

ORACLE APPLICATIONS 11i SECURITY QUICK REFERENCE

Version 1.2 – December 2004

DEFAULT ORACLE APPLICATIONS USERS

Default passwords for all standard Oracle Applications users accounts should be changed and all unused accounts should be disabled.

Default Oracle Applications Users		
User Name	Module	Disable ¹
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

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

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>
```

DEFAULT ORACLE DATABASE ACCOUNTS

Account Name	Change Password
SYS	✓
SYSTEM	✓
APPS ^{1,2}	✓
APPLSYS ¹	✓
APPLSYSPUB	
CTXSYS	✓
DBSNMP	✓
OWAPUB	✓
PORTAL30	✓
PORTAL30_SSO	✓
SCHEMAS (ABM ... XTR) ³	✓

¹ APPS and APPLSYS passwords must be identical

² APPS password must be changed in these files:
 <IAS_HOME>/Apache/modplsql/cfg/wdbsvr.app
 <FND_TOP>/resource/wfmail.cfg
 <ORACLE_HOME>/reports60/server/CGIcmd.dat

³ Change all schema passwords – over 200 schemas

WEB SESSION TIMEOUT

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>
```

SECURITY RELATED PROFILE OPTIONS

Profile Option	Default	Suggest
Sign-On: Audit Level	(none)	FORM
Sign-on: Notification	No	Yes
Signon Password Failure Limit	(none)	3
Signon Password Hard to Guess	NO	YES
Signon Password Length	5	6
Signon Password No Reuse	(none)	365
Utilities: Diagnostics	No	No
Concurrent: Report Access Level	User	User
AuditTrail: Activate	No	Yes

“Signon Password Hard to Guess” Rules

- The password contains at least one letter and at least one number.
- The password does not contain the username.
- The password does not contain repeating characters.

APPLSYSPUB PERMISSIONS

The APPLSYSPUB account should have limited permissions. These permissions 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_SIGNON
EXECUTE ON FND_WEBFILEPUB
SELECT ON FND_LOOKUPS
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_PRODUCT_GROUPS
SELECT ON FND_PRODUCT_INSTALLATIONS
```

To check permissions;

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

DEFAULT ORACLE APPLICATIONS PORTS

Component	Port #
Database	1521
RPC/FNDFS	1526
Reports Server	7000
Web Server (Apache)	8000
Forms Server	9000
Servlet	8880
TCF Server	15000
Metrics Server Data	9110
Metrics Server Requests	9120

DATABASE LISTENER

Listener Password

listener.ora → PASSWORDS_<listener name>

Listener Logging

listener.ora → LOG_DIRECTORY

listener.ora → LOG_FILE

listener.ora → LOG_STATUS ON

Valid Node Checking (8i = protocol.ora, 9i=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)

DATABASE AUDITING

Enable auditing by setting **audit_trail** to TRUE or DB in the init.ora file.

Audit Statement	Description
audit session;	Session auditing – connects to the database
audit user;	Create, alter, and drop user
audit database link;	Create or drop database links
audit public database link;	Create or drop public database links
audit system audit;	Audit and noaudit statements

To check current system-level audit options –

```
select * from DBA_STMT_AUDIT_OPTS
select * from DBA_PRIV_AUDIT_OPTS
```

To check current object-level audit options –

```
select * from DBA_OBJ_AUDIT_OPTS
where owner = <owner>
and object_name = <name>
```

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

APPLICATIONS AUDITING (AUDITTRAILS)

1. Set System Profile Option **AuditTrail:Activate** to TRUE
2. **Security -> AuditTrail -> Install** to set schemas for auditing
3. **Security -> AuditTrail -> Groups** to create audit groups and set tables to be audited. Set audit group to **Enabled Requested**
4. **Security -> AuditTrail -> Tables** to set columns in tables to be audited
5. Run **AuditTrail Update Tables** to activate auditing

AuditTrails Objects

- Shadow Table = <table name>_A
- Update Trigger = <table name>_AU
- Insert Trigger = <table name>_AI
- Delete Trigger = <table name>_AD
- Changes View = <table name>_AV#
- Complete View = <table name>_AC#

Suggested Tables to Audit

FND_AUDIT_GROUPS
FND_AUDIT_SCHEMAS
FND_AUDIT_TABLES
FND_AUDIT_COLUMNS

Other Possible Tables to Audit

FND_FORM
FND_FORM_FUNCTIONS
FND_MENUS
FND_MENU_ENTIRES
FND_REQUEST_GROUPS
FND_REQUEST_GROUP_UNITS
FND_USER_RESP_GROUPS
FND_RESP_FUNCTIONS
ALR_ALERTS
FND_CONCURRENT_PROGRAMS
FND_DATA_GROUPS
FND_DATA_GROUP_UNITS
FND_ORACLE_USERID

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

**INTEGRIGY**

Integrigy Corporation
2052 Lincoln Park West, Suite 1301
Chicago, Illinois 60614
888/542-4802
sales@integrigy.com

Oracle Applications 11i Security Quick Reference

Version 1.2 – December 2004

Oracle Applications 11.5.1 – 11.5.10

Copyright © 2003, 2005 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 is a trademark of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates.