configured to have a post-bind user ID or group ID. For additional details, refer to the section “Create and configure machines to run on UNIX” in the “Administration Console Online Help”.

5.3.5 Choice of the SSL cipher suite

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

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

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

```
....

<ssl>
```

```
      <enabled>true</enabled>

      <ciphersuite>TLS_RSA_WITH_AES_256_CBC_SHA</ciphersuite>

      <ciphersuite>TLS_RSA_WITH_AES_128_CBC_SHA</ciphersuite>

      <ciphersuite>TLS_RSA_WITH_RC4_128_SHA</ciphersuite>

      <ciphersuite>TLS_RSA_WITH_RC4_128_MD5</ciphersuite>

</ssl>

....
```

Note the following:

- Configuration of WebLogic Server to support the above defined cipher suites might also require an additional command line argument to be passed to WebLogic Server, so that a FIPS 140-2 compliant crypto module is utilized. This is done by adding **-Dweblogic.security.SSL.nojce=true** as a JVM argument.
- The restriction on cipher suites needs to be performed for every managed server.
- The order of cipher suites is important – Oracle WebLogic Server chooses the first available cipher suite in the list, that is also supported by the client.
- Cipher suites with RC4 are enabled despite it being second best to AES. This is primarily for older clients that do not support AES (for instance, Microsoft Internet Explorer 6, 7 and 8 on Windows XP).
- Cipher suites using Triple DES (3DES) are not listed since the maximum effective security provided by the algorithm is 112 bits.

5.3.6 Usage of WebLogic Connection Filters

Although firewalls restrict the ability of machines to communicate with the WebLogic Server, machines in the data center can still access network services provided by the WebLogic Server.

Configure the Oracle WebLogic Server installation to use connection filters to ensure that only certain machines in the data center can access the WebLogic Server services like HTTP, LDAP, RMI-IIOP etc.

5.3.7 Usage of Domain-wide Administration Port for Administrative Traffic

When Oracle WebLogic Server is configured to enable administrative access via the administration port, data is exchanged over SSL, preventing any attacker from sniffing sensitive information about the WebLogic Server configuration.

Furthermore, once the Administration port is enabled, WebLogic Server will serve administration requests on a dedicated port with dedicated resources. A denial service attack mounted on the HTTP/HTTPS channels will not prevent administrators from logging into the WebLogic Server administration console to take corrective actions.

Hence, it is recommended to enable the use of the administration port. Additionally, employ firewall rules or WebLogic Connection Filters to restrict access to the Administration Port to trusted machines from where administrators can log in.

Do note that the Administration Port requires that SSL be enabled on every Managed Server. Additionally, the administration port will be common across all servers in the domain

Further details on configuring the administration port can be found in the “Administration Console Online Help” guide in the Oracle WebLogic Server documentation.

5.3.8 Secure the Embedded LDAP port

In a WebLogic Server cluster, restrict access to the embedded LDAP server port only to machines in the WebLogic Server cluster, through the user of connection filters.

5.3.9 Disable Remote Access to the JVM Platform MBean Server

The MBean server provided by the JDK (from JDK 5 onwards) provides details in MBeans, containing information about the JVM that is useful for monitoring the JVM process.

Besides the JVM’s platform MBean server, Oracle provides three other MBean servers – the Domain Runtime MBean server, Runtime MBean server and the Edit MBean server. It is possible to configure the Runtime MBean server (that is available on each managed server) as the platform MBean server, allowing JMX clients to access not only the JVM MBeans, but also the WebLogic Server MBeans.

If the Runtime MBean server of WebLogic has been configured as the platform MBean server, enabling remote access creates an access path that is no longer secured by the WebLogic Server Security Framework, but instead by the security features of the Java platform alone. In such a case where remote access to the platform MBean server (and the runtime MBean server) is required, it is recommended that JMX clients access the MBeans via the Runtime MBean server.

Oracle Financial Services recommends that changes once done in this regard, be tested thoroughly for impact on business continuity.

5.3.10 Precautions when using SNMP

It is recommended to refer the WebLogic SNMP Management Guide to configure SNMP agents in Oracle WebLogic Server. Due care must be observed over the usage of SNMP v1 and v2 since passwords are sent over clear text in these older version of the protocol. Additional steps required for securing SNMP v3 communication are outlined in the guide.

Oracle Financial Services recommends that changes once done in this regard, be tested thoroughly for impact on business continuity.

5.4 Securing the WebLogic Security Service

You need to ensure the following.

5.4.1 Enable SSL, but avoid using Demonstration Certificates

Enable the use of SSL so that the servers can be accessed via the SSL listen ports for all supported protocols (including HTTPS).

Oracle WebLogic Server includes demonstration private keys, certificates and trusted certificate authorities that are not intended for use in production. Usage of these keys in production is a security risk due to the free availability of private keys; anyone who has a copy of the WebLogic Server has knowledge of the private keys and can compromise SSL/TLS traffic.

Therefore,

- Use a local CA to issue certificates, or
- Use a root or intermediate CA like VeriSign, Thawte etc. to issue certificates

Oracle Financial Services does not recommend the use of self-signed certificates in production.

Consider avoiding the use of certificates with a MD5 signature; usage of certificates with SHA-1 signatures is recommended. Most root and intermediate CAs have begun phasing out the use of MD5 for signing certificates.

5.4.2 Enforce Security Constraints on Digital Certificates

Oracle WebLogic Server performs certificate validation whenever it establishes an outbound SSL connection, or when a two-way SSL connection is established. As part of certificate validation, WebLogic Server checks if the certificate contains the Basic Constraints extension. Ensuring the presence of the Basic Constraints extension will prevent attackers from generating new certificates to aid in website spoofing.

Ensure the check for Basic Constraints extension is enabled, by verifying whether the following line is absent in the WebLogic Server startup command.

```
-Dweblogic.security.SSL.enforceConstraints=off
```

Also verify if any messages have been logged at WebLogic server boot, providing information about the presence of certificates that could be rejected by clients.

5.4.3 Ensure that Host Name Verification is Enabled

Oracle WebLogic Server implements host name verification when it acts as a SSL client; this prevents main-in-the-middle attacks from being performed against SSL itself.

It should be noted that the Oracle FLEXCUBE ELCM application deployed on WebLogic Server will establish outbound SSL connections in certain scenarios, for instance, when requests are made to the Oracle BI Publisher server. In such an event, Oracle WebLogic Server will behave as a SSL client.

Oracle WebLogic Server will behave as a SSL client in several scenarios besides the outbound SSL requests made by applications deployed on Oracle WebLogic Server. For instance, managed servers will establish SSL connections with the Admin server at boot time. Hence, it is recommended to ensure that host name verification is enabled in Oracle WebLogic Server, which happens to be the secure default.

Oracle Financial Services highly recommends the usage of certificates that will pass verification. Oracle Financial Services also recommends against the usage of demonstration certificates in production. It should be noted that usage of demonstration certificates in a testing or development environment containing a multi-server WebLogic cluster, will result in boot failures for managed servers.

5.4.4 Impose Size and Time Limits on Messages

Consider enforcing constraints on size and on the amount of time taken for a message to arrive at the server. This will ensure protection against denial-of-service attacks against WebLogic Server. Additional details are provided in the Oracle WebLogic Server documentation, in the guide "Securing a Production Environment", and also in the "Administration Console Online Help".

Oracle Financial Services recommends that changes, once done in this regard, be tested thoroughly for impact on business continuity – it is quite possible that WebLogic Server receive valid messages that are large enough to be considered as an attack, when such is not the case.

5.4.5 Restrict the Number of Open Sockets

Consider limiting the number of sockets opened by WebLogic Server, to prevent some forms on denial-of-service attacks. Further details are available in the Oracle WebLogic Server documentation, in the guide "Securing a Production Environment", and also in the "Administration Console Online Help".

Oracle Financial Services recommends that changes, once done in this regard, be tested thoroughly for impact on business continuity – the number of sockets opened is dependent entirely on system load, which is bound to vary across time, and also across installations.

5.4.6 Configure WebLogic Server to Manage Overload

Oracle WebLogic Server can be configured to detect, avoid and recover from overload conditions. Configuring WebLogic Server to manage overload conditions allows for WebLogic Server administrators to connect to it, and take remedial actions. Further details on this topic are available in the Oracle WebLogic Server documentation, in the guide "Securing a Production Environment", and also in the "Administration Console Online Help".

Oracle Financial Services recommends that changes, once done in this regard, be tested thoroughly for impact on business continuity – the definition of an overload condition depends on the system capabilities; therefore, overload conditions are bound to be defined differently for machines of differing capabilities.

5.4.7 User Lockouts and Login Time Limits

The Oracle WebLogic Server guide on "Securing a Production Environment" has a section on configuring user lockouts and login time limits to prevent attacks on user accounts. In general, Oracle FLEXCUBE ELCM does not utilize the WebLogic Security Service for managing FLEXCUBE ELCM user accounts.

Therefore, changes recommended by the WebLogic Server guide should be applied only after assessing the impact on production. The changes applied would be suitable for accounts managed by Oracle WebLogic Server. Note that the WebLogic Server Online Console guide will reference "Compatibility Security" which is deprecated in Oracle WebLogic Server 10.3.

Generally, Oracle FLEXCUBE ELCM employs its own protection mechanisms with respect to user lockouts.

5.4.8 Enable Configuration Auditing

Configuration auditing can be enabled to ensure that changes to any WebLogic resource configuration in the WebLogic domain are audited. Enabling this option also allows for auditing of management operations performed by a user on any WebLogic resource.

For additional details, refer to the “Administration Console Online Help”, and the “Configuring WebLogic Security Providers” section in the “Securing WebLogic Server” guide of the Oracle WebLogic Server documentation.

Note that enabling configuration auditing will affect the performance of the system, even though auditing may be enabled for auditing a few events (including configuration changes).

5.4.9 System Administrator Accounts

Create at least two system administrator accounts (WebLogic user accounts) for administration of the WebLogic server. The first administrator account will be created when the WebLogic domain is created. Create the second account with the Admin security role.

Provide unique names to the administrator accounts that cannot be easily guessed. Oracle Financial Services discourages naming the WebLogic administrator account as ‘weblogic’ with a password of ‘weblogic’.

Again, having two system administrators ensures that at least one system administrator has access to the WebLogic server in the event of the other being locked out.

5.5 Securing the Oracle FLEXCUBE ELCM Application

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

5.5.1 Enforce the Usage of SSL

The FLEXCUBE ELCM Installer allows a deployer to configure FLEXCUBE ELCM such that all HTTP connections to the FLEXCUBE ELCM application are over SSL/TLS. In other words, all HTTP traffic in the clear will be prohibited; only HTTPS traffic will be allowed. It is highly recommended to enable this option is a production environment, especially when WebLogic Server acts as the SSL terminator.

Ensure that the following snippet of code is present in the web.xml file of the FLEXCUBE ELCM web module i.e. in FCJNeoWeb.war.

```
<security-constraint>

      <web-resource-collection>

            <web-resource-name>FLEXCUBE ELCM</web-resource-name>

            <description>All endpoints secured</description>

            <url-pattern>/*</url-pattern>

      </web-resource-collection>

      <user-data-constraint>

            <transport-guarantee>CONFIDENTIAL</transport-guarantee>

      </user-data-constraint>
```

```
</security-constraint>
```

5.5.2 Ensure the Servlet Servlet is Disabled

Oracle FLEXCUBE ELCM does not use the ServletServlet to create default mappings for servlets. All servlets are directly mapped to the required URLs.

Ensure that the following code snippet (or a similar one that uses the weblogic.servlet.ServletServlet) *does not exist* in the web.xml of the Oracle FLEXCUBE ELCM web application.

```
<servlet>
  <servlet-name>ServletServlet</servlet-name>
  <servlet-class>weblogic.servlet.ServletServlet</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>ServletServlet</servlet-name>
  <url-pattern>/myservlet/*</url-pattern>
</servlet-mapping>
```

6. Desktop Security

6.1 Application of Security Patches

Oracle Financial Services highly recommends the following:

- Browsers should be upgraded whenever newer versions are released, for they often include new security features. Additionally, in-built security features of browsers should not be turned off.
- Security patches issued by the Operating System vendor should be applied regularly.
- Updates to anti-virus software and anti-spyware programs should be applied regularly.
- Security Updates to other environmental software like Microsoft Core XML Services (MSXML) should be applied regularly.

Additionally, it is recommended that major upgrades such as browser upgrades and Operating System service packs be tested for impact on business continuity.

6.2 Hardening Microsoft Internet Explorer

Oracle FLEXCUBE ELCM is certified for usage in Microsoft Internet Explorer version 7 and 8. Microsoft has provided guidance for enhancing Internet Explorer security in the following documents for the respective versions of the browsers:

- Internet Explorer 7 Desktop Security Guide
- Internet Explorer 8 Desktop Security Guide

Customers are encouraged to employ the recommendations provided by Microsoft in the above mentioned guides.

Among the guidelines provided in these documents, Oracle Financial Services specifically recommends the following settings to all customers of FLEXCUBE ELCM:

- Certificate Security
- Ensure the usage of SSL 3.0 and TLS 1.0. Disable SSL 2.0 as it is an insecure protocol.
- Privacy Settings
- Set Form autocomplete options to Disabled. This will prevent inadvertent caching of data keyed by users.

In addition to the above, it is recommended to enable the popup blocker with a specific rule to disable popup-blocking for the FLEXCUBE ELCM web application.

Application of the following recommendations from Microsoft is not recommended:

- Privacy Settings
- Empty Temporary Internet Files Folder When Browser is closed – Oracle FLEXCUBE ELCM relies heavily on client-side caching performed by Internet Explorer using this folder. The application will behave slowly after this setting is enabled, since the browser will download resources from the server after every browser restart. Hence, it is not recommended to enable this setting. It should be noted that the details of transactions performed by the FLEXCUBE ELCM users are not cached in the Temporary Internet Files folder (irrespective of this setting).

- Other Security Recommendations
- Do not Save encrypted pages to disk – By default, Internet Explorer stores both encrypted and unencrypted content in the Temporary Internet Files folder. Enabling this setting is bound to cause performance issues (especially when FLEXCUBE ELCM is accessed over HTTPS), since the browser will no longer cache resources. As stated before, details of transactions performed by users will not be cached in the Temporary Internet Files folder (irrespective of this setting).

6.3 Terminal Lockout Policy

Oracle Financial Services recommends that a terminal lockout policy be put in place to automatically lockout unattended PC sessions after a certain duration. This is primarily because Oracle FLEXCUBE ELCM will not lock out the browser session, although it does expire the browser session after certain period of inactivity. Users may however be able to access unattended sessions while the FLEXCUBE ELCM user is still logged in. Hence, organizations are expected to set a corporate policy for handling unattended PC sessions; it is recommended to enable the feature to lock workstations, or to enable password-protected screensavers.

7. Oracle FLEXCUBE Limits Controls

7.1 Overview

This chapter describes the various programs available within Oracle FLEXCUBE, 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.

7.2 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 via the FLEXCUBE ELCM 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 will disable logging across all modules and across all users in the system.

7.3 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.

7.4 Security Violation Report

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

- Time
- The name of the operator
- The name of the function
- The ID of the terminal
- A message giving the reason for the login

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

7.4.1 Sign-on Messages

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

7.5 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

7.6 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.

7.7 Change User Password

Users can use this function to change their passwords. A user password should contain a minimum of six characters (parameterizable). It should be different from the current and two previous passwords. The program will prompt the user to confirm the new password when the user will have to sign-on again with the new password. There's no provision of auto generating password as par as password policy maintained and emailing it to the customer with the user id. Password should be created by the administrator and conveyed to the user manually just as it's given to the new employees of a company. Users need to change it during their first login.

7.8 List of Logged-in Users

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

7.9 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 will be 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 e.g. 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 will have access to the application. The other users will be denied access.

Security Practices Guide
[October] [2013]
Version 12.0.0.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax:+91 22 6718 3001
www.oracle.com/financialservices/