



ORACLE E-BUSINESS SUITE 11i/R12 SECURITY QUICK REFERENCE

VERSION 3.0 – APRIL 2011

1. DEFAULT ORACLE EBS USERS

Default passwords for all standard Oracle EBS user accounts should be changed and all unused accounts should be disabled.

DEFAULT ORACLE APPLICATIONS USERS		
USER NAME	MODULE	DISABLE ¹
AME_INVALID_APPROVER	AME	yes
APPSMGR	AOL/FND	yes
ASADMIN (R12)	AOL/FND	yes
ASGADM	ASG	see module
ASGUEST	AS	see module
AUTOINSTALL	AOL/FND	yes
CONCURRENT MANAGER	AOL/FND	yes
FEEDER SYSTEM	AOL/FND	yes
GUEST ²	AOL/FND	no
IBE_ADMIN	IBE, ONT	see module
IBE_GUEST	IBE	see module
IBEGUEST	IBE, IBU	see module
IEXADMIN	IEX	see module
INDUSTRY DATA (R12)	AOL/FND	yes
INITIAL SETUP	AOL/FND	yes
IRC_EMP_GUEST	IRC	see module
IRC_EXT_GUEST	IRC	see module
MOBADM	ASG	yes
MOBDEV	ASG	yes
MOBILEADM	ASG	see module
OP_CUST_CARE_ADMIN	XDP	see module
OP_SYSADMIN	XDP	see module
ORACLE12.0.0 – ORACLE12.9.0	AOL/FND	yes
PORTAL30	AOL/FND	yes
PORTAL30_SSO	AOL/FND	yes
STANDALONE BATCH PROCESS	AOL/FND	yes
SYSADMIN	AOL/FND	no
WIZARD	AOL/FND	yes
XML_USER	AOL/FND	yes

¹ If the module is not being used, the account can be disabled. Otherwise, see the module documentation for more information on this account.

² Change the GUEST password using the AutoConfig variable “s_guest_pass” and run AutoConfig. See MOS Note ID 43353.1.

2. DEFAULT ORACLE DATABASE ACCOUNTS

All database passwords should be changed including both default Oracle Database accounts as well as all Oracle EBS database accounts. Use FNDCPASS (11.5/12.0) or AFPASSWD (12.1) to change the passwords in both the application and database. Other standard Oracle, third-party, or custom database accounts may exist and default passwords should be changed.

ACCOUNT NAME ⁴	CHANGE PASSWORD METHOD
SYS, SYSTEM	manual
CTXSYS, DBSNMP, OUTLN, ...	manual
APPS, APPLSYS ^{1, 2}	FNDCPASS SYSTEM or AFPASSWD -s
APPLSYSPUB	See note ⁴
EDWREP, ODM	manual
AD_MONITOR, EM_MONITOR	manual
OWAPUB	manual
PORTAL30, PORTAL30_*	manual
SSOSDK	manual
SCHEMAS (ABM ... ZX) ³	FNDCPASS ALLORACLE or AFPASSWD -a

¹ APPS and APPLSYS passwords must be identical.

² After changing the APPS password, AutoConfig must be run.

³ Change all schema passwords (over 250 schemas) – use “FNDCPASS ALLORACLE” or “AFPASSWD -a” to change all.

⁴ Changing the APPLSYSPUB password is recommended. Refer to MOS Note ID 11i/189367.1 or R12/403537.1 for instructions. APPLSYSPUB password must always be uppercase even if the database has case-sensitive passwords enabled.

3. FND CHANGE PASSWORD UTILITY

Change APPS/APPLSYS Passwords

```
FNDCPASS apps/apps @ Y system/manager \  
SYSTEM APPLSYS <new password>
```

Note: AutoConfig must be run and all application tier services restarted after changing the APPS password.

Change Oracle EBS Schema Password (e.g., GL, FA, AR, etc.)

```
FNDCPASS apps/apps @ Y system/manager \  
ORACLE <schemaname> <new password>
```

Change All Oracle EBS Schema Passwords (e.g., GL, FA, AR, etc.)

```
FNDCPASS apps/apps @ Y system/manager \  
ALLORACLE <new password>
```

Change Oracle EBS Application User Password

```
FNDCPASS apps/apps @ Y system/manager \  
USER <username> <new password>
```

Lock All Oracle EBS Schema Accounts (R12.1+)

```
AFPASSWD apps/apps@<twotask> -L TRUE
```

4. SYSTEM PROFILE OPTIONS – SECURITY RELATED

PROFILE OPTION	DEFAULT	SUGGEST
AUDITING		
Sign-On:Audit Level	(null)	Form
Sign-On:Notification	No	Yes
AuditTrail:Activate	No	Yes
Passwords		
Signon Password Failure Limit	(null)	6
Signon Password Hard To Guess (1 letter, 1 number, no repeating characters, not username)	No	Yes
Signon Password Length	5	8
Signon Password No Reuse	(null)	720
Signon Password Case	insensitive	sensitive
Signon Password Custom (see MOS Note ID 362663.1)	(null)	Java Class
Diagnostics		
Utilities:Diagnostics	No	No
FND: Diagnostics	Yes	No
Hide Diagnostics menu entry	No	Yes
Other Security		
Concurrent:Report Access Level	User	User
FND Validation Level	Error	Error
FND Function Validation Level	Error	Error
Framework Validation Level	Error	Error
Restrict text input	Yes	Yes
FND: Developer Mode	(null)	No

5. AUTOCONFIG VARIABLES – SECURITY RELATED

AUTOCONFIG VARIABLE NAME	DEFAULT	SUGGEST
TIMEOUT		
Applications Session Timeout (s_sesstimeout) See MOS Note ID 307149.1	1800000 (30 min)	1800000 (30 min)
OC4J Session Timeout (s_oc4j_sesstimeout)	30 min	30 min
Security		
Application Server Security Authentication (s_appserverid_authentication)	OFF	SECURE
Applications 'GUEST' User (s_guest_pass)	ORACLE	strong password
Applications 'GWYUID' Password (s_gwyuid_pass) (APPLSYSPUB)	PUB	strong password

6. APPLSYSPUB PERMISSIONS

The APPLSYSPUB account should have only these grants –

```
INSERT ON FND_UNSUCCESSFUL_LOGINS
INSERT ON FND_SESSIONS
EXECUTE ON FND_DISCONNECTED
EXECUTE ON FND_MESSAGE
EXECUTE ON FND_PUB_MESSAGE
EXECUTE ON FND_SECURITY_PKG
EXECUTE ON FND_SIGNON
EXECUTE ON FND_WEBFILEPUB
SELECT ON FND_APPLICATION
SELECT ON FND_APPLICATION_TL
SELECT ON FND_APPLICATION_VL
SELECT ON FND_LANGUAGES_TL
SELECT ON FND_LANGUAGES_VL
SELECT ON FND_LOOKUPS
SELECT ON FND_PRODUCT_GROUPS
SELECT ON FND_PRODUCT_INSTALLATIONS
```

These permissions are set in –

```
<FND_TOP>/admin/sql/afpub.sql
```

To check permissions –

```
SELECT * FROM sys.dba_tab_privs
where grantee = 'APPLSYSPUB'
```

7. APPLICATIONS AUDITING (WHO COLUMNS)

Most Oracle EBS tables have information on the creation and last update of a row in the following columns –

- CREATION_DATE
- CREATED_BY → FND_USERS table
- LAST_UPDATE_LOGIN → FND_LOGINS tables
- LAST_UPDATE_DATE
- LAST_UPDATED_BY → FND_USERS table

8. END-USER APPLICATION ACCESS AUDITING

Enable simple logging of user, responsibility, and forms accesses by setting system profile option “**Sign-On: Audit Level**” to “FORM” at the site level.

END-USER AUDIT TABLES

applsys.fnd_logins	applsys.fnd_login_responsibilities
fnd_concurrent_requests	applsys.fnd_login_resp_forms
icx.icx_failures	applsys.fnd_unsuccessful_logins

END-USER AUDIT REPORTS

Signon Audit Users	Signon Audit Concurrent Requests
Signon Audit Responsibilities	Signon Audit Unsuccessful Logins
Signon Audit Forms	

9. DEFAULT ORACLE E-BUSINESS SUITE PORTS

COMPONENT	AUTOCONFIG VARIABLE	PORT # + x
Database	s_dbport	1521
RPC/FNDFS	s_rpcport	1626
Reports Server	s_repsport	7000
Web Server (Apache)	s_webport	8000
	s_webssl_port	4443
	s_active_webport	8000
Web Proxy	s_proxyport	80
JServ oprocmgr (11i)	s_oprocmgr_port	8699
Forms Servlet (jserv) (11i)	s_forms_servlet_portrange	8701-8710
Discoverer Servlet (jserv) (11i)	s_disco_servlet_portrange	8711-8720
XML Servlet (jserv) (11i)	s_xmlsvcs_servlet_portrange	8741-8750
OA Core Servlet (jserv) (11i)	s_oacore_servlet_portrange	8721-8740
Servlet (jserv) – old (11i)	s_servletport	8800
Web Server (moplsq) (11i)	s_web_port_pls	8888
Forms Server	s_formsport	9000
Metrics Server Data	s_metdataport	9100
Metrics Server Requests	s_metreqport	9200
VisiBroker Server Agent	s_osagent_port	10000
MSCA Mobile Server	s_mwaportno	10200-10299
MSCA Mobile Dispatcher	s_mwadispatcher_port	10300-10399 10800-10899
MCSA Telnet Server (R12)	s_mwatelnetportno	10200-10299
JTF Fulfilment Server	s_jtfuf_port	9300 or 11000
TCF Server (not used with forms servlet)	s_tcfport	15000
ONS Local Port (R12)	s_ons_localport	6100
ONS Remote Port (R12)	s_ons_remoteport	6200
ONS Request Port (R12)	s_ons_requestport	6500
Java Object Cache Port (R12)	s_java_object_cache_port	12345
OC4J JMS Port Range for Oacore (R12)	s_oacore_jms_portrange	~23000- 23099
OC4J JMS Port Range for Forms (R12)	s_forms_jms_portrange	~23500- 23599
OC4J JMS Port Range for Home (R12)	s_home_jms_portrange	~24000- 24099
OC4J JMS Port Range for Oafm (R12)	s_oafm_jms_portrange	~24500- 24599
OC4J AJP Port Range for Oacore (R12)	s_oacore_ajp_portrange	~21500- 21599
OC4J AJP Port Range for Forms (R12)	s_forms_ajp_portrange	~22000- 22099
OC4J AJP Port Range for Home (R12)	s_home_ajp_portrange	~22500- 22599
OC4J AJP Port Range for Oafm (R12)	s_oafm_ajp_portrange	~20000- 20099
Oracle Connection Manager Port	s_cmanport	1532

Port numbers may be modified during installation or may be automatically incremented by x during installation where x is a number 1 to 100 (typical less than 10). Port number ranges are often a grouping of 3, 4, 5, or 6 contiguous ports in the specified range.

10. RECOMMENDED FILE PERMISSIONS

PATH	FILES	UNIX PERM
\$ORACLE_HOME	All	0750
\$ORACLE_HOME/bin	All	0751
\$ORACLE_HOME/network/admin/<sid>	listener.ora sqlnet.ora	0600
\$ORACLE_HOME/appsutil/install/<sid>	*.sql *.sh	0600 0700
\$IAS_TOP/Apache/modplsql/cfg (11i)	wdbsvr.app	0600
\$806_HOME/reports60/server (11i)	CGIcmd.dat	0600
\$APPL_TOP/admin/<sid>	defaults.txt adaldefaults.txt	0600
\$FND_TOP/secure	All	0750

11. MY ORACLE SUPPORT (MOS) SECURITY NOTES

Best Practices for Securing the Oracle E-Business Suite (11i/R12)	189367.1 11i 403537.1 R12
DMZ Configuration with Oracle E-Business Suite (11i/R12)	287176.1 11i 380490.1 R12
11i: A Guide to Understanding and Implementing SSL for Oracle Applications/ Enabling SSL in Release 12	123718.1 11i 376700.1 R12
Enabling SSL with Oracle Application Server 10g and the E-Business Suite	340178.1
Encrypting EBS 11i Network Traffic using Advanced Security Option (also for R12)	391248.1
Oracle Applications Credit Card Encryption for 11i	338756.1
Using Transparent Data Encryption (TDE) with the E-Business Suite	403294.1 11i 732764.1 R12 828229.1 R12
Using Oracle Database Vault with Oracle E-Business Suite Releases 11i and 12	950018.1
Configuring Oracle Connection Manager With Oracle E-Business Suite Release 12	558959.1

 **INTEGRIGY**

<http://www.integrigy.com>

Version 3.0 – April 2011
Oracle E-Business Suite 11.5.10 – 12.1.3

Copyright © 2011 Integrigy Corporation

Information in this document is subject to change without notice and does not represent a commitment on the part of Integrigy Corporation. Integrigy does not guarantee or warrant the accuracy or completeness of the information in this document. Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates.