INTEGRIGY

Oracle E-Business Suite 11i/R12 Security Quick Reference

Version 5.2 – April 2018

1. Default Oracle EBS Users

Default passwords for all standard, seeded Oracle EBS application user accounts should be changed and all unused accounts should be disabled by end-dating.

Default Oracle E-Business Suite Users		
User Name	**Module**	**End-date** [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	yes
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	**no** [3]
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 should be end-dated. Otherwise, see the module documentation for more information.

[2] Change the GUEST password using the AutoConfig variable "s_guest_pass" and run AutoConfig. See MOS Note ID 443353.1.

[3] Should not be end-dated, but check that FND_USER table ENCRYPTED_USER_PASSWORD = "INTERNAL USER-NOLOGIN".

2. Default Oracle Database Accounts

All database passwords should be changed including both default Oracle Database accounts as well as all Oracle EBS schema database accounts. Use FNDCPASS (11.5/12.0) or AFPASSWD (12.1/12.2) to change the passwords in both the application and database. Other standard Oracle, third-party, and custom database accounts may exist and default passwords should be changed.

Account Name	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 for R12. 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 0 Y system/manager \
SYSTEM APPLSYS <new password>
```

Note: AutoConfig must be run and application tier restarted.

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

```
FNDCPASS apps/apps 0 Y system/manager \
ORACLE <schemaname> <new password>
```

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

```
FNDCPASS apps/apps 0 Y system/manager \
ALLORACLE <new password>
```

Lock All Oracle EBS Schema Accounts (12.1 – 12.2)

```
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 [1]	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

[1] Not used in R12. See MOS Note IDs 736547.1, 804296.1, 976613.1, and 736547.1 for more information.

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, which are set in `<FND_TOP>/admin/sql/afpub.sql` –

```
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_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
SELECT ON FND_NEW_MESSAGES
```

To check permissions –

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

Verify `EXECUTE on FND_SIGNON` and `SELECT ON FND_USER_VIEW` are not granted to 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 s_webssl_port s_active_webport	8000 4443 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 Serlvet (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 (moplsql) (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	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 Ports Oacore (R12)	s_oacore_jms_portrange	~23000-23099
OC4J JMS Ports for Forms (R12)	s_forms_jms_portrange	~23500-23599
OC4J JMS Ports for Home (R12)	s_home_jms_portrange	~24000-24099
OC4J JMS Ports for Oafm (R12)	s_oafm_jms_portrange	~24500-24599
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 adalldefaults.txt	0600
$FND_TOP/secure	All	0750

11. My Oracle Support (MOS) Security Notes

Secure Configuration Guide for Oracle E-Business Suite Release (11i/R12)	189367.1 (11i) 403537.1 (12.1)
DMZ Configuration with Oracle E-Business Suite (11i/R12)	287176.1 (11i) 380490.1 (12.1) 1375670.1 (12.2)
Enabling SSL/TLS in Oracle E-Business Suite (11i/R12)	123718.1 (11i) 376700.1 (12.1) 1367293.1 (12.2)
FAQ: Oracle E-Business Suite Security	2063486.1
Security Configuration and Auditing Scripts for Oracle E-Business Suite	2069190.1
Using Transparent Data Encryption (TDE) with the E-Business Suite	403294.1 (11i) 828229.1 (12.1) 1585296.1 (12.2)
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 5.2 – April 2018

Oracle E-Business Suite 11.5.10 – 12.0.6 – 12.1.3 – 12.2