

Oracle E-business (General)

Table of Contents

1. [Practice Safe Cloning](#)
2. [Execute E-Business Suite Security Report](#)
3. [Execute Database Security Report](#)
4. [Change passwords and disable unused default Oracle Applications accounts](#)
5. [Enable Detail Auditing for Key Oracle EBS Tables](#)
6. [Review Unsuccessful Logins](#)
7. [Track last updated details using Who Column Values](#)
8. [Review System Audit Reports](#)
9. [Enable Privileged User and System Activity With OAM](#)
10. [Enable Application Server Trust Level Option](#)
11. [Limit Access to Forms Allowing SQL Query](#)
12. [Limit Access to Security Related Forms](#)
13. [Restrict and review administrative responsibilities assigned to users](#)
14. [Activate Secure Server Authentication to Oracle Application Database Server](#)
15. [Configure Concurrent Manager For Safe Authentication](#)
16. [Minimize usage of shared application accounts](#)
17. [Enable Oracle User Management \(UMX\)](#)
18. [Enable custom password profile options for Oracle Application Login](#)
19. [Use DMZ architecture to manage external/internet implementation](#)
20. [Use SSL\(HTTPS\) between client\(browser\) and web server](#)
21. [Disable unauthenticated access using workflow notification mailer](#)
22. [Hide critical application account passwords in log files](#)
23. [Review GUEST application user account responsibility](#)
24. [Encrypt creditcard and other sensitive information](#)
25. [Database\(Oracle\) Best Practices](#)
26. [Harden external web servers](#)
27. [Enable Application Auditing for critical resources](#)

Sponsored Links

[DBA University](#)

DBA University, Inc. is based in Chicago, USA that is dedicated to the training and placement of Oracle DBAs and Oracle Application DBAs using expert instructors and a world class computer LAB offered through affordable prices.

1. Practice Safe Cloning

Many copies of production environments are created, a.k.a. cloning, for various purposes. These copies are typically used for performance test by DBAs or developers or to test upgrade/patching of the production database. Cloning of production environment to test area introduces several risks to an organization. Oracle provides rapidclone utility to clone Oracle applications environment.

REFERENCE

Metalink Notes: 419475.1

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: PCI-DSS, HIPAA, EU Privacy Law
Categories: Database Tier

2. Execute E-Business Suite Security Report

This built-in report validates the profile option values, seeded application user accounts for security. Use the following procedure to execute the report: Start Oracle E-Business Suite Connect to responsibility Application Diagnostics Select the Diagnose menu option Click button Select Application and select Application "Oracle Application Object Library" Scroll down to group "EbusinessSecurity" Select test name "Best Practices: E-Business Suite Security Tests" Input Parameters (* required) None

MAINOPTIONS

Versions: 12.1.1+, 12+
Compliance: S-OX, PCI-DSS, HIPAA, GLBA, EU Privacy Law
Categories: Database Tier, Application Tier
Architecture: Internet/External, Multi-Node

3. Execute Database Security Report

Start Oracle E-Business Suite Connect to responsibility Application Diagnostics Select the Diagnose menu option Click button Select Application and select Application "Oracle Application Object Library" Scroll down to group "EbusinessSecurity" Select test name "Best Practices: Database Security Tests" Input Parameters (*

required)None

MAINOPTIONS

Versions: 12.1.1+, 12+

Compliance: S-OX, PCI-DSS, HIPAA, GLBA, EU Privacy Law

Categories: Database Tier, Application Tier

Architecture: Internet/External, Multi-Node

4. Change passwords and disable unused default Oracle Applications accounts

Oracle ships seeded user accounts with default passwords. Change the default passwords immediately. Default passwords for database accounts are widely known, and if not changed could allow unauthorized access to various parts of the system. Also, disable unused application account access. In addition, Change SYSADMIN account password

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9

Compliance: S-OX, PCI-DSS, HIPAA, GLBA, EU Privacy Law

Categories: Database Tier, Application Tier

Architecture: Internet/External, Multi-Node

5. Enable Detail Auditing for Key Oracle EBS Tables

Consider auditing some of the key tables that control system security:

ALR_ALERTS

FND_AUDIT_COLUMNS

FND_AUDIT_GROUPS

FND_AUDIT_SCHEMAS

FND_AUDIT_TABLES

FND_CONCURRENT_PROGRAMS

FND_DATA_GROUPS

FND_DATA_GROUP_UNITS

FND_ENABLED_PLSQL

FND_FLEX_VALIDATION

FND_FORM

FND_FORM_FUNCTIONS

FND_GRANTS

FND_MENUS

FND_MENU_ENTIRES

FND_ORACLE_USERID

FND_PROFILE_OPTIONS

FND_PROFILE_OPTION_VALUES

FND_REQUEST_GROUPS

FND_REQUEST_GROUP_UNITS

FND_RESP_FUNCTIONS

FND_USER_RESP_GROUPS

REFERENCE

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Architecture: Internet/External, Multi-Node

6. Review Unsuccessful Logins

The system automatically stores unsuccessful logon attempts in the APPLSYS.FND_UNSUCCESSFUL_LOGINS and ICX.ICX_FAILURES tables. The ICX_FAILURES table holds more information than the FND_UNSUCCESSFUL_LOGINS. Both the FND_UNSUCCESSFUL_LOGINS and ICX_FAILURES tables contain unsuccessful logins via the Personal Home Page (Self Service/Web Interface). Failed Forms logins are logged only to the FND_UNSUCCESSFUL_LOGINS table. This functionality cannot be disabled.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Categories: Application Tier
Architecture: Internet/External, Multi-Node

7. Track last updated details using Who Column Values

For most E-Business Suite tables, database rows are updated with the creation and last update information. The system stores this information in the following columns (known as "Who Columns"):

Who Column Name	Description
CREATION_DATE	Date and Time row was created
CREATED_BY	Oracle Applications user ID from FND_USER
LAST_UPDATE_LOGIN	Login ID from FND_LOGINS
LAST_UPDATE_DATE	Date and Time row as last updated
LAST_UPDATED_BY	Oracle Applications user ID from FND_USERS

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Categories: Database Tier, Application Tier
Architecture: Internet/External, Multi-Node

8. Review System Audit Reports

Oracle E-Business Suite ships standard reports to access signon, unsuccessful signon, responsibility usage, form usage and concurrent request usage. Access these reports through the system administrator responsibility.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA

Categories: Application Tier
Architecture: Internet/External, Multi-Node

9. Enable Privileged User and System Activity With OAM

Oracle Application Manager (OAM) provides screens for monitoring current and past system activity. In addition, OAM provides a framework extensible for running custom OAM reports. Monitoring features include current and historic user activity down to the page access level and current and historical Concurrent Manager activity.

REFERENCE

See Metalink Note 278881.1 for more detailed information

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: PCI-DSS
Categories: Application Tier
Architecture: Internet/External, Multi-Node

10. Enable Application Server Trust Level Option

Responsibilities or applications with the specified level of trust can only be accessed by an application server with at least the same level of trust. Users can see this profile option, but they cannot update it.

REFERENCE

Metalink Note 187403.1

MAINOPTIONS

Categories: Application Tier
Architecture: Internet/External, Multi-Node

11. Limit Access to Forms Allowing SQL Query

To improve flexibility, some forms allow users to enter SQL statements. Unfortunately, this feature may be abused. Restrict access to these forms by assigning the responsibility to a small group of users.

REFERENCE

Form Function Form Name ALR_ALRALERT ALRALERT FND_FNDCPMCP_SYS FNDCPMCP
FND_FNDCPMPE FNDCPMPE FND_FNDFFMDC FNDFFMDC FND_FNDFFMVS FNDDFFMVS
FND_FNDPOMPO FNDPOMPO FND_FNDSCAPP FNDSCAPP FND_FNDSCDDG FNDDSCDDG
FND_FNDSCMOU FNDSCMOU PSB_PSBSTPTY PSBSTPTY MSDCSDFN MSDCSDFN MSDCSDFA
MSDCSDFA MSD_MSDAUDIT MSDAUDIT JTFRSDGR JTFRSDGR JTFBRWKB JTFBRWKB
ONT_OEXPCFVT OEXPCFVT OEXDEFWK OE_DEF_ATTR_DEF_RULES JTFTKOBT JTFTKOBT
JTF_GRID_ADMIN JTFGRDMD JTFGDIAG JTFGDIAG JTFGANTT JTFGANTT WMS_WMSRULEF
WMSRULEF QP_QPXPRFOR QPXPRFOR QP_QPXPTMAP QPXPTMAP GMAWFPCL_F GMAWFPCL

GMAWFCOL_F GMAWFCOL AME_WEB_APPROVALS - PERWSAPI PERWSAPI FFXWSMNG
FFXWSMNG FFXWSDFE FFXWSDFE FFXWSBQR FFXWSBQR PAYWSDAS PAYWSDAS PAYWSDYG
PAYWSDYG PERWSSCP PERWSSCP

MAINOPTIONS

Versions: 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Categories: Application Tier
Architecture: Internet/External, Multi-Node

12. Limit Access to Security Related Forms

Some forms allow users to modify the EBS security setup. Through these forms users could alter security configuration (e.g. grant inappropriate privileges to themselves or to others). Assign users only those responsibilities necessary for them to perform their tasks.

REFERENCE

Form Function Form Name FND_FNDATDAG FNDATDAG Audit Groups FND_FNDATDAI FNDATDAI Audit Installations FND_FNDATDAT FNDATDAT Audit Tables FND_AUDIT_COLUMNS FND_FNDFMFBF FNDFMFBF Forms FND_FNDFMFUN FNDFMFUN Functions FND_FNDMMNNU FNDMMNNU Menus FND_FNDPOMPV FNDPOMPV Profile System Values FND_FNDRSGRP FNDRSGRP Request Groups FND_FNDSCAUS FNDSCAUS Users FND_USER FND_FNDSCPLS FNDSCPLS Web Enabled PL/SQL FND_FNDSCRSP XDP_FNDSCRSP FNDSCRSP Responsibilities

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Categories: Application Tier
Architecture: Internet/External, Multi-Node

13. Restrict and review administrative responsibilities assigned to users

Oracle Applications responsibilities like SYSADMIN responsibility has broad administrative privileges. For this reason, regularly review this list of users having administrative responsibilities including SYSADMIN and product administrative responsibility.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Categories: Application Tier
Architecture: Internet/External, Multi-Node

14. Activate Secure Server Authentication to Oracle Application Database Server

Usually Oracle EBS is deployed in a multi-tier configuration with one database server and many possible middle-tier application servers. The application servers include Apache JSP/Servlet, Forms, Discoverer and

also some client programs such as Application Desktop Integrator. Any program which makes a SQLNet connection to the Oracle Applications database needs to be trusted at some level. The Server Security feature ensures that SQLNet connections originate from trusted machines.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: PCI-DSS, HIPAA
Categories: Database Tier, Application Tier
Architecture: Multi-Node

15. Configure Concurrent Manager For Safe Authentication

Concurrent Manager passes the APPS schema password to concurrent programs on the command line. Because some Operating Systems allow all machine users to read a program's command line arguments, the password may be intercepted. ENCRYPT signals Concurrent Manager to pass the username/password in the environment variable FCP_LOGIN. Concurrent Manager leaves argument \$1 blank. To prevent username/password from being passed, enter SECURE in the Execution Options field. With this change, Concurrent Manager does not pass the username/password to the program.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Categories: Application Tier
Architecture: Internet/External, Multi-Node

16. Minimize usage of shared application accounts

When users share one generic account associating accountability to individual users is a challenge. System cannot identify which user performs a function. Instead, create shared responsibilities which is assigned to multiple users. It helps to share the same functions, reports and permission sets while the system tracks individual user actions.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA
Categories: Application Tier
Architecture: Internet/External, Multi-Node

17. Enable Oracle User Management (UMX)

UMX provides a common user registration flow in which a user can enter a new password or select to have one generated randomly. UMX uses workflow to drive the registration process once a request has been submitted.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+

Categories: Application Tier
Architecture: Internet/External, Multi-Node

18. [Enable custom password profile options for Oracle Application Login](#)

Enabling the profile options support strong application passwords, account lockout after failed logon attempts and session inactivity timeout.

For additional password security custom password rules can be implemented by using Signon Password Custom profile option to define a custom validation Java class. To enable custom password validation for Oracle Application Login Use oracle.apps.fnd.security.PasswordValidation to customize password implementation if SSO is not implemented. The details of the functions are:

Signon Password Case - enables to use upper and lower case chars

Signon Password Failure Limit - control number unsuccessful login attempts

Signon Password Hard To Guess - checks for atleast one char & one number, doesn't contain username and no repeating characters

Signon Password Length - minimum length of the password

Signon Password No Reuse - number of days before which one cannot reuse an old password

Password Expire section in user - define form, to make passwords expire

Oracle supports Single Sign-on(SSO) integration with other enterprise identity management platforms. Check out SSO sections for more details.

REFERENCE

Metalink Notes: 362663.1

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9

Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law

Categories: Database Tier, Application Tier

19. [Use DMZ architecture to manage external/internet implementation](#)

If Oracle EBS is exposed to the external users using internet, implement DMZ, external web-tiers, firewall and reverse proxies in a secure external EBS deployment

REFERENCE

Metalink note: 189367.1

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9

Compliance: PCI-DSS, HIPAA, GLBA, EU Privacy Law

Categories: Application Tier

Architecture: Internet/External, Multi-Node

20. Use SSL(HTTPS) between client(browser) and web server

Information sent over the network and across the internet in http protocol is easily intercepted. Secure sockets layer(SSL) is a well known encryption scheme that ensures safe transfer of data in-transit.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: PCI-DSS, HIPAA, EU Privacy Law
Categories: Desktop Tier, Application Tier
Architecture: Internet/External, Multi-Node

21. Disable unauthenticated access using workflow notification mailer

When the parameter SEND_ACCESS_KEY is set to Y in workflow e-mail notification settings, Oracle EBS suite sign-on process is bypassed since the e-mail notification contains an access key. When set to N, an unauthenticated user who clicks on the notification link must sign-on before accessing the notification details web page.

MAINOPTIONS

Versions: 11.5.10+, 11.5.9
Compliance: S-OX, PCI-DSS, HIPAA, GLBA, EU Privacy Law
Categories: Application Tier

22. Hide critical application account passwords in log files

adpatch utility used for patching Oracle application tier stores passwords in clear text if flags are not properly used during the adpatch execution

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9
Compliance: PCI-DSS, HIPAA, EU Privacy Law
Categories: Application Tier

23. Review GUEST application user account responsibility

Oracle EBS uses GUEST application account to represent unauthenticated user session for certain applications. Limit guest user responsibilities to those necessary for sign-on and guest access.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+
Compliance: S-OX, PCI-DSS
Architecture: Multi-Node

24. Encrypt creditcard and other sensitive information

Oracle Payables, Oracle Order Capture, Oracle Order Management, Oracle Service Contracts, Oracle istore and iPayments modules in Oracle applications store creditcard information of customers. It is recommended that creditcard encryption is enabled using Oracle supplied patch.

For details on this refer Oracle Applications Credit Card Encryption:

Metalink Note: 338756.1

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9

Compliance: PCI-DSS, GLBA

Categories: Database Tier

25. Database(Oracle) Best Practices

Refer to Oracle Database Best Practices at

<http://www.checklist20.com/bestpractices.html#cid=70&cn=Oracle%20Database>

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+, 11.5.9

Compliance: S-OX, PCI-DSS, HIPAA, GLBA, EU Privacy Law

Categories: Database Tier

Architecture: Internet/External, Multi-Node

26. Harden external web servers

If any of the E-biz modules are implemented for external partners and customers, setup external webtier with minimal required codebase.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+

Compliance: S-OX, PCI-DSS, HIPAA, GLBA

Architecture: Multi-Node

27. Enable Application Auditing for critical resources

Set SIGNONAUDIT:LEVEL to "Form" at the site level. At this setting, the system logs all user sign-ons, responsibility selections and form accesses to APPLSYS.FND_LOGINS, APPLSYS.FND_LOGIN_RESPONSIBILITIES and APPLSYS.FND_LOGIN_RESP_FORMS.

MAINOPTIONS

Versions: 12.1.1+, 12+, 11.5.10+

Architecture: Internet/External, Multi-Node

Sponsored Links

[DBA University](#)

DBA University, Inc. is based in Chicago, USA that is dedicated to the training and placement of Oracle DBAs and Oracle Application DBAs using expert instructors and a world class computer LAB offered through affordable prices.