



ORACLE APPLICATIONS 11i SECURITY QUICK REFERENCE

VERSION 2.0 – MARCH 2007

1. DEFAULT ORACLE APPLICATIONS USERS

Default passwords for all standard Oracle Applications 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
ASGADM	ASG	see module
ASGUEST	AS	see module
AUTOINSTALL	AOL/FND	yes
CONCURRENT MANAGER	AOL/FND	yes
FEEDER SYSTEM	AOL/FND	yes
GUEST	AOL/FND	no
IBE_ADMIN	IBE, ONT	see module
IBE_GUEST	IBE	see module
IBEGUEST	IBE, IBU	see module
IEXADMIN	IEX	see module
INITIAL SETUP	AOL/FND	yes
IRC_EMP_GUEST	IRC	see module
IRC_EXT_GUEST	IRC	see module
MOBILEADM	ASG	see module
OP_CUST_CARE_ADMIN	XDP	see module
OP_SYSADMIN	XDP	see module
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. DEFAULT ORACLE DATABASE ACCOUNTS

All database passwords should be changed including both default Oracle Database as well as Oracle Applications database accounts. Use the FNDCPASS utility to change the passwords in both the application and database.

ACCOUNT NAME ⁴	CHANGE PASSWORD
SYS, SYSTEM	yes
CTXSYS, MDSYS, ORDSYS, ...	yes
APPS ^{1,2}	yes
APPLSYS ¹	yes
APPLSYSPUB	optional ⁵
EDWREP, ODM	yes
AD_MONITOR	yes
OWAPUB	yes
PORTAL30, PORTAL30_*	yes
SSOSDK	yes
SCHEMAS (ABM ... ZX) ³	yes

¹ APPS and APPLSYS passwords must be identical

² After changing the APPS password, AutoConfig must be run to update the password in the following files:
<iAS_HOME>/Apache/modplsql/cfg/wdbsvr.app
<ORACLE_HOME>/reports60/server/CGIcmd.dat

³ Change all schema passwords – over 250 schemas

⁴ Other standard Oracle, third-party, or custom database accounts may exist and default password should be changed.

⁵ Changing the APPLSYSPUB password is recommended, but may cause issues as the password change is not properly handled by the application. Also, using ADI and other client tools may require the new password.

3. FND CHANGE PASSWORD UTILITY

Change Oracle Database Passwords

FNDCPASS command changes the password in the Applications and in the database.

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

Change Applications User Passwords

```
FNDCPASS apps/apps 0 Y system/manager \
USER <user> <password>
```

4. SECURITY RELATED PROFILE OPTIONS

PROFILE OPTION	DEFAULT	SUGGEST
Sign-On:Audit Level	(none)	Form
Sign-on:Notification	No	Yes
Signon Password Failure Limit	(none)	6
Signon Password Hard to Guess	No	Yes
Signon Password Length	5	8
Signon Password No Reuse	(none)	720
Signon Password Case (RUP4)	insensitive	sensitive
Utilities:Diagnostics	No	No
Concurrent:Report Access Level	User	User
AuditTrail:Activate	No	Yes

“Signon Password Hard to Guess” Rules

- The password contains has the following attributes -
 - at least one letter
 - at least one number
 - does not contain the username
 - does not contain repeating characters

5. 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 dba_tab_privs
where grantee = 'APPLSYSPUB'
```

6. DEFAULT ORACLE APPLICATIONS PORTS

COMPONENT	AUTOCONFIG	PORT #
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 or (80/443)
Web Proxy	s_proxyport	80
JServ oprocmgr	s_oprocmgr_port	8699
Forms Servlet (jserv)	s_forms_servlet_portrange	8701-8710
Discoverer Servlet (jserv)	s_disco_servlet_portrange	8711-8720
XML Servlet (jserv)	s_xmlsvcs_servlet_portrange	8741-8750
OA Core Servlet (jserv)	s_oacore_servlet_portrange	8721-8740
Servlet (jserv) – old	s_servletport	8800
Web Server (moplsq)	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_mwaporntno	10200
MSCA Mobile Dispatcher	s_mwadispatcher_port	10300
JTF Fulfilment Server	s_jtfuf_port	11000
TCF Server (not used with forms servlet)	s_tcfport	15000

Port numbers valid for 11.5.10+. All 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).

8. WEB SESSION TIMEOUT

Should be set in AutoConfig with the variable s_sesstimeout.

Set these two parameters to be equal (30 minutes = 1800000 seconds).

System Profile Option – **ICX: Session Timeout = <minutes>**

```
<ORAHTTP_TOP>/Jserv/etc/zone.properties
```

```
session.timeout=<seconds>
```

9. DATABASE LISTENER

LISTENER PASSWORD

```
listener.ora → PASSWORDS_<listener name>
```

LISTENER ADMIN RESTRICTIONS

```
listener.ora →  
ADMIN_RESTRICTIONS_<listener>=ON
```

LISTENER LOGGING

```
listener.ora → LOG_DIRECTORY  
listener.ora → LOG_FILE  
listener.ora → LOG_STATUS ON
```

VALID NODE CHECKING (8i = protocol.ora, 9i, 10g=sqlnet.ora)

```
tcp.validnode_checking = yes  
tcp.invited_nodes = (x.x.x.x | name, x.x.x.x | name)  
tcp.excluded_nodes=( x.x.x.x | name, x.x.x.x | name)  
(see Managed SQL*Net Access in 11.5.10)
```

COMMON LISTENER SECURITY ERRORS IN LOG

```
TNS-01169 → Invalid listener password attempt  
TNS-12508 → Blocked by ADMIN_RESTRICTIONS
```

7. APPLICATIONS AUDITING (WHO COLUMNS)

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

10. APPLICATIONS AUDITING (END-USER)

Enable auditing by setting System Profile Option **Sign-On: Audit Level** to FORMS at the site level.

END-USER AUDIT TABLES

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

END-USER AUDIT REPORTS

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

11. 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	wdbsvr.app	0600
\$806_HOME/reports60/server	CGIcmd.dat	0600
\$APPL_TOP/admin/<sid>	defaults.txt adadefaults.txt	0600
\$FND_TOP/secure	All	0750

12. METALINK 11i SECURITY NOTES

Best Practices for Securing the Oracle E-Business Suite 11i	189367.1
DMZ Configuration with Oracle E-Business Suite 11i	287176.1
11i: A Guide to Understanding and Implementing SSL for Oracle Applications	123718.1
Enabling SSL with Oracle Application Server 10g and the E-Business Suite	340178.1
Encrypting EBS 11i Network Traffic using Advanced Security Option / Advanced Networking Option	391248.1
Oracle Applications Credit Card Encryption	338756.1
Using Transparent Data Encryption (TDE) with the eBusiness Suite (EBS)	403294.1



<http://www.integrigy.com>

Version 2.0 – March 2007

Oracle Applications 11.5.7 – 11.5.10 CU2

Copyright © 2007 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, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates.