

*Best Practices for Securing
Oracle E-Business Suite*

Oracle Corporation

Version 3.0.1

ORACLE®

Latest version of this document available under [Metalink Note 189367.1](#).

Revision History

Version	Release Date	Descriptions
1.2	May 2002	Version 1.2 of the Best Practices for Security E-Business Suite.
2.0	May 2003	Update for new features.
2.1	Jan 2004	Minor Edits.
3.0	Dec 2004	Major Rewrite, new sections, expanded advice, focus on 11.5.9 and above.

Copyright © 2002, 2003, 2004, Oracle. All rights reserved.

Primary Authors: Andy Philips, Ashok Subramanian

Contributors: David Kerr, George Buzsaki, Erik Graversen, Deepak Louis, Rajiv Muthyala, Remi Aimsuphanimit, Emily Nordhagen.

Excerpts of documents [IntA, IntB] reproduced with permission from Integrigy Corporation.

This document is provided for informational purposes only and the information herein is subject to change without notice. Please report any errors herein to Oracle Corporation by filing a documentation bug against product code 510, component SEC_COMP. Oracle Corporation does not provide any warranties covering and specifically disclaims any liability in connection with this document.

Oracle is a registered trademark.

Oracle Corporation World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
650.506.7000
Fax 650.506.7200
Worldwide Support:
<http://www.oracle.com/support>

Table of Contents

Overview	1
System Wide Advice	2
Oracle TNS Listener Security	3
Hardening	3
Network	3
Authentication	4
Authorization	5
Audit	5
Oracle Database Security	7
Hardening	7
Authentication	7
Authorization	9
Audit	10
Oracle Application Tier Security	13
Hardening	13
Authorization	15
Audit	18
E-Business Suite Security	19
Hardening	19
Network	20
Authentication	21
Authorization	24
Audit	26
Advanced Audit	28
Desktop Security	31
Hardening	31
Operating Environment Security	33
Hardening	33
Network	34
Authentication	35
Authorization	36
Maintenance	36
Extras for Experts	39
Detect and Prevent Duplicate User Sessions	39
Customize Password Validation	39
Advanced Security/Networking Option (ASO/ANO)	39
Configure Listener on a Non-Default .dbc Port	40
Multi-Node Topology	40
Hardening External Procedure (EXTPROC) Services	40
Appendix A: Security Setup Forms	45
Appendix B: Security Setup Forms That Accept SQL Statement	47
Appendix C: Processes Used by E-Business Suite	49
Appendix D: Ports Used by E-Business Suite	51
Appendix E: Sample Linux Hardening of the Application Tier	53
Appendix F: References & More Resources	57

Table of Contents

Security Checklist

This section contains a summary of this document's best practice suggestions and their page locations. Use this summary as a security reference guide or checklist.

Overview

- Keep software up to date 2
- Restrict network access to critical services 2
- Follow the principle of least privilege 2
- Monitor system activity 2
- Keep up to date on latest security information 2

Oracle TNS Listener Security

- Harden operating environment 3
- Add IP restrictions or enable Valid Node Checking 3
- Specify connection timeout 4
- Enable TNS Listener password 4
- Enable admin restrictions 5
- Enable TNS Listener logging 5

Oracle Database Security

- Harden operating environment 7
- Disable XDB 7
- Review database links 7
- Remove operating system trusted remote logon 7
- Implement two profiles for password management 8
- Change default installation passwords 8
- Restrict access to SQL trace files 9
- Remove operating system trusted remote roles 9
- Limit file system access within PL/SQL 9
- Limit dictionary access (11.5.10 only) 9
- Revoke unnecessary grants to APPLSYSPUB 9
- Configure the database for auditing 10
- Audit database connections 10
- Audit database schema changes 11
- Audit other activities 11
- Audit administrators and their actions 11
- Review audit records 11
- Maintain audit records 12
- Secure audit records 12

Oracle Application Tier Security

- Harden operating environment 13
- Remove application server banner 13
- Remove unnecessary directives 13
- Turn off directory indexing 14
- Unload Apache autoindex module 14
- Disable XSQL 15
- Prevent search engine indexing 15
- Protect administrative web pages 15
- Protect administrative servlet pages 16
- Disable test pages 17
- Configure mod_plsql 17
- Remove unneeded DAD configurations 17
- Enable mod_plsql custom authorization 17
- Restrict mod_plsql web administration 18
- Configure logging 18

E-Business Suite Security

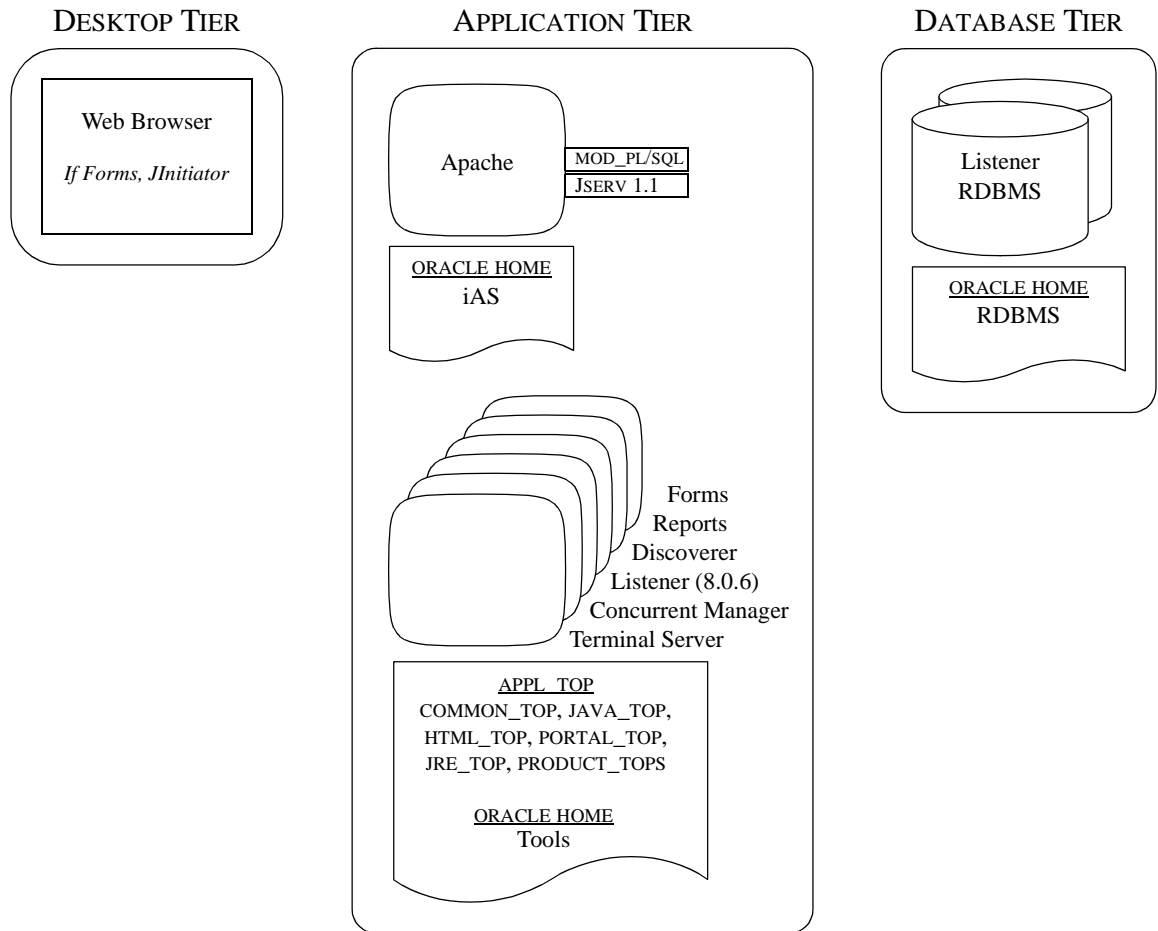
- Harden operating environment 19
- Strike passwords from adpatch logs 19
- Set Workflow notification mailer SEND_ACCESS_KEY to N 20
- Set Tools environment variables 20
- Use SSL (HTTPS) between browser and web server 20
- Use Terminal Services for client-server programs 20
- Change passwords for seeded application user accounts 21
- Tighten logon and session profile options 21
- Create new user accounts safely 22
- Create shared responsibilities instead of shared accounts 22
- Configure Concurrent Manager for safe authentication 22
- Activate Server Security 22
- Review Guest user responsibilities 24
- Review users with administrative responsibilities 24
- Limit access to security related forms 24
- Limit access to forms allowing SQL entry 24
- Set other security related profile options 24
- Restrict responsibilities by web server trust level 24
- Set Sign-On audit level 26
- Monitor system activity with OAM 26
- Retrieve audit records using Reports 26
- Retrieve audit records using SQL 26
- Purge audit records 27
- Review data tracked (no Reports available) 27

Security Checklist

<input type="checkbox"/> Configuring audit trail	28
<input type="checkbox"/> Generate and identify audit trail objects	28
<input type="checkbox"/> Choose tables to audit	28
<input type="checkbox"/> Retrieve audit records using SQL	29
<input type="checkbox"/> Purge audit records	29
<input type="checkbox"/> References on E-Business Suite auditing	29
Desktop Security	
<input type="checkbox"/> Configure browser	31
<input type="checkbox"/> Update browser	31
<input type="checkbox"/> Turn off AutoComplete in Internet Explorer	31
<input type="checkbox"/> Set policy for unattended PC sessions	31
Operating Environment Security	
<input type="checkbox"/> Cleanup file ownership and access	33
<input type="checkbox"/> Cleanup file permissions	33
<input type="checkbox"/> Lockdown operating system libraries and programs	33
<input type="checkbox"/> Filter IP packets	34
<input type="checkbox"/> Prevent spoofing	34
<input type="checkbox"/> Secure telnet connections	35
<input type="checkbox"/> Secure ftp connections	35
<input type="checkbox"/> Verify network configuration	35
<input type="checkbox"/> Monitor for attacks	35
<input type="checkbox"/> Configure accounts securely	35
<input type="checkbox"/> Limit root access	35
<input type="checkbox"/> Manage user accounts	36
<input type="checkbox"/> Restrict guest accounts	36
<input type="checkbox"/> Secure NFS	36
<input type="checkbox"/> Secure operating system Devices	36
<input type="checkbox"/> Secure scripts	36
<input type="checkbox"/> Secure executables	36
<input type="checkbox"/> Secure file access	36
Extras for Experts	
<input type="checkbox"/> EXTPROC Listener Configuration	41
<input type="checkbox"/> EXTPROC Testing Procedure	42

Security Checklist

Overview



In today's environment, a properly secured computing infrastructure is critical. When securing the infrastructure, a balance must be struck between risk of exposure, cost of security and value of the information protected. Each organization determines its own correct balance. To that end, we provide best practices (practical advice) for securing Oracle's E-Business Suite.

The recommendations that follow cross three tiers of machines (browser, application middle-tier and database) and fall into five categories (hardening, network security, authentication, authorization and auditing). We cover security for the Database and Listener, the Application Server, the E-Business Suite and individual desktops. We follow this with advice for hardening operating systems including a sample Linux hardening (in the Appendix). The last section "Extras for Experts" collects together advice that goes beyond the typical best practice.

Each section contains advice spanning five categories:

- **Hardening** Covers hardening the file system, programs, products and configuration.
- **Network** Covers physical topology, firewalls, IP restrictions at web server and database listener.
- **Authentication** Covers account management, password management and other account related activities.
- **Authorization** Covers restrictions to executables, data files, web pages, administrative tools, etc.
- **Audit** Covers configuration, on-going review and purging.

SYSTEM WIDE ADVICE

Some advice applies to the entire E-Business deployment and the infrastructure in which it operates.

KEEP SOFTWARE UP TO DATE

One of principles of good security practice is to keep all software versions and patches up to date. Throughout this document, we assume an E-Business Suite maintenance level of 11.5.9 or later. The latest version of Autoconfig (TXK) configures a system following advice from this document. It also contains a patch set checker to assist with patch application. This cannot be emphasized enough, for many reasons including good security practice, move to the latest version of Autoconfig and Patch Tools (AD).

RESTRICT NETWORK ACCESS TO CRITICAL SERVICES

Keep both the E-Business application middle-tier and the database behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

If firewalls cannot be used, be certain to configure the TNS Listener Valid Node Checking feature which restricts access based upon IP.

Restricting database access often causes application client/server programs to fail. To resolve this, consider using static IP address, dynamic IP address, a software/hardware VPN or Windows Terminal Services or its equivalent.

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

The principal of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, etc., especially early on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

MONITOR SYSTEM ACTIVITY

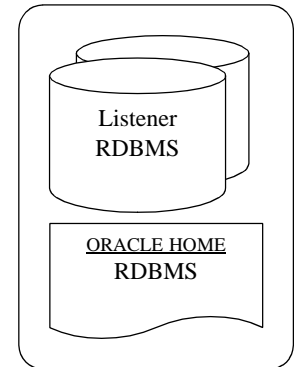
System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

KEEP UP TO DATE ON LATEST SECURITY INFORMATION

Oracle improves its software and documentation. Check this note yearly for revisions.

Oracle TNS Listener Security

DATABASE TIER



Oracle clients communicate with the database using the Transparent Network Substrate (TNS) protocol. When the Listener receives a connection request (port 1521, by default), it starts up a new database process and establishes a connection between the client and the database.

This section contains security recommendations for the TNS Listener.

HARDENING

HARDEN OPERATING ENVIRONMENT

Follow the hardening instructions for “Operating Environment Security” on page 33.

NETWORK

ADD IP RESTRICTIONS OR ENABLE VALID NODE CHECKING

Valid Node Checking allows or denies access from specified IP addresses to Oracle services. To enable Valid Node Checking for 9i and above, set the following parameters in `$TNS_ADMIN/sqlnet.ora`:

```
tcp.validnode_checking = YES
tcp.invited_nodes = ( X.X.X.X, hostname, ... )
tcp.excluded_nodes = ( hostname, X.X.X.X, ... )
```

The first parameter turns on Valid Node Checking. The latter two parameters respectively specify the IP addresses or hostnames that are permitted to make or are denied from making network connections to Oracle services. Replace `X.X.X.X` with the middle-tiers' IP addresses. Middle-tier applications include web servers, forms servers, reports servers, concurrent managers, discoverer, terminal servers, central administrator machines and any remote monitoring tool that uses SQLNet.

Note, to use SQLNet clients such as `sqlplus`, `toad`, `ADI` from a windows desktop, that desktop cannot use DHCP. Use a static or dynamic IP address.

AutoConfig supports automated configuration. For more information, refer to [Metalink Note 165195.1: Using AutoConfig to Manage System Configurations with Oracle Applications 11i](#). AutoConfig enabled systems may use the latest OAM minipack (included in 11.5.10 Maintenance Pack) to implement the manual steps high-

lighted above. For more details, see the Managed SQLNet Access feature in [Metalink Note 281758.1](#): Additional Features in Oracle Applications Manager in Release 11.5.10.

SPECIFY CONNECTION TIMEOUT

In `$TNS_ADMIN/listener.ora`, set the following parameter:

```
CONNECT_TIMEOUT_$(ORACLE_SID) = 10
```

For example,

```
CONNECT_TIMEOUT_VSEC1159 = 10
```

Where `VSEC1159` is the name of the `ORACLE_SID` in this example.

Use the parameter `CONNECT_TIMEOUT` to specify the amounts of time, in seconds, for the Oracle Listener to wait for the connection from a client to complete.

AUTHENTICATION

ENABLE TNS LISTENER PASSWORD

Despite the fact that setting a password for the Listener is one of the most important hardening procedures, when first created the Listener has no password. Set the password in `$TNS_ADMIN/listener.ora` by adding the following:

```
PASSWORDS_$(LISTENER_NAME) = <password>
```

For example, if the name of the Listener is `VSEC1159`, add:

```
PASSWORDS_VSEC1159 = Be3tpr3ct1ce
```

Once set, supply the password before doing any administrative work. Set the password with the command `SET PASSWORD <password>`. To stop the Listener, use the following commands in `lsnrctl` utility, assuming the password is `Be3tpr3ct1ce`.

```
LSNRCTL> set password
Password: Enter Be3tpr3ct1ce here; it will not be displayed
The command completed successfully
LSNRCTL> stop
Connecting to
(DES...)
The command completed successfully
```

Note, password protecting the TNS Listener has the following effects:

- Only a user with read access to the `$TNS_ADMIN/listener.ora` file can stop the TNS Listener.
- It is no longer possible to stop the TNS Listener using `lsnrctl` without providing the password. The work-around is to change the stop script to kill the TNS Listener process.
- The Listener process requires a password to list `SERVICES` or `STATUS`.
- This breaks some monitoring and remote administration tools, if they do not expect to provide a password.
- Cannot start, stop, check status or run services on remote machines via `lsnrctl`. Use Enterprise Manager for remote administration.

AUTHORIZATION

ENABLE ADMIN RESTRICTIONS

In `$TNS_ADMIN/listener.ora`, set the following parameter:

```
ADMIN_RESTRICTIONS_$(ORACLE_SID)=ON
```

For example,

```
ADMIN_RESTRICTIONS_VSEC1159=ON
```

Where `VSEC1159` is the name of the `ORACLE_SID`.

Note, when `ADMIN_RESTRICTIONS` is `ON`, all the `set` commands in `lsnrctl` are disabled and the only way to change the configuration is to edit the `listener.ora` file. Because `set password` is disabled, this might break some remote administration tools that do reconfiguration.

AUDIT

ENABLE TNS LISTENER LOGGING

To enable logging, in `$TNS_ADMIN/listener.ora` set the following parameters:

```
LOG_STATUS = ON  
LOG_DIRECTORY_$(ORACLE_SID) = $TNS_ADMIN  
LOG_FILE_$(ORACLE_SID) = $(ORACLE_SID)
```

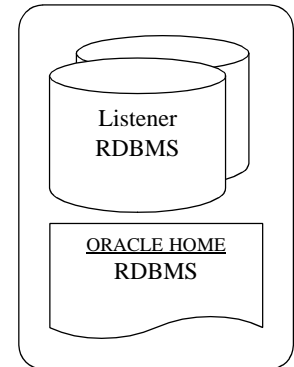
For example,

```
LOG_STATUS = ON  
LOG_DIRECTORY_VSEC1159 = /u01/oracle/vsec1159db/9.2.0.5/network/admin  
LOG_FILE_VSEC1159 = VSEC1159
```

Where `VSEC1159` is the name of the `ORACLE_SID`.

Oracle Database Security

DATABASE TIER



This section contains security recommendations for the Database.

HARDENING

HARDEN OPERATING ENVIRONMENT

Follow the hardening instructions for “Operating Environment Security” on page 33.

DISABLE XDB

To support XDB, the TNS Listener process listens on two additional TCP ports: 2100 for ftp access and 8080 for http access. Oracle E-Business Suite does not require these services; they should be disabled.

To disable XDB, remove or comment out the line in `init.ora` that reads

```
*.dispatchers=(PROTOCOL=TCP) (SERVICE=sidXDB)'
```

REVIEW DATABASE LINKS

Review database links in both production and development environments.

AUTHENTICATION

Middle-tier applications logon to the database via common product accounts rather than end-user accounts. Some individuals (IT Administrators) may require direct access to the application database via their own schema.

REMOVE OPERATING SYSTEM TRUSTED REMOTE LOGON

This setting prevents the database from using an insecure logon protocol. Make sure `init.ora` contains:

```
REMOTE_OS_AUTHENT=FALSE
```

IMPLEMENT TWO PROFILES FOR PASSWORD MANAGEMENT

The database provides parameters to enforce password management policies. However, some of the database password policy parameters could lock-out the E-Business Suite. Because of this, we make specific recommendations for or against using certain management features depending upon schema type.

Password Parameters	Application Profile	Administrator Profile
FAILED_LOGIN_ATTEMPTS	UNLIMITED	5
PASSWORD_LIFE_TIME	UNLIMITED	90
PASSWORD_REUSE_TIME	180	180
PASSWORD_REUSE_MAX	UNLIMITED	UNLIMITED
PASSWORD_LOCK_TIME	UNLIMITED	7
PASSWORD_GRACE_TIME	UNLIMITED	14
PASSWORD_VERIFY_FUNCTION	<i>Recommended</i>	<i>Recommended</i>

Database profiles contain limits on database resources and password policies. Create two database profiles: one for middle-tier application schemas and one for human beings. Assign middle-tier application schemas to the first profile and all accounts used by administrators to the second profile.

For more information on profiles, see CREATE PROFILE in the Oracle SQL Reference documentation.

CHANGE DEFAULT INSTALLATION PASSWORDS

Immediately after installation, change default passwords for all schemas and users. Default passwords for database accounts are widely known, and if not changed could allow unauthorized access to various parts of the system. For a list of registered schemas associated with the E-Business Suite, run `adutconf.sql`. Use `FNDCPASS` utility to synchronize password changes in both the middle-tier and the database.

```
# Change Oracle Database User Password
FNDCPASS apps/apps 0 Y system/manager ORACLE <account> <password>
```

Refer to the Oracle Applications System Administrator's Guide for more information on `FNDCPASS`. For information on `adutconf.sql`, refer to the AD Utilities Reference Guide for 11.5.9. Refer to the white paper A Security Checklist for Oracle 9i for information about schemas owned by the Oracle database.

Account Name	Change Password
APPLSYS ^a	Y
APPLSYSPUB	N
APPS ^b	Y
CTXSYS	Y
DBSNMP	Y
PORTAL30	Y
PORTAL30_SSO	Y
PRODUCT SCHEMAS: [ABM . . . XTR] ^c	Y
SYS	Y
SYSTEM	Y

a. The passwords of APPS and APPLSYS must be identical.

- b. Run Autoconfig to make sure the relevant parameter files have been updated to reflect this password change.
- c. Change all schema passwords. Find the complete set of schemas using this query:

```
select ORACLE_USERNAME from fnd_oracle_userid;
```

AUTHORIZATION

RESTRICT ACCESS TO SQL TRACE FILES

The `init.ora` parameter `_TRACE_FILES_PUBLIC` grants file system read access to anyone who has activated SQL tracing. Set this to *False*.

```
_TRACE_FILES_PUBLIC=FALSE
```

REMOVE OPERATING SYSTEM TRUSTED REMOTE ROLES

Set the `init.ora` parameter `REMOTE_OS_ROLES` to *False* to prevent insecure remote roles.

```
REMOTE_OS_ROLES=FALSE
```

LIMIT FILE SYSTEM ACCESS WITHIN PL/SQL

The parameter `UTL_FILE_DIR` limits file system access for all database accounts using the PL/SQL API `UTL_FILE`. Oracle E-Business Suite maintains some files and needs this parameter set.

```
UTL_FILE_DIR = <dir1>,<dir2>,<dir3>...
```

Avoid:

```
UTL_FILE_DIR = *
```

LIMIT DICTIONARY ACCESS (11.5.10 ONLY)

Set `O7_DICTIONARY_ACCESSIBILITY` to *False* to prevent users with Select ANY privilege from reading data dictionary tables. 11.5.10 Rapid Install defaults this value automatically.

```
O7_DICTIONARY_ACCESSIBILITY = FALSE
```

Note, prior to 11.5.10, this parameter cannot be set to *False*.

REVOKE UNNECESSARY GRANTS TO APPLSYSPUB

The following table lists the privileges that should be granted to the APPLSYSPUB schema. These are set in `<FND_TOP>/admin/sql/afpub.sql`.

APPLSYSPUB
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

APPLSYSPUB
INSERT ON FND_SESSIONS
INSERT ON FND_UNSUCCESSFUL_LOGINS
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

To check permissions, login as SYSTEM and issue the following query:

```
SELECT * FROM dba_tab_privs WHERE grantee = 'APPLSYSPUB';
```

To revoke unnecessary privileges granted to APPLSYSPUB schema, apply patch 3763612. 11.5.10 Rapid Install has a clean APPLSYSPUB by default. In addition, you should understand the implications of privileges on custom objects granted to PUBLIC or a role.

AUDIT

This section describes the auditing capabilities available in Oracle database for Oracle E-Business Suite. These recommendations should not have a measurable performance impact.

CONFIGURE THE DATABASE FOR AUDITING

In `init.ora`, set `AUDIT_TRAIL` to `DB`, `OS` or `TRUE`. Consult with the Applications Database Administrator before setting this value to `TRUE`. When set to `OS`, the database stores its audit records on the file system:

```
AUDIT_TRAIL = OS
```

Set parameter `AUDIT_FILE_DEST` to the directory where the audit records should be stored. When not set, `AUDIT_FILE_DEST` defaults to `$ORACLE_HOME/rdbms/audit`. In this example, the database places audit records in directory `/u01/app/oracle/admin/audit`.

```
AUDIT_FILE_DEST = /u01/app/oracle/admin/audit
```

Restart the database for these parameters to take effect.

Note, the database generates some audit records by default, whether or not `AUDIT_TRAIL` is enabled. For example, Oracle automatically creates an operating system file as an audit record when a user logs in as `SYSDBA` or as `INTERNAL`.

AUDIT DATABASE CONNECTIONS

Monitoring and auditing database sessions provides valuable information on database activity and is the only way to identify certain types of attacks (for example, password guessing attacks on an application schema). By auditing database sessions, suspicious connections to highly privileged schemas may be identified.

To audit sessions, login through `sqlplus` as `SYSTEM` and issue the following command:

```
SQL> audit session;
```

AUDIT DATABASE SCHEMA CHANGES

Audit any changes to the standard Oracle E-Business Suite database schema or creation of new schema. As rare events, these changes may indicate inappropriate or malicious activity.

To audit sessions, login through `sqlplus` as `SYSTEM` and issue the following command:

```
SQL> audit user;
```

AUDIT OTHER ACTIVITIES

To complete the recommended auditing, enable three other audit events: *create database link*, *alter system* and *system audit*. The remaining audit options generate significant entries of little value. Oracle E-Business Suite dynamically creates, alters and drops objects (tables, index, packages, etc.) on a regular basis. Auditing these other actions provides little meaningful information.

To audit the last three events, login through `sqlplus` as `SYSTEM` and issue the following commands:

```
SQL> AUDIT DATABASE LINK;           -- Audit create or drop database links
SQL> AUDIT PUBLICDATABASE LINK;     -- Audit create or drop public database links
SQL> AUDIT SYSTEM AUDIT;           -- Audit statements themselves
SQL> AUDIT ALTER ANY ROLE by ACCESS; -- Audit alter any role statements
SQL> AUDIT ALTER DATABASE by ACCESS; -- Audit alter database statements
SQL> AUDIT ALTER SYSTEM by ACCESS;  -- Audit alter system statements
SQL> AUDIT CREATE ROLE by ACCESS;    -- Audit create role statements
SQL> AUDIT DROP ANY ROLE by ACCESS;  -- Audit drop any role statements
SQL> AUDIT PROFILE by ACCESS;       -- Audit changes to profiles
SQL> AUDIT PUBLIC SYNONYM by ACCESS; -- Audit public synonyms statements
SQL> AUDIT SYSDBA by ACCESS;        -- Audit SYSDBA privileges
SQL> AUDIT SYSOPER by ACCESS;       -- Audit SYSOPER privileges
SQL> AUDIT SYSTEM GRANT by ACCESS;  -- Audit System grant privileges
```

AUDIT ADMINISTRATORS AND THEIR ACTIONS

Connections to the database as well as `SYSDBA` and `SYSOPER` actions (instance startup/shutdown) are always logged to the directory `$ORACLE_HOME/rdbms/audit`. This file contains the operating system user and terminal ID.

REVIEW AUDIT RECORDS

If `AUDIT_TRAIL` is set to `OS`, review audit records stored in the file name in `AUDIT_FILE_DEST`.

If `AUDIT_TRAIL` is set to `DB`, retrieve audit records from the `SYS.AUD$` table. The contents can be viewed directly or via the following views:

- `DBA_AUDIT_EXISTS`
- `DBA_AUDIT_OBJECT`
- `DBA_AUDIT_SESSION`
- `DBA_AUDIT_STATEMENT`
- `DBA_AUDIT_TRAIL`
- `DBA_OBJ_AUDIT_OPTS`
- `DBA_PRIV_AUDIT_OPTS`
- `DBA_STMT_AUDIT_OPTS`

The audit trail contains a lot of data; begin by focusing on the following:

- Username Oracle Username.
- Terminal Machine from which the user originated.
- Timestamp Time the action occurred.
- Object Owner The owner of the object that the user touched.
- Object Name The name of the object that the user touched.
- Action Name The action that occurred against the object (INSERT, UPDATE, DELETE, SELECT, EXECUTE).

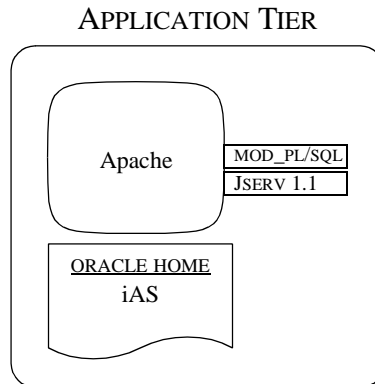
MAINTAIN AUDIT RECORDS

Archive and purge the audit trail on a regular basis, at least every 90 days. The database connection entries take up significant space. Backup the audit file before purging.

SECURE AUDIT RECORDS

Audit data may contain confidential or privacy related data. Restrict audit trail access appropriately.

Oracle Application Tier Security



This section contains security recommendations for the Application Server.

HARDENING

HARDEN OPERATING ENVIRONMENT

Follow the hardening instructions for “Operating Environment Security” on page 33.

REMOVE APPLICATION SERVER BANNER

To avoid exposing Apache version and enabled modules, turn off the banner in both `httpd_pls.conf` and `httpd.conf`:

```
Set ServerSignature off
Set ServerTokens Prod
```

REMOVE UNNECESSARY DIRECTIVES

If not using Autoconfig, use the following guidelines to remove unnecessary Apache directives.

In addition to any example or sample directories, remove or comment out references to documentation directories and other directives not needed to operate the application. Comment following in `httpd.conf` and `httpd_pls.conf`:

```
Alias /jservdocs/ "/apps/sid/product/iAS/Apache/Jserv/docs/"
```

These directives are specific to `${IAS_ORACLE_HOME}/Apache/Apache/conf/httpd_pls.conf`

```
#<Directory "/apps/<ORACLE_SID>/product/iAS/Apache/Apache/icons">
# Options MultiViews
# AllowOverride None
# Order allow,deny
# Allow from all
#</Directory>
```

```
#<Directory "/apps/<ORACLE_SID>/product/iAS/Apache/Apache/htdocs">
# Options MultiViews
# AllowOverride None
# Order allow,deny
# Allow from all
```

```
#</Directory>
```

TURN OFF DIRECTORY INDEXING

There are two goals when protecting a web server:

- Reduce the amount of information available.
- Reduce access to non-application related areas.

Directory indexes display the contents of a directory if there is not an index.htm or similar file available. Disabling this entry prevents an intruder from viewing the files in a directory, potentially finding a file that may be of use in their quest to access the system. The quickest way to disable this feature is to modify

`${IAS_ORACLE_HOME}/Apache/Apache/conf/httpd.conf` and `${IAS_ORACLE_HOME}/Apache/Apache/conf/httpd_pls.conf` configuration files and comment out the following line:

```
# IndexOptions FancyIndexing
```

UNLOAD APACHE AUTOINDEX MODULE

This module automatically generates directory indexes. To disable the module in `httpd.conf`, comment these lines as follows.

```
#LoadModule autoindex_module libexec/mod_autoindex.so
#AddModule mod_autoindex.c
```

As well as these autoindex directives:

```
#<IfModule mod_autoindex.c>
# IndexOptions FancyIndexing
# AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
# AddIconByType (TXT,/icons/text.gif) text/*
# AddIconByType (IMG,/icons/image2.gif) image/*
# AddIconByType (SND,/icons/sound2.gif) audio/*
# AddIconByType (VID,/icons/movie.gif) video/*
# AddIcon /icons/binary.gif .bin .exe
# AddIcon /icons/binhex.gif .hqx
# AddIcon /icons/tar.gif .tar
# AddIcon /icons/world2.gif .wrl .wrl.gz .vrm .vrm .iv
# AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
# AddIcon /icons/a.gif .ps .ai .eps
# AddIcon /icons/layout.gif .html .shtml .htm .pdf
# AddIcon /icons/text.gif .txt
# AddIcon /icons/c.gif .c
# AddIcon /icons/p.gif .pl .py
# AddIcon /icons/f.gif .for
# AddIcon /icons/dvi.gif .dvi
# AddIcon /icons/uuencoded.gif .uu
# AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
# AddIcon /icons/tex.gif .tex
# AddIcon /icons/bomb.gif core
# AddIcon /icons/back.gif ..
# AddIcon /icons/hand.right.gif README
# AddIcon /icons/folder.gif ^^DIRECTORY^^
# AddIcon /icons/blank.gif ^^BLANKICON^^
# DefaultIcon /icons/unknown.gif
# ReadmeName README
# HeaderName HEADER
#<IfModule>
#IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
```

DISABLE XSQL

In `xml.conf`, comment out the following lines:

```
#Alias /xsql/ "/u01/oracle/vsec1159ora/ias/xdk/"
#ApJServAction .xsql /servlets/oracle.xml.xsql.XSQLServlet
```

PREVENT SEARCH ENGINE INDEXING

For internet facing web servers, enable robot exclusion. This may be done either with a `robots.txt` file or using a META tag. See <http://www.robotstxt.org/wc/robots.html> for more information.

AUTHORIZATION

Within Oracle Application Server, a number of web pages provide administrative and testing functionality. These pages offer information about various services, the server's state and its configuration. While useful for debugging, these pages must be restricted or disabled in a production system.

PROTECT ADMINISTRATIVE WEB PAGES

Use the configuration files `httpd.conf` and `httpd_pls.conf` to limit web page access to a list of trusted hosts. To do this, create a file `trusted.conf` and include it in the `httpd.conf` and `httpd_pls.conf` files. This new file contains the following content. Replace *<list of TRUSTED IPs>* with host machines from which administrators may connect.

```
<Location ~ "/(dms0|DMS|Spy|AggreSpy)">
  Order deny,allow
  Deny from all
  Allow from localhost <list of TRUSTED IPs>
</Location>

<Location ~ "/dev60html/run(form|rep).htm">
  Order deny,allow
  Deny from all
  Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/OA_HTML/bin/appsweb*">
  Order deny,allow
  Deny from all
  Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/html/bin/appsweb*">
  Order deny,allow
  Deny from all
  Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/jinitiator/bin/appsweb*">
  Order deny,allow
  Deny from all
  Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/xsql/admin/xml.properties">
  Order deny,allow
```

```
Deny from all
Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/OA_JAVA/jdbc111.zip">
Order deny,allow
Deny from all
Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/OA_JAVA/apps.zip">
Order deny,allow
Deny from all
Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/OA_JAVA/sax2.zip">
Order deny,allow
Deny from all
Allow from localhost <list of TRUSTED IPs>
</Location>

<Location "/OA_JAVA/appsborg.zip">
Order deny,allow
Deny from all
Allow from localhost <list of TRUSTED IPs>
</Location>
```

PROTECT ADMINISTRATIVE SERVLET PAGES

In Oracle E-Business Suite, there are 15 aliases defined for servlet access.

oa_servlets, servlets, servlet, jsp, configurator, mobile, forms, discoverer4i, emailcenter, soar/servlet, webservices, dmsOACore, dmsDisco, dnsForms, pricing

To restrict servlet access solely to trusted hosts, add the following directives to trusted.conf file.

```
<Location ~ "/(oa_servlets|servlets|servlet|jsp|configurator|mobile|forms|discoverer4i|emailcenter|soap/servlet|webservices|dmsOACore|dmsDisco|dmsForms|pricing)/oracle.xml.xsql.XSQLServlet/soapdocs/webapps/soap/WEB-INF/config/soapConfig.xml" >
Order deny,allow
Deny from all
Allow from localhost <list of TRUSTED IPs>
</Location>

<Location ~ "/(oa_servlets|servlets|servlet|jsp|configurator|mobile|forms|discoverer4i|emailcenter|soap/servlet|webservices|dmsOACore|dmsDisco|dmsForms|pricing)/oracle.xml.xsql.XSQLServlet/xsql/lib/XSQLConfig.xml" >
Order deny,allow
Deny from all
Allow from localhost <list of TRUSTED IPs>
</Location>

<Location ~ "/(oa_servlets|servlets|servlet|jsp|configurator|mobile|forms|discoverer4i|emailcenter|soap/servlet|webservices|dmsOACore|dmsDisco|dmsForms|pricing)/IsItWorking">
Order deny,allow
Deny from all
Allow from localhost <list of TRUSTED IPs>
```

```
</Location>

<Location ~ "/(oa_servlets|servlets|servlet|jsp|configurator|mobile|forms|
discoverer4i|emailcenter|soap/servlet|webservices|dmsOACore|dmsDisco|
dmsForms|pricing)/DMSDUMP.*$">
    Order deny,allow
    Deny from all
    Allow from localhost <list of TRUSTED IPs>
</Location>
```

DISABLE TEST PAGES

Add the following directives in both `httpd.conf` and `httpd_pls.conf` to disable these test pages:

```
<Location "^/fcgi-bin/echo.*$">
    Order deny,allow
    Deny from all
</Location>

<Location "^/fcgi-bin/echo2.*$">
    Order deny,allow
    Deny from alls
</Location>

<Location "/forms60java/gss_1.1.2_bin.jar">
    Order deny,allow
    Deny from all
</Location>
```

CONFIGURE MOD_PLSQL

`mod_plsql`, an Apache extension module, enables dynamic web page creation from PL/SQL. This module maps browser requests into database stored procedure calls. It is generally indicated by a `/pls` virtual path.

Each `mod_plsql` request is associated with a Data Access Descriptor (DAD). A DAD contains the set of configuration values used for database access including:

- the database alias (Net8 service name),
- a connect string, if the database is remote, and
- other system parameters used by the applications.

REMOVE UNNEEDED DAD CONFIGURATIONS

The default configuration file of Oracle Application Server for `mod_plsql` component is `${IAS_ORACLE_HOME}/Apache/modplsql/cfg/wdbsvr.app`. Remove unneeded DAD configurations. The DAD with name of `ORACLE_SID` is required. For those customers who do not use Portal, remove it using instructions from Oracle Security Alert #61. Take care when modifying a parameter value; check that the modification occurs in the appropriate section of the DAD.

ENABLE MOD_PLSQL CUSTOM AUTHORIZATION

Enable `mod_plsql` custom authorization to prevent unauthorized PL/SQL procedure execution through the browser. To ensure correct configuration, see the Oracle Applications System Administrator's Guide, Appendix G: Setting Up and Maintaining Oracle Applications. Follow the mandatory step "Test that CUSTOM authentication is working."

In `wdbsvr.app` parameter file, set `CUSTOM_AUTH` to `CUSTOM`.

```
[WVGATEWAY]
defaultDAD      = <Data Access Descriptor comes here>
custom_auth     = CUSTOM
```

RESTRICT MOD_PLSQL WEB ADMINISTRATION

`mod_plsql` provides a tool to create and administer DADs. This tool, available by default, uses the same configuration file `wdbsvr.app`. To disable the administrative interface, make the following changes in `$IAS_ORACLE_HOME/ias/Apache/modplsql/cfg/plsql_pls.conf` file:

```
<Location /pls/admin_>
  Order deny,allow
  Deny from all
# Uncommenting next line allows selected hosts to use the admin page
# Allow from localhost <list of TRUSTED IPs>
</Location>
```

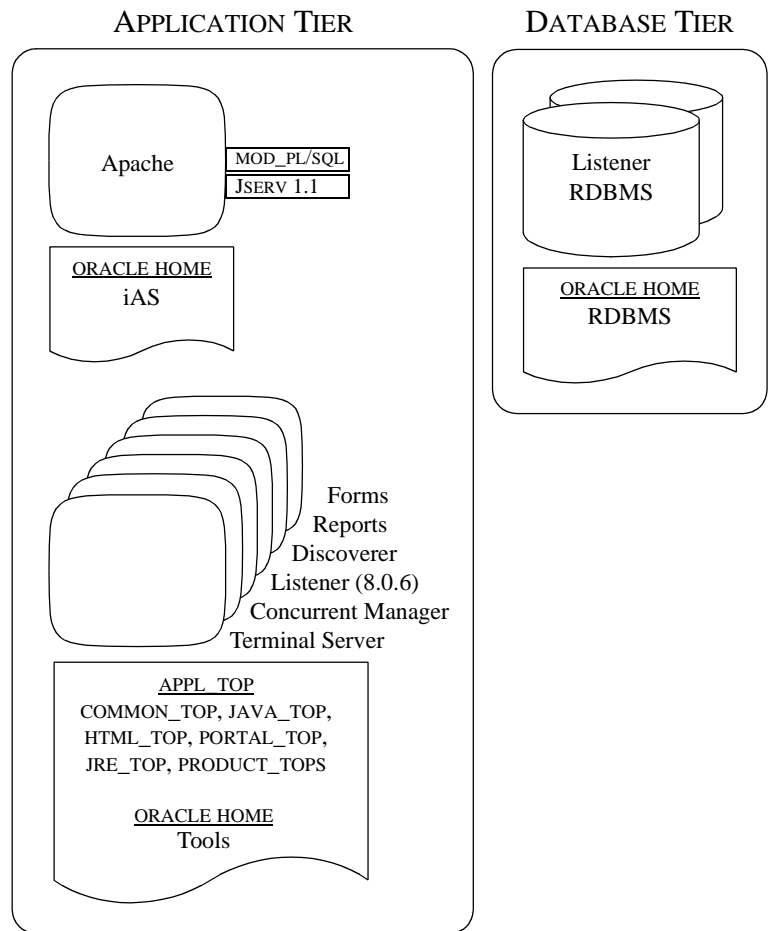
The location above must match `adminPath` in `wdbsvr.app`, if `adminPath` has been changed.

AUDIT

CONFIGURE LOGGING

Oracle Application Server respects Apache's logging parameters. When activated, the server logs data about who has accessed the system, when and the nature of the requested operation. At a minimum, log server access.

E-Business Suite Security



This section contains security recommendations for the Oracle E-Business Suite.

HARDENING

HARDEN OPERATING ENVIRONMENT

Follow the hardening instructions for "Operating Environment Security" on page 33.

STRIKE PASSWORDS FROM ADPATCH LOGS

To stop adpatch from logging passwords, apply AD.H and use the following flag:

```
adpatch flags=hidepw
```

SET WORKFLOW NOTIFICATION MAILER SEND_ACCESS_KEY TO N

When SEND_ACCESS_KEY is set to *Y*, the workflow notification email bypasses the E-Business Suite sign-on process; email notifications contain an access key. The key allows the user to access the Notification Details web page directly without authenticating. Set SEND_ACCESS_KEY to *N* to prevent inclusion of the key with the Notification Detail link. When set to *N*, an unauthenticated user who clicks on the notification link must sign on before accessing the Notification Details web page.

For more information, refer to Oracle Workflow Administrator's Guide.

SET TOOLS ENVIRONMENT VARIABLES

Follow instructions in Metalink notes for setting these values.

Form Environment Variable	Value	Metalink Note
FORMS60_RESTRICT_ENTER_QUERY	TRUE	125767.1
REPORTS60_CGINODIAG	YES	TBD

NETWORK

USE SSL (HTTPS) BETWEEN BROWSER AND WEB SERVER

Information sent over the network and across the Internet in clear text may be intercepted. Secure Sockets Layer (SSL) is an encryption scheme that negotiates an exchange of encryption keys. These keys are packaged in Certificates issued by a Certificate Authority (CA).

For information on setting up SSL with the Oracle E-Business Suite, refer to “11i: A Guide to Understanding and Implementing SSL for Oracle Applications”.

USE TERMINAL SERVICES FOR CLIENT-SERVER PROGRAMS

Deploy components requiring direct connection to the E-Business Suite database on servers rather than on end-user desktop machines.

A majority of the E-Business Suite architecture supports this through a three-tier architecture; browser sessions connect to middle-tier servers running Oracle 9i Application Server. For the few exception cases in which Oracle E-Business Suite components or associated development tools connect to the database directly, deploy a remote server environment based on Windows Server Terminal Services, Citrix or Tarantella.

These client/server programs include Oracle Workflow Builder and Oracle Discoverer, ADI, Oracle Financial Analyzer and Oracle Sales Analyzer. For a list of certified client/server components refer to [Metalink Note 277535.1](#).

While deploying the required applications development and/or production runtime tools on Terminal Services, configure SQLNet Valid Node Checking and Application Server Security. The former isolates SQLNet access to the Terminal Server and the latter identifies the terminal server to applications. These both prevent end-user desktops from connecting to the production database instance. Register the terminal server used to deploy the client/server components as a Managed SQLNet Access node. Further details are provided in section “Add IP restrictions or enable Valid Node Checking” on page 3 and “Activate Server Security” on page 22.

AUTHENTICATION

CHANGE PASSWORDS FOR SEEDED APPLICATION USER ACCOUNTS

Oracle ships seeded user accounts with default passwords. Change the default passwords immediately. Depending on product usage, some seeded accounts may be disabled. Do not disable SYSADMIN or GUEST user accounts.

Account	Product / Purpose	Change	Disable
ANONYMOUS	FND/AOL – Anonymous for non-logged users	Y	Y
APPSMGR	Routine maintenance via concurrent requests	Y	Y
ASGADM	Mobile gateway related products	Y	Y ^a
ASGUEST	Sales Application guest user	Y	Y ^b
AUTOINSTALL	AD	Y	Y
CONCURRENT MANAGER	FND/AOL: Concurrent Manager	Y	Y
FEEDER SYSTEM	AD – Supports data from feeder system	Y	Y
GUEST	Guest application user	Y	N
IBE_ADMIN	iSupport Admin user	Y	Y ^c
IBE_GUEST	iSupport Guest user	Y	Y ^c
IBEGUEST	iSupport Guest user	Y	Y ^c
IEXADMIN	Internet Expenses Admin	Y	Y
INITIAL SETUP	AD	Y	Y
IRC_EMP_GUEST	iRecruitment Employee Guest Login	Y	Y
IRC_EXT_GUEST	iRecruitment External Guest Login	Y	Y
MOBILEADM	Mobile Applications Admin	Y	Y
OP_CUST_CARE_ADMIN	Customer Care Admin for Oracle Provisioning	Y	Y
OP_SYSADMIN	OP (Process Manufacturing) Admin User	Y	Y
STANDALONE BATCH PROCESS	FND/AOL	Y	Y
SYSADMIN	Application Systems Admin	Y	N
WIZARD	AD – Application Implementation Wizard	Y	Y

- a. Required for Mobile Sales, Service, and Mobile Core Gateway components.
- b. Required for Sales Application.
- c. Required for iStore.

TIGHTEN LOGON AND SESSION PROFILE OPTIONS

For local application users, the profile option settings below support strong passwords, account lockout after too many failed logons and session inactivity timeout. For more information on Single Sign-On deployments, see the Oracle Internet Directory Administrator's Guide or refer to [Metalink Note 233436.1](#).

Profile Option Name	Recommendation
SIGNON_PASSWORD_LENGTH	6

SIGNON_PASSWORD_HARD_TO_GUESS	YES
SIGNON_PASSWORD_NO_REUSE	180
ICX_SESSION_TIMEOUT	30

CREATE NEW USER ACCOUNTS SAFELY

Starting from release 11.5.10, Oracle User Management (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. See UMX Documentation for more details.

CREATE SHARED RESPONSIBILITIES INSTEAD OF SHARED ACCOUNTS

When users share one account, the system cannot identify which user performs a function, preventing accountability. Users share the same functions or permission sets, while the system tracks individual user actions.

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. To prevent this, define the concurrent program executable as a *HOST* program in the Concurrent Program Executable form. Enter *ENCRYPT* in the Execution Options field of the Concurrent Programs window when defining a concurrent program using this executable. *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.

ACTIVATE SERVER SECURITY

Oracle E-Business Suite 11i 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.

Setup Server Security

The application server security feature is not activated initially.

Application Server Security has three states:

- OFF** Inactivates Server Security. Server and code IDs are not checked. Appropriate for machines completely under an administrator's control. OK for development systems without production data.
- ON** Equivalent to OFF from a security perspective. Not recommended for production systems.
- SECURE** Recommended; only registered application servers and trusted code modules may connect.

Check Server Security Status

Check the Server Security status using the `STATUS` command in the `AdminAppServer` utility before activating server security to ensure that all desired Application Servers have been registered. For details, see System Administrators Guide, Administering Server Security.

Adding Server IDs

Register application servers as trusted machines with a database server. The .dbc file contains the Application Server's ID.

Use the AdminAppServer utility to generate server IDs and register them with a database. The program adds them to the database automatically when the AdminAppServer is used to create a .dbc file:

```
jre oracle.apps.fnd.security.AdminAppServer apps/<apps-passwd> \  
ADD [SECURE_PATH=$FND_TOP/secure] \  
DB_HOST=<database host> \  
DB_PORT=<database port> \  
DB_NAME=<database sid>
```

See the section on Creating DBC files in Administering Oracle Applications Security in Release 11i for more details.

Updating Server IDs

```
jre oracle.apps.fnd.security.AdminAppServer apps/<apps-passwd> \  
UPDATE DBC=<dbc file path> APPL_SERVER_ID
```

Providing the APPL_SERVER_ID argument forces a new ID to be generated and added to the .dbc file. If the APPL_SERVER_ID argument is not provided, AdminAppServer synchronizes the server IDs found in the .dbc file with the database automatically.

Deleting Server IDs

```
jre oracle.apps.fnd.security.AdminAppServer apps/<apps-passwd> \  
DELETE DBC=<dbc file path>
```

Server Security Activation

To activate basic server security from the command line (*ON* mode):

```
jre oracle.apps.fnd.security.AdminAppServer apps/<apps-passwd> \  
AUTHENTICATION ON DBC=<dbc file path>
```

To activate full server security from the command line (*SECURE* mode):

```
jre oracle.apps.fnd.security.AdminAppServer apps/<apps-passwd> \  
AUTHENTICATION SECURE DBC=<dbc file path>
```

To deactivate server security from the command line (*OFF* mode):

```
jre oracle.apps.fnd.security.AdminAppServer apps/<apps-passwd> \  
AUTHENTICATION OFF DBC=<dbc file path>
```

Autoconfig Support for Server Security Option

To enable Autoconfig support for Server Security option, apply patch 3438169.

References

See [Metalink Note 145646.1](#) for information about how to verify and see the status of the .dbc file including ones that use APPL_SERVER_ID.

AUTHORIZATION

REVIEW GUEST USER RESPONSIBILITIES

To represent an unauthenticated user session the E-Business Suite uses a guest account for certain applications (such as iStore). Limit guest user responsibilities to those necessary for sign-on and guest access. The Define User Form allows the System Administrator to review and modify guest user responsibilities.

REVIEW USERS WITH ADMINISTRATIVE RESPONSIBILITIES

In E-Business Suite, the SYSADMIN responsibility has broad administrative privileges. For this reason, regularly review this list of users. In addition to the generic SYSADMIN responsibility, most products have their own administrative responsibility. Review these responsibilities from time to time. Define and assign appropriate responsibilities for end users that clearly reflect their line of duty.

LIMIT ACCESS TO SECURITY RELATED FORMS

Some forms allow users to modify the E-Business Suite 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. "Appendix A: Security Setup Forms" on page 45 contains a list of forms that allow security setup. Consider auditing the database tables listed there.

LIMIT ACCESS TO FORMS ALLOWING SQL ENTRY

To improve flexibility, some forms allow users to enter SQL statements. Unfortunately, this feature may be abused. "Appendix B: Security Setup Forms That Accept SQL Statement" on page 47 contains a list of Forms that allow the user to edit code, add code or otherwise affect executable code. Restrict access to these forms by assigning the responsibility to a small group of users. Consider auditing the database tables listed in the appendix.

Refer to [Metalink Note 125767.1](#): Upgrading Developer 6i with Oracle Applications 11i for more information on security related to forms.

SET OTHER SECURITY RELATED PROFILE OPTIONS

Refer to the table below and set the suggested values for the profile options.

Profile Option	Suggest
AuditTrail:Activate	Yes
Concurrent:Report Access Level	User
FND:Diagnostics	No
Sign-on:Notification	Yes
Utilities:Diagnostics	No

RESTRICT RESPONSIBILITIES BY WEB SERVER TRUST LEVEL

When web servers have been assigned a server trust level the system may restrict access to a responsibility based upon that trust level. Three trust levels are supported:

1. administrative
2. normal

3. external

Typically, *administrative* web servers are used exclusively by system administrators, are considered secure and have full application access with few limitations. *Normal* web servers are those used by employees within a company's intranet and requiring non-administrative responsibilities. Lastly, customers or employees outside of a company's firewall connect to *external* servers. These have access to a small set of responsibilities.

Setting the Server Trust Level for a Server

To assign a trust level to a Web server, the administrator sets the NODE_TRUST_LEVEL profile option. This option, a server-based profile option, can be set to either 1, 2 or 3. The number 1 means *administrative*, 2 means *normal* and 3 means *external*. To avoid having to set the NODE_TRUST_LEVEL for every single Web server, administrators may wish to set the NODE_TRUST_LEVEL profile to some default level of trust at the site level. If no value is set for NODE_TRUST_LEVEL, the Web server is assumed to have a trust level of 1 (i.e., *administrative*).

Restricting Access to a Responsibility

When a user logs on to Oracle Applications via a Web server, the system determines which responsibilities are valid for that user, and of those responsibilities, which can be accessed from that particular Web server. The system returns only responsibilities appropriate for the Web server Trust Level.

To restrict access to a responsibility, set the Application Server Trust Level profile option value for that responsibility to be the number 1, 2 or 3. This indicates that only Web servers with the same or greater ordinal trust level may access that responsibility.

For example, a responsibility with an Application Server Trust Level set to 1 (*administrative*) would only be available if the Web server has its Application Server Trust Level set to 1 (*administrative*), as well. A responsibility with Application Server Trust Level set to 2 (*normal*) would only be available if the Web server has its Server Trust Level set to either 1 (*administrative*) or 2 (*normal*).

Profile Option - Application Server Trust Level

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. The system administrator access is described in the following table:

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	No	No

The internal name for this profile option is APPL_SERVER_TRUST_LEVEL.

References

For more information on how to enable and use the above security features, refer to Oracle Applications System Administrator's Guide, Volume 1 Release 11i for more information about this feature.

[Metalink Note 187403.1](#) describes what "Server Access Control" is and how to enable it

AUDIT

This chapter describes how to configure and use Oracle E-Business Suite audit features. It provides an explanation of the features available, configuration steps and best practices for auditing. It also suggests which common application objects like foundation objects, users and responsibilities to audit.

Often, E-Business Suite deployments do not take advantage of the auditing features due to the perceived complexity and performance issues. Properly configuring auditing and limiting auditing to appropriate tables should not have a measurable performance impact.

SET SIGN-ON AUDIT LEVEL

The valid settings for the profile option `SIGNONAUDIT:LEVEL` are `None`, `User`, `Responsibility` and `Form`. At site level, set this profile option to `Form` to enable as much auditing as possible. 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`, respectively.

Refer to the Oracle Applications System Administrator's Guide for more information.

Profile Option Name	Description	Recommend
<code>SIGNONAUDIT:LEVEL</code>	Set at site-level to track actions starting when the user logs on.	Form

MONITOR 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. See OAM documentation for complete product information.

Regarding Page Access Tracking, it tracks Oracle Applications usage statistics non-intrusively and with negligible performance impact. It tracks Web-based and Form-based accesses across technology stacks and correlates them for each user session. See [Metalink Note 278881.1](#) for more detailed information about Page Access Tracking.

RETRIEVE AUDIT RECORDS USING 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.

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

RETRIEVE AUDIT RECORDS USING SQL

The system stores end-user access data in the following tables. Develop SQL scripts to query these tables to generate reports.

- `APPLSYS.FND_LOGINS`
- `APPLSYS.FND_LOGIN_RESPONSIBILITIES`
- `APPLSYS.FND_LOGIN_RESP_FORMS`

E-Business Suite Security

- APPLSYS.FND_UNSUCCESSFUL_LOGINS
- FND_CONCURRENT_REQUESTS
- ICX.ICX_FAILURES

PURGE AUDIT RECORDS

Purge end-user access data using the *Purge Signon Audit Data* concurrent program. The current program purges all audit records older than a user supplied date. Run this concurrent program between once a week and once a month, retaining 30 to 90 days of records. This concurrent program purges the following tables:

- FND_LOGIN_RESP_FORMS
- FND_LOGIN_RESPONSIBILITIES
- FND_LOGINS
- FND_UNSUCCESSFUL_LOGINS

Purge concurrent request data using the *Purge Concurrent Request and/or Manager Data* concurrent program. Run this concurrent program at least once a week and retain 14 to 90 days of records.

Periodically archive and truncate the FND_SIGNON_XXXX tables.

REVIEW DATA TRACKED (NO REPORTS AVAILABLE)

Some data tracked by the system do not have associated reports. Nevertheless, these audit records contain valuable information.

Who Columns

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

Join with FND_USERS and FND_LOGINS tables to identify the application user tracked in the audit record. Note, only the last update to record is saved. To save the entire history of a row, enable Oracle E-Business Suite Audit Trail.

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.

ADVANCED AUDIT

Oracle E-Business Suite implements its own auditing mechanisms, Audit Trails.

Auditing database row changes is performance intensive. Limit auditing to non-transactional data. Auditing transactional data may cause significant performance degradation. Tables with more than a few changes an hour should not be considered for row level auditing. Plan and consult with a DBA before enabling Audit Trails.

This feature keeps a complete history of changes made at a table and column level. When initialized, a concurrent program creates a shadow table and places triggers on the columns to be audited. The triggers store column changes in the shadow table -- a table whose name is the instance table's name appended with `_A`.

CONFIGURING AUDIT TRAIL

To enable Audit Trail, follow these steps:

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

GENERATE AND IDENTIFY AUDIT TRAIL OBJECTS

To create the shadow tables as explained in the auditing section above, run the *AuditTrail Update Tables* concurrent program, which activates auditing. This program creates triggers on each audited column in the original table. In addition, it creates two views for each column with the names `_AC#` and `_AV#` where # is a sequential number.

- 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#`

CHOOSE TABLES TO AUDIT

Consider auditing some of the 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

RETRIEVE AUDIT RECORDS USING SQL

Access Audit Trail records through SQL. Oracle does not ship Audit Trail reports. Use shadow tables and views for accessing the records.

PURGE AUDIT RECORDS

Purge the audit trail information on a regular basis. Prior to purging, disable the Audit Trail.

Use the following procedure to purge audit data:

1. As System Administrator, select *Security -> Audit Trail -> Groups*.
2. Select the Security Audit group and set the group state to Disable – Purge Table.
3. Run the Audit Trail Update Tables Report.
4. Purge the data from the shadow table.
5. Select *Security -> Audit Trail -> Groups*.
6. Select the Security Audit group and set the group state to Enable.
7. Run the Audit Trail Update Tables Report

REFERENCES ON E-BUSINESS SUITE AUDITING

- Oracle8i Administrator's Guide – Auditing Database Use
- Oracle Applications System Administrator's Guide – User and Data Auditing
- [Metalink Note 105624.1](#) – Troubleshooting (Audit Trail)
- [Metalink Note 60828.1](#) – Overview of Oracle Applications AuditTrails
- [Metalink Note 69660.1](#) – Understanding Data Auditing in Oracle Application Tables

Desktop Security



This section contains security recommendations for the Desktop.

HARDENING

CONFIGURE BROWSER

See [Metalink Note 285218.1](#) for information about securing the desktop.

UPDATE BROWSER

- Update browser when new versions are released; they often include new security features.
- Check browser for built-in safety features.
- When using Internet Explorer:
 - upgrade to at least Version 6.0.
 - check Microsoft website for the latest browser security patches (<http://www.microsoft.com>)

TURN OFF AUTOCOMPLETE IN INTERNET EXPLORER

For kiosk machines, change Internet Explorer's autocomplete settings. IE can automatically show previous values entered in the same form field. Although desirable for frequently accessed pages, for privacy and security reasons this feature should be disabled.

To turn OFF the Auto Complete feature:

1. Navigate through *Tools* -> *Internet Options* -> *Content*
2. From the *Content* tab, click the *AutoComplete* button.
3. Uncheck "forms" and "User names and passwords on forms".

Also, do not use the "remember password" function; this is a known security vulnerability.

SET POLICY FOR UNATTENDED PC SESSIONS

People may attempt to access unattended workstation while the user is still logged into the system. The user should never leave their workstation unattended while logged into the system because it makes the system accessible to others who may walk up to the computer. Organizations should set a corporate policy for handling unattended PC sessions. Users are recommended to use the password-locked screen savers feature on all PCs.

Operating Environment Security

The environment in which Oracle Applications run contributes to or detracts from overall system security. This section contains security recommendations for tightening Oracle file system security along with more general advice for overall system hardening.

HARDENING

CLEANUP FILE OWNERSHIP AND ACCESS

1. The directory `$ORACLE_HOME/bin` contains Oracle executables. Check that the operating system owner of these executables matches the operating system user under which the files have been installed. A typical mistake is to install the executables in user `oracle`'s directory but owned by `root`.
2. Check that the operating system user chosen as the owner of Oracle E-Business Suite owns all of the files in the `$APPL_TOP` directory.
3. Prevent remote login to the Oracle (and root) accounts. Instead, require that legitimate users connect to their own accounts and `su` to the Oracle account. Better yet, use `sudo` to restrict access to executables. Find more information about `sudo` at <http://www.courtesan.com/sudo>.

CLEANUP FILE PERMISSIONS

Refer to the product installation documentation for the complete instructions on setting file permissions.

On Unix systems:

1. Set the permissions on `$ORACLE_HOME/bin` to 0751 (0755 in 9iR2) or less. Set all other directories in `$ORACLE_HOME` to 0750 or less.
2. Set file permissions for `listener.ora`, `sqlnet.ora` and, if applicable, `protocol.ora` to 0600.
3. Set file permissions for `tnsnames.ora` to 0644.
4. Ensure that the owner, group and modes of the Oracle files created upon installation are set to allow minimum privilege. The following commands make this change. Note, the group and owner are for illustration only, the correct intended group and owner should be substituted.

```
$chgrp -R <oinstall> $ORACLE_HOME
$chown -R <oracle> $ORACLE_HOME
```
5. Review owners and groups when cloning a database.
6. Protect the `$ORACLE_HOME/rdbms/admin` directory including `catalog.sql`, `catproc.sql` and backup scripts.
7. Secure scripts containing usernames and passwords.
8. Verify that set userid (SUID) and set group id (SGID) are not set on binaries. In general, Oracle recommends that the SUID and SGID bits to be removed from binaries shipped by Oracle.

Warning: If Concurrent Manager runs on the Database tier, the BEQ adapter requires the SUID or SGID bit set to avoid TCP cost. This is the same for any third part products running on the db tier.

On windows systems, NTFS must be used. The FAT/FAT32 file system provides no security.

LOCKDOWN OPERATING SYSTEM LIBRARIES AND PROGRAMS

The database and applications place few requirements on the underlying operating system.

1. X Server
 - a. Oracle Installer requires access to the X server which in turn requires access to an X font server.

- b. All Application middle-tiers and web-tiers require the X server.
 - c. A production Database does not use an X server.
2. Printers
Applications require access to printers – normally via the lpd interface on port 515/TCP. If possible, restrict access to the operating system users who absolutely need the printing facility from the shell.
 3. Electronic Mail
Applications require access to a SMTP Mail Transfer Agent (SMTP MTA) typically `sendmail` or `qmail` on port 25/.`dbc`. This is required for outbound emails, typically notifications from the workflow system. If possible, restrict access to the operating system users who absolutely need the mail facility from the shell.
 4. Remote Access
Use secure shell (`ssh`) to access middle-tier and database hosts. This replaces `telnet`, `rsh`, `rlogin`, `rcp` and `ftp`.

Although not required by the E-Business Suite, the following services may provide operational convenience:

1. NTP – Network Time Protocol – for synchronizing the clock on the UNIX hosts
2. CRON – for operating system cleanup and log file rotation
3. Monitoring agents – for monitoring operating system, database and application components for health and security

NETWORK

To secure the network, limit access to services users need and make those services as secure as possible. Disabling unused services reduces securing and monitoring work.

FILTER IP PACKETS

IP filtering helps to prevent unwanted access. On the internet or large network, use a firewall machine or router with firewalling capabilities.

A firewall machine sits between the internet and the intranet or the intranet and the internal servers. It provides a point of resistance by protecting inside systems from external users. A firewall machine can filter packets and/or be a proxy server. Firewalls may be software or hardware. For software, dedicate a machine to be the firewall. Do not assume that using Network Address Translation (NAT) substitutes for a firewall.

Filtering out unused services at the firewall or router level stops infiltration attempts earlier in the process. Unless running NFS between networks, turn off all RPC ports on the router. Better yet, enable only specific ports in use, adding new ones as needed.

On the host, create access control lists in `/var/adm/inetd.sec` to limit which hosts can connect to the local machine. Turn off unused services in `/etc/inetd.conf`.

PREVENT SPOOFING

To prevent hostname spoofing, turn off source routing and filter packets originating outside the network that have source IP address from the inside network.

On the system side, only use qualified hostnames in system files (NFS, `hosts.equiv`, etc.). If possible, do not allow `hosts.equiv` or `.rhosts`. If not possible, verify that all `.rhost` and `.netrc` file permissions are 600. Consider using a cron job to automatically check and enforce this.

SECURE TELNET CONNECTIONS

Enforce the use of SSH (secure shell). SSH provides encrypted traffic to prevent snooping. If telnet must be used, at least restrict telnet to a limited number of machines and turn off root login (except console, see “Limit root access” below).

SECURE FTP CONNECTIONS

Unless required, turn off this service. To copy files, use the scp or sftp programs that come with ssg. Standard ftp sends passwords in clear text and, for this reason, should not be used.

VERIFY NETWORK CONFIGURATION

Use scanning tools to find common security violations. Add all networking patches.

MONITOR FOR ATTACKS

Consider installing an Intrusion Detection System (IDS), For example, Snort is a nice free IDS system.

AUTHENTICATION

Good security requires secure accounts.

CONFIGURE ACCOUNTS SECURELY

- Make sure that *all accounts* have a non-guessable password. To ensure that the passwords are not guessable, use crack (a password cracking tool) on a regular basis. Often, people use passwords associated with them: license plate numbers, children's names or a hobby. A password tester may check for these. In addition, change passwords from time to time.
- To implement password security on HP systems use HP's trusted system package via SAM (if NIS or NIS+ is not running).
- Consider using one-time passwords such as skey.
- Automatically disable accounts after several failed login attempts.
- `.netrc` files weaken security.

LIMIT ROOT ACCESS

- The fewer people with root access, the easier it is to track changes.
- The root password must be a strong, non-guessable password. In addition, change the root password every 3 months and whenever someone leaves company. Always logout of root shells; never leave root shells unattended.
- Limit root to console login, only (specified in `/etc/security`).
- Root, and only root, should have UID 0.
- Check root `.*` files for security holes. The root `.*` files SHOULD have 700 permissions. The minimal umask for root is 022 (rwxr-xr-x). A umask of 077 (rwx-----) is best, but often not practical.
- To avoid trojan horse programs, always use full pathnames including aliases. Root should NEVER have `..` in path. NEVER allow non-root write access to any directories in root's path.
- If possible, do not create root's temporary files in publicly writable directories.

MANAGE USER ACCOUNTS

Do not share user accounts. Remove or disable user accounts upon termination. Disable login for well known accounts that do not need direct login access (bin, daemon, sys, uucp, lp, adm). Require strong passwords and, in some cases, a restricted shell.

RESTRICT GUEST ACCOUNTS

As with any account, only create a guest account for the time required. Remove the account when its purpose is completed. Use a non-standard account name for the account - avoid "guest". Use a strong password and a restricted shell. If reasonable, give the account an 077 umask.

AUTHORIZATION

SECURE NFS

Only run NFS as needed, apply latest patches. When creating the /etc/exports file, use limited access flags when possible (such as *readonly* or *nosuid*). By using fully qualified hostnames, only the named host may access the file system.

SECURE OPERATING SYSTEM DEVICES

Device files /dev/null, /dev/tty and /dev/console should be world writable but NEVER executable. Most other device files should be unreadable and unwritable by regular users.

SECURE SCRIPTS

Never use setuid/setgid shell scripts. Instead, write a compiled program in a language like "C". Scripts should ALWAYS have full pathnames.

SECURE EXECUTABLES

Always get programs from a known source. Use a checksum to verify they have not been altered. When compiling a program, make sure the compiler has not been altered.

SECURE FILE ACCESS

Create minimal writable file systems (esp. system files/directories). Limit user file writes to their own directories and /tmp. Add directories for specific groups. Limit important file access to authorized personnel. Use setuid/setgid only where absolutely necessary.

MAINTENANCE

Good security practice does not end after installation. Continued maintenance tasks include:

- Install the latest software patches.
- Install latest operating system patches.
- Verify user accounts.
- Run security software and review output.

Operating Environment Security

- Keep up to date on security issues by subscribing to security mailing lists, reading security news groups and following the latest security procedures.
- Implement trusted file systems like NIS, NIS+ or others such as HP-UX trusted system.
- Test the system with tools like SATAN (network security), COPS (various system checks), TIGER (searches for root compromise) and CRACK (password checker).
- Install Tripwire to detect changes to files.
- Monitor log files including btmp, wtmp, syslog, sulog, etc. Consider setting up automatic email or paging to warn system administrators of any suspicious behavior. Also check the snort logs.

Extras for Experts

Security policy must balance risk of attack, cost of defense and value of data protected. This section contains recommendations that improve security, but may not be appropriate for every deployment.

DETECT AND PREVENT DUPLICATE USER SESSIONS

When properly patched and configured, the E-Business Suite raises a Workflow event when the same user has multiple, open sessions. A subscription attached to this event may take some action including closing the old session under the same user name or sending an email notification to the administrator.

Patch 2128669 contains an example demonstrating how to write a custom event and/or additional subscriptions. The subscription calls a rule function that updates the `ICX_SESSIONS` table setting the `DISABLED_FLAG= 'Y'` for all other sessions for the user. This renders the other sessions invalid. The next user action returns the browser to a login screen indicating the session is invalid. User names appearing in the subscription's parameter list are excluded from this functionality.

This functionality is disabled by default.

CUSTOMIZE PASSWORD VALIDATION

To customize password validation create a Java class that implements the `oracle.apps.fnd.security.PasswordValidation` Java interface. The interface requires three methods:

1. `public boolean validate(String user, String password)`
This method takes a username and password, and returns *True* or *False*, indicating whether the user's password is valid or invalid, respectively.
2. `public String getErrorStackMessageName()`
This method returns the name of the message to display when the user's password is deemed invalid (i.e., the `validate()` method returns *False*).
3. `public String getErrorStackApplicationName()`
This method returns the application short name for the aforementioned error message.

After writing the customized password validator, set profile option `SIGNON_PASSWORD_CUSTOM` to the full name of the class. If the name of the Java class is `yourco.security.AppsPasswordValidation`, then the value of `SIGNON_PASSWORD_CUSTOM` must be `"yourco.security.AppsPasswordValidation"`. Note, this class must be loaded into the Application database using the `loadjava` command.

ADVANCED SECURITY/NETWORKING OPTION (ASO/ANO)

Oracle Advanced Security provides a single source of integration with network encryption and authentication solutions, single sign-on services, and security protocols. The option protects against threats to the security of distributed environments. Specifically, Oracle Advanced Security provides the following features:

- **Data Integrity:** Prevents data modification during transmission.
- **Data Privacy:** Prevents data disclosure during transmission.
- **Authentication:** Identifies users, hosts and clients securely and provides single sign-on.
- **Authorization:** Ensure that a user, program, or process receives appropriate object access privileges.

Expect a Metalink Note soon providing more information on using ASO/ANO for Oracle E-Business Suite 11i.

CONFIGURE LISTENER ON A NON-DEFAULT .dbc PORT

By default, the TNS Listener receives service requests on TCP port 1521. Configure it to listen on another port number. Although not foolproof, this makes attacks more difficult.

MULTI-NODE TOPOLOGY

“Multi-Node” refers to topologies where Web and Forms processes run on more than one machine. For information on how to configure Oracle E-Business Suite Rapid Install with Oracle9i Application Server across multiple nodes, refer to [Metalink Note 217368.1](#).

HARDENING EXTERNAL PROCEDURE (EXTPROC) SERVICES

The Oracle database uses the external procedure service to call external C programs. This extends the functionality of PL/SQL to routines that can be written in C to perform complex calculations, such as mathematical modeling or files system interactions. This functionality exploits the ability of the Listener to issue operating system commands. The external procedures are supposed to issue the commands to the Listener on a special IPC pipe named EXTPROC. The specification exists in the `listener.ora` parameter file as

```
(ADDRESS_LIST = (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC))
```

These external procedures operate by instructing the Listener to issue these operating system commands on their behalf. Because the Listener runs with the privilege of the operating system user, the only limits on external procedures are the limits on what that account can do.

The following Oracle E-Business suite components use EXTPROC services:

1. Oracle Intermedia (9.2) cartridges -- InterMedia needs to be installed with 11i.
2. Oracle Email Center.
3. Oracle Demand Planning Express implementation.

To protect against some EXTPROC attack vectors:

1. Create two Oracle TNS Listeners, one for the Oracle database and one for PL/SQL EXTPROC.
2. Remove EXTPROC specific entries from the Oracle Database Listener configuration files.
3. Configure the Oracle EXTPROC Listener with an IPC protocol address only.

If TCP connectivity is required, configure a TCP protocol address, but use a port other than the one the Oracle Listener for the database is using. Ensure that the Oracle Listener created for PL/SQL EXTPROC runs as an unprivileged operating system user (e.g., “nobody” on Unix). On Windows platforms, run the Oracle TNS Listener process as an unprivileged user and not as the Windows LOCAL SYSTEM user. Give this user the operating system privilege to “Logon as a service.”

4. If the Oracle Listener for PL/SQL EXTPROC has been configured with a TCP address, do the following:
 - a. Modify the EXTPROC specific entry in `$ORACLE_HOME/network/admin/tnsnames.ora` to reflect the correct port for the new Oracle Listener.
 - b. Enable Valid Node Checking and restrict access to those network clients requiring EXTPROC.
 - c. Restrict access to the Oracle Listener for PL/SQL EXTPROC only. Use a separate `$TNS_ADMIN/sqlnet.ora` file for this Oracle Listener. Store this file in any directory other than the one in which the database `listener.ora` and `sqlnet.ora` files are located. Copy the `listener.ora` with the configuration of the Oracle Listener for PL/SQL EXTPROC into this other directory as well. Before starting the Oracle Listener for PL/SQL EXTPROC, set the `TNS_ADMIN` environment variable (or Windows Registry parameter) to specify the directory in which the new configuration files for PL/SQL EXTPROC are stored.

5. Ensure that the file permissions on separate `$TNS_ADMIN/listener.ora` are set to 600. Because it contains the password, only the owner should read the file.
6. Change the password to a strong password for any privileged database account or an ordinary user given administrative privileges in the database that has the ability to add packages or libraries and access system privileges in the database (such as `CREATE ANY LIBRARY`). This step may not be applicable for default E-Business Suite implementations. This may be useful for customizations that involve addition of new schemas or customized PL/SQL code to be called as an external procedure service.

EXTPROC LISTENER CONFIGURATION

See below for the format of the dedicated EXTPROC Listener. The parameters appear in `$TNS_ADMIN/listener.ora`. Replace the `$ORACLE_SID` with name of the Oracle database instance (SID), `$ORACLE_HOME` with the value of ORACLE HOME directory for this Listener and `$TNS_ADMIN` with the directory location of the Listener parameter files.

```
$ORACLE_SID_EXTPROC =
  (ADDRESS_LIST =
    (ADDRESS= (PROTOCOL= IPC) (KEY= EXTPROC$ORACLE_SID))
  )

SID_LIST_$ORACLE_SID_EXTPROC =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = $ORACLE_HOME)
      (PROGRAM = extproc)
    )
  )

STARTUP_WAIT_TIME_$ORACLE_SID_EXTPROC = 0
CONNECT_TIMEOUT_$ORACLE_SID_EXTPROC = 10
TRACE_LEVEL_$ORACLE_SID_EXTPROC = OFF

LOG_DIRECTORY_$ORACLE_SID_EXTPROC = $TNS_ADMIN
LOG_FILE_$ORACLE_SID_EXTPROC = $ORACLE_SID_EXTPROC
TRACE_DIRECTORY_$ORACLE_SID_EXTPROC = $TNS_ADMIN
TRACE_FILE_$ORACLE_SID_EXTPROC = $ORACLE_SID_EXTPROC
```

The configuration below should appear in `$TNS_ADMIN/tnsnames.ora`. Replace `$ORACLE_SID` with the name of the Oracle database instance (SID).

```
extproc_connection_data =
  (DESCRIPTION=
    (ADDRESS_LIST =
      (ADDRESS= (PROTOCOL=IPC) (KEY=EXTPROC$ORACLE_SID))
    )
    (CONNECT_DATA=
      (SID=PLSExtProc)
      (PRESENTATION = RO)
    )
  ) )
```

Example: EXTPROC Listener configured separately

This example shows how to configure EXTPROC Listener services. In it, the LISTENER NAME is `VSEC1159_EXTPROC` and `ORACLE_SID` is `VSEC1159`.

Extras for Experts

```
VSEC1159_EXTPROC =
  (ADDRESS_LIST =
    (ADDRESS= (PROTOCOL= IPC) (KEY= EXTPROCVSEC1159))
  )

SID_LIST_VSEC1159_EXTPROC =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = /u01/oracle/vsec1159db/9.2.0.5)
      (PROGRAM = extproc)
    )
  )

STARTUP_WAIT_TIME_VSEC1159_EXTPROC = 0
CONNECT_TIMEOUT_VSEC1159_EXTPROC = 10
TRACE_LEVEL_VSEC1159_EXTPROC = OFF

LOG_DIRECTORY_VSEC1159_EXTPROC = /u01/oracle/vsec1159db/9.2.0.5/network/admin
LOG_FILE_VSEC1159_EXTPROC = VSEC1159_EXTPROC
TRACE_DIRECTORY_VSEC1159_EXTPROC = /u01/oracle/vsec1159db/9.2.0.5/network/admin
TRACE_FILE_VSEC1159_EXTPROC = VSEC1159_EXTPROC
```

Example: The tnsnames.ora parameter that corresponds to EXTPROC Listener.

```
extproc_connection_data =
  (DESCRIPTION=
    (ADDRESS_LIST =
      (ADDRESS= (PROTOCOL=IPC) (KEY=EXTPROCVSEC1159))
    )
    (CONNECT_DATA=
      (SID=PLSExtProc)
      (PRESENTATION = RO)
    )
  ) )
```

EXTPROC TESTING PROCEDURE

This section explains a procedure to test if EXTPROC is enabled. The EXTPROC Listener must be configured and working for InterMedia option to run. Do the following to test whether InterMedia is working:

1. Create a user to work with InterMedia Text:

```
create user textuser identified by <password> \
  default tablespace users temporary tablespace temp;
```

2. Grant 'ctxapp' role to textuser:

```
grant connect, resource, ctxapp to <password>;
```

3. Connect as textuser and create required test objects:

```
connect textuser/<password>

drop table quick;

create table quick (
  quick_id          number
  constraint quick_pk primary key,
```

Extras for Experts

```
text                varchar2(80) );

insert into quick ( quick_id, text ) values ( 1, 'The cat sat on the mat' );
insert into quick ( quick_id, text ) values ( 2, 'The quick brown fox jumps over
the lazy dog' );
insert into quick ( quick_id, text ) values ( 3, 'The dog barked like a dog' );
commit;

create index quick_text on quick ( text ) indextype is ctxsys.context;

col text format a45
col s format 999
select text, score(42) s from quick
  where contains ( text, 'dog', 42 ) >= 0
 order by s desc;
```

If the above query works without any error, the InterMedia option is enabled and the EXTPROC Listener is properly configured.

Cleanup the test user (textuser) created during this test.

Appendix A: Security Setup Forms

Form Function	Form Name	Table Name
FND_FNDATDAG	FNDATDAG Audit Groups	FND_AUDIT_GROUPS
FND_FNDATDAI	FNDATDAI Audit Installations	FND_AUDIT_SCHEMAS
FND_FNDATDAT	FNDATDAT Audit Tables	FND_AUDIT_TABLES FND_AUDIT_COLUMNS
FND_FNDFMFBF	FNDFMFBF Forms	FND_FORM
FND_FNDFMFUN	FNDFMFUN Functions	FND_FORM_FUNCTIONS
FND_FNDMNMNU	FNDMNMNU Menus	FND_MENUS FND_MENU_ENTIRES
FND_FNDPMPV	FNDPMPV Profile System Values	FND_PROFILE_OPTION_VALUES
FND_FNDRSGRP	FNDRSGRP Request Groups	FND_REQUEST_GROUPS FND_REQUEST_GROUP_UNITS
FND_FNDSCAUS	FNDSCAUS Users	FND_USER FND_USER_RESP_GROUPS
FND_FNDSCPLS	FNDSCPLS Web Enabled PL/SQL	FND_ENABLED_PLSQL
FND_FNDSCRSP XDP_FNDSCRSP	FNDSCRSP Responsibilities	FND_RESP_FUNCTIONS

To find which users have a particular function (e.g FND_FNDATDAG), use the following version-specific queries.

11.5.9

```

select fu.user_name
from fnd_user fu,
     fnd_user_resp_groups furg,
     fnd_responsibility fr,
     fnd_compiled_menu_functions fcmf,
     fnd_form_functions fff
where furg.responsibility_id = fr.responsibility_id
and furg.responsibility_application_id = fr.application_id
and fr.menu_id = fcmf.menu_id
and fcmf.grant_flag = 'Y'
and fcmf.function_id = fff.function_id
and fff.function_name = 'FND_FNDATDAG'
and furg.user_id = fu.user_id
and sysdate between furg.start_date and nvl(furg.end_date, sysdate+1)
and sysdate between fu.start_date and nvl(fu.end_date, sysdate+1)
and sysdate between fr.start_date and nvl(fr.end_date, sysdate+1)
union
select distinct wu.name
from fnd_grants fg,
     wf_user_roles wur,
     fnd_compiled_menu_functions fcmf,
     fnd_form_functions fff,
     wf_roles wr,
     wf_users wu
where fg.menu_id = fcmf.menu_id
and fcmf.function_id = fff.function_id
and fff.function_name = 'FND_FNDATDAG'
and fg.grantee_type in ('USER', 'GROUP')
and fg.grantee_key = wur.role_name
and wur.role_name = wr.name
and wur.role_orig_system = wr.orig_system

```

Appendix A: Security Setup Forms

```
and wur.role_orig_system_id = wr.orig_system_id
and wur.user_name = wu.name
and wur.user_orig_system = wu.orig_system
and wur.user_orig_system_id = wu.orig_system_id
and wu.orig_system in ('FND_USR', 'PER')
and sysdate between fg.start_date and nvl(fg.end_date, sysdate+1)
and sysdate between nvl(wur.start_date, sysdate-1)
                    and nvl(wur.expiration_date, sysdate+1)
and sysdate between nvl(wr.start_date, sysdate-1)
                    and nvl(wr.expiration_date, sysdate+1)
and sysdate between nvl(wu.start_date, sysdate-1)
                    and nvl(wu.expiration_date, sysdate+1);
```

11.5.10

```
select fu.user_name
from fnd_user fu,
     fnd_user_resp_groups furg,
     fnd_responsibility fr,
     fnd_compiled_menu_functions fcmf,
     fnd_form_functions fff
where furg.responsibility_id = fr.responsibility_id
and furg.responsibility_application_id = fr.application_id
and fr.menu_id = fcmf.menu_id
and fcmf.grant_flag = 'Y'
and fcmf.function_id = fff.function_id
and fff.function_name = 'FND_FNDATDAG'
and furg.user_id = fu.user_id
and sysdate between fu.start_date and nvl(fu.end_date, sysdate+1)
and sysdate between fr.start_date and nvl(fr.end_date, sysdate+1)
union
select distinct incrns.name
from fnd_grants fg,
     wf_user_roles wur,
     fnd_compiled_menu_functions fcmf,
     fnd_form_functions fff,
     wf_roles wr,
     wf_users wu,
     wf_users incrns
where fg.menu_id = fcmf.menu_id
and fcmf.function_id = fff.function_id
and fff.function_name = 'FND_FNDATDAG'
and fg.grantee_type in ('USER', 'GROUP')
and fg.grantee_key = wur.role_name
and wur.role_name = wr.name
and wur.role_orig_system = wr.orig_system
and wur.role_orig_system_id = wr.orig_system_id
and wur.user_name = wu.name
and wur.user_orig_system = wu.orig_system
and wur.user_orig_system_id = wu.orig_system_id
and wu.parent_orig_system = incrns.parent_orig_system
and wu.parent_orig_system_id = incrns.parent_orig_system_id
and incrns.orig_system in ('FND_USR', 'PER')
and sysdate between fg.start_date and nvl(fg.end_date, sysdate+1)
and sysdate between nvl(wur.start_date, sysdate-1)
                    and nvl(wur.expiration_date, sysdate+1)
and sysdate between nvl(wr.start_date, sysdate-1)
                    and nvl(wr.expiration_date, sysdate+1)
and sysdate between nvl(wu.start_date, sysdate-1)
                    and nvl(wu.expiration_date, sysdate+1)
and sysdate between nvl(incrns.start_date, sysdate-1)
                    and nvl(incrns.expiration_date, sysdate+1);
```

Appendix B: Security Setup Forms That Accept SQL Statement

Form Function	Form Name	Table Name
ALR_ALRALERT	ALRALERT	ALR_ALERTS
FND_FNDCPMCP_SYS	FNDCPMCP	FND_CONCURRENT_PROGRAMS
FND_FNDCPMPE	FNDCPMPE	FND_EXECUTABLES
FND_FNDPOMPO	FNDPOMPO	FND_PROFILE_OPTIONS
FND_FNDSCAPP	FNDSCAPP	FND_APPLICATION
FND_FNDSCDDG	FNDSCDDG	FND_DATA_GROUPS FND_DATA_GROUP_UNITS
FND_FNDSCMOU	FNDSCMOU	FND_ORACLE_USERID
PSB_PSBSTPTY	PSBSTPTY	PSB_ATTRIBUTE_TYPES
MSDCSDFN	MSDCSDFN	MSD_CS_DEFINITIONS
MSDCSDFA	MSDCSDFA	MSD_CS_DEFINITIONS
MSD_MSDAUDIT	MSDAUDIT	MSD_AUDIT_SQL_STATEMENTS
JTFRSDGR	JTFRSDGR	JTF_RS_DYNAMIC_GROUPS_B JTF_RS_DYNAMIC_GROUPS_TL
JTFBRWKB	JTFBRWKB	JTF_BRM_RULES_B
ONT_OEXPCFVT	OEXPCFVT	OE_PC_CONSTRAINTS OE_PC_CONDITIONS OE_PC_ASSIGNMENTS OE_PC_VTMPLTS
ONT_OEXDEFWK, QP_OEXDEFWK	OEXDEFWK	OE_DEF_ATTR_DEF_RULES
JTFTKOBT	JTFTKOBT	JTF_OBJECTS_B JTF_OBJECTS_TL JTF_OBJECT_USAGES
JTF_GRID_ADMIN	JTFGRDMD	JTF_GRID_DATASOURCES_B JTF_GRID_COLS_B
JTFGDIAG	JTFGDIAG	JTF_GRID_DATASOURCES_B JTF_GRID_COLS_B
JTFGANTT	JTFGANTT	JTF_RS_RESOURCE_EXTNS JTF_RS_GROUPS_B JTF_RS_TEAMS_B
WMS_WMSRULEF	WMSRULEF	
QP_QPXPRFOR	QPXPRFOR	QP_PRICE_FORMULAS_B
QP_QPXPTMAP	QPXPTMAP	QP_ATTRIBUTE_SOURCING
GMAWFPCF_F	GMAWFPCF	GMA_PROCDEF_WF
GMAWFCOL_F	GMAWFCOL	GMA_ACTDEF_WF
AME_WEB_APPROVALS	-	AME_ATTRIBUTE_USAGES AME_APPROVAL_GROUPS
PERWSAPI	PERWSAPI	N/A
FFXWSMNG	FFXWSMNG	FF_FUNCTIONS
FFXWSDFP	FFXWSDFP	FF_FUNCTIONS
FFXWSBQR	FFXWSBQR	FF_QP_REPORTS

Appendix B: Security Setup Forms That Accept SQL Statement

PAYWSDAS	PAYWSDAS	HR_ASSIGNMENT_SET_CRITERIA
PAYWSDYG	PAYWSDYG	PAY_TRIGGER_COMPONENTS PAY_TRIGGER_INITIALISATIONS PAY_TRIGGER_SUPPORT
PERWSSCP	PERWSSCP	PER_SECURITY_PROFILES

Appendix C: Processes Used by E-Business Suite

Process Name	Description	Script
tnslsnr	Applications RPC Listener process	adalnctl.sh
httpd httpds java	Apache Web Server Listener	adapcctl.sh
FNDLIBR FNDSM INVLIBR	Concurrent Manager	adcmctl.sh
oad osagent jre oracle.disco.locator.Locator	Discoverer processes	addisctl.sh
d2lc60	Forms Metrics Client	adfmctl.sh
d2ls60	Forms Metrics Server	adfmsctl.sh
f60srvm f60webmx	Forms Server Listener process	adfrmctl.sh
rwmts60	Reports Server	adrepctl.sh
jre oracle.apps.fnd.tcf.ServerControl	TCF SocketServer process	adtcctl.sh
java oracle.apps.jtf.fm.engine.processor.Processor java oracle.apps.jtf.fm.engine.remote.RemoteCommand	Fulfillment Server process	jtffmctl.sh

Appendix D: Ports Used by E-Business Suite

Appendix D: Ports Used by E-Business Suite

Variable Name	Description	Default Value	Firewall Configuration	Technology	Component
s_dbport	Port on the database server used by the Net8 Listener	1521	Port should be open on the second level firewall	RDBMS	TNS Listener
s_repsport	Port on the concurrent processing server used by the Reports server	7000		Developer 6i	Reports
s_rpcport	RPC port on the concurrent processing server that receives incoming Report Review Agent requests	1626		Applications	Concurrent processing
s_formsport	Port on the Forms server used by the Forms Listener	9000	Port should be open on the first level firewall if forms server is used	Developer 6i	Forms
s_tcfport	Port on the Forms server used by the TCF socket server	-1	Port need not be open if server is used	Applications	TCF
s_metdataport	Port on the Forms server used by the Metrics Server as a data port	9100	Port should be open on the first level firewall if forms server is used	Developer 6i	Forms
s_metreqport	Port on the Forms server used by the Metrics Server as a request port	9200	Port should be open on the first level firewall if forms server is used	Developer 6i	Forms
s_mwaPortNo	MSCA Server Port Number	10200		Applications	Mobile
s_mwaDispatcherPort	MSCA Dispatcher Port Number	10300		Applications	Mobile
s_oemweb_port	OEM Web Utility Port	10000		iAS	OEM
s_osagent_port	VisiBroker Server Agent Port	10100	Port should be open on the first level firewall if disco plus is used. Not required if viewer is used.	iAS	Discoverer
s_webport	Port on the webserver where http server listens for non-ssl requests	80	Port should be open on the first level firewall	iAS	Oracle HTTP Server
s_webssl_port	Port on the webserver where http server listens for ssl requests	443	Port should be open on the first level firewall	iAS	Oracle HTTP Server
s_active_webport	Value of this variable is set to value of s_webport when Listener is configured in non-ssl mode and to the value of s_webssl_port when ssl is configured	80/443	This is not a separate port that we are opening. It is either s_webport or s_websslport	iAS	Oracle HTTP Server
s_webport_pls	Port on the webserver where http server listens for mod/plsql requests	8888	Port need not be open on any level of firewall	iAS	Oracle HTTP Server
s_oprocmgr_port	Port on the webserver where Jserv processes register with the oprocmgr	8699	Port need not be open on any level of firewall	iAS	Oracle HTTP Server
s_forms_servlet_portrange	Port range on the webserver for Forms group where jserv processes listen for ajp requests	8701-8710		iAS	Jserv
s_disco_servlet_portrange	Port range on the webserver for Disco group where jserv processes listen for ajp requests	8711-8720		iAS	Jserv

Appendix D: Ports Used by E-Business Suite

s_xmlsvcs_servlet_porrange	Port range on the webserver for XMLSVCS group where jserv processes listen for ajp requests	8741-8750		iAS	Jserv
s_oacore_servlet_porrange	Port range on the webserver for OA core group where jserv processes listen for ajp requests	8721-8740		iAS	Jserv
s_servletport	Port on the webserver where jserv process listen for ajp requests .Used only by iAS 1.0 and 1.0.2.1S	8800		iAS	Jserv
s_proxyport	Applications server side proxy port used by imeeting	80		Applications	iMeeting
s_jtfuf_port	JTF fulfilment server port	11000		Applications	JTF

Appendix E: Sample Linux Hardening of the Application Tier

This section contains an example of how we hardened an Application Tier running the Linux Operating System. We provide this for illustration purposes, only. Customer experience may vary.

Use standard install of Operating System including X and ssh. During EBS installation, use the native X interface on the console.

Perform the EBS installation using AutoConfig as a Rapid Install Vision multinode configuration with the functionality split onto separate hosts for web service, Forms and Discoverer service, and Reports and Concurrent Manager service. Copy the context file generated during the installation of the database onto each middle-tier and run the rapid installation via NFS from a shared staging area.

After the installation of the Operating System and EBS, stop (and disable) unnecessary daemons - networked daemons in particular.

```
$ chkconfig --level 3 sgi_fam off
$ chkconfig --level 3 xinetd off
$ chkconfig --level 3 nfslock off
$ chkconfig --level 3 portmap off
$ chkconfig --level 3 gpm off
$ chkconfig --level 3 atd off
```

With these changes and a runlevel change to 3, netstat on the Linux box is very short:

```
$ netstat -lptuxn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp        0      0 0.0.0.0:22      0.0.0.0:*       LISTEN 846/sshd
tcp        0      0 127.0.0.1:25    0.0.0.0:*       LISTEN 902/sendmail: accep

Active UNIX domain sockets (only servers)
Proto RefCnt Flags  Type State I-Node PID/Program Path
unix    2      [ ACC ] STREAM LISTENING 1215 969/xfss /tmp/.font-unix/fs7100
```

The only network accessible daemon running is the ssh daemon. Sendmail listens only on the localhost interface kept active for outbound mail. Examples of outbound email include workflow generated messages and monitoring alerts. Middle-tier Java calls the X server which in turn calls the X fontserver running on a UNIX socket.

Running processes include:

```
UID      PID     PPID    C  STIME TTY          TIME CMD
root     14      0   0  18:02 ?          00:00:00 [kupdated]
root     13      0   0  18:02 ?          00:00:00 [bdflush]
root     12      0   0  18:02 ?          00:00:00 [krefilld]
root     11      0   0  18:02 ?          00:00:00 [kreclaimd]
root     10      0   0  18:02 ?          00:00:00 [kswapd]
root      9      0   0  18:02 ?          00:00:00 [ksoftirqd_CPU3]
root      8      0   0  18:02 ?          00:00:00 [ksoftirqd_CPU2]
root      7      0   0  18:02 ?          00:00:00 [ksoftirqd_CPU1]
root      6      0   0  18:02 ?          00:00:00 [ksoftirqd_CPU0]
root      1      0   2  18:02 ?          00:00:04 init
root      2      1   0  18:02 ?          00:00:00 [keventd]
root      3      1   0  18:02 ?          00:00:00 [keventd]
root      4      1   0  18:02 ?          00:00:00 [keventd]
root      5      1   0  18:02 ?          00:00:00 [keventd]
root     15      1   0  18:02 ?          00:00:00 [mdrecoveryd]
root     23      1   0  18:02 ?          00:00:00 [kjournald]
root    150      1   0  18:02 ?          00:00:00 [kjournald]
root    151      1   0  18:02 ?          00:00:00 [kjournald]
root    152      1   0  18:02 ?          00:00:00 [kjournald]
root    153      1   0  18:02 ?          00:00:00 [kjournald]
root    154      1   0  18:02 ?          00:00:00 [kjournald]
root    659      1   0  18:03 ?          00:00:00 syslogd -m 0
root    664      1   0  18:03 ?          00:00:00 klogd -2
root    846      1   0  18:03 ?          00:00:00 /usr/sbin/sshd
```

Appendix E: Sample Linux Hardening of the Application Tier

```
root 1034 846 0 18:04 ? 00:00:00 /usr/sbin/sshd
root 1035 1034 0 18:04 pts/0 00:00:00 -bash
root 1090 1035 0 18:05 pts/0 00:00:00 ps -eHf
root 902 1 0 18:03 ? 00:00:00 sendmail: accepting connections
root 921 1 0 18:03 ? 00:00:00 crond
xfs 969 1 0 18:03 ? 00:00:00 xfs -droppriv -daemon
root 1026 1 0 18:03 tty1 00:00:00 /sbin/mingetty tty1
root 1027 1 0 18:03 tty2 00:00:00 /sbin/mingetty tty2
root 1028 1 0 18:03 tty3 00:00:00 /sbin/mingetty tty3
root 1029 1 0 18:03 tty4 00:00:00 /sbin/mingetty tty4
root 1030 1 0 18:03 tty5 00:00:00 /sbin/mingetty tty5
root 1031 1 0 18:03 tty6 00:00:00 /sbin/mingetty tty6
```

CONFIGURE THE X SERVER

To fulfill the requirement for an available X server, configure VNC on display 66 on each middle-tier host. Running the X server on each middle-tier avoids dependencies on additional hosts, thereby making the deployment more resilient.

VNC listens for web requests starting at port 5800. To prevent a web browser from being used as a VNC client modify the `vncserver` script and comment out the `-httpd` parameter to `Xvnc`.

```
#!/$cmd .= " -httpd $vncClasses";
```

The entire VNC invocation is as follows:

```
$ oravncserver :66 -geometry 800x600 -depth 8 -dpi 72 -cc 3 -nolisten local -localhost
```

To prevent VNC from listening on a UNIX domain socket start the `vncserver` script using `-no` local parameters. The `-localhost` makes `Xvnc` listen only on the localhost interface for RFB requests (127.0.0.1:5966). Although the X server listens on all interfaces for the X port (0.0.0.0:6066), it is protected by the `xauth` cookie and only accepts connections from localhost (`xhost + localhost`).

```
sort -t: +ln | egrep 'Xvnc|^Proto'
```

```
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 127.0.0.1:5966 0.0.0.0:* LISTEN 2442/Xvnc
tcp 0 0 0.0.0.0:6066 0.0.0.0:* LISTEN 2442/Xvnc
```

WEB-TIER OPEN PORTS

Open the following ports for the Web-tier components.

```
$ netstat -lptuxn
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:1632 0.0.0.0:* LISTEN 23574/tnslsnr
tcp 0 0 0.0.0.0:51217 0.0.0.0:* LISTEN 23673/osagent
tcp 0 0 0.0.0.0:51226 0.0.0.0:* LISTEN 23694/oad
tcp 0 0 0.0.0.0:51235 0.0.0.0:* LISTEN 23706/jre
tcp 0 0 0.0.0.0:51237 0.0.0.0:* LISTEN 23725/dis4pr
tcp 0 0 0.0.0.0:6066 0.0.0.0:* LISTEN 10157/Xvnc
tcp 0 0 0.0.0.0:8006 0.0.0.0:* LISTEN 23391/httpd
tcp 0 0 0.0.0.0:8106 0.0.0.0:* LISTEN 23391/httpd
tcp 0 0 0.0.0.0:8206 0.0.0.0:* LISTEN 23511/httpd
tcp 0 0 127.0.0.1:5966 0.0.0.0:* LISTEN 10157/Xvnc
tcp 0 0 130.35.84.120:16060 0.0.0.0:* LISTEN 23408/java
tcp 0 0 130.35.84.120:17060 0.0.0.0:* LISTEN 23409/java
tcp 0 0 130.35.84.120:19060 0.0.0.0:* LISTEN 23410/java
udp 0 0 0.0.0.0:10100 0.0.0.0:* 23673/osagent
udp 0 0 0.0.0.0:32810 0.0.0.0:* 23673/osagent
udp 0 0 0.0.0.0:32811 0.0.0.0:* 23694/oad
udp 0 0 0.0.0.0:32812 0.0.0.0:* 23694/oad
udp 0 0 0.0.0.0:32813 0.0.0.0:* 23706/jre
udp 0 0 0.0.0.0:9306 0.0.0.0:* 23625/java
```

Appendix E: Sample Linux Hardening of the Application Tier

```
Active UNIX domain sockets (only servers)
Proto RefCnt Flags Type State I-Node PID/Program name Path
unix 2 [ ACC ] STREAM LISTENING 1236 - /tmp/.font-unix/fs7100
unix 2 [ ACC ] STREAM LISTENING 3360927 23574/tnslsnr /var/tmp/.oracle/s#23574.1
unix 2 [ ACC ] STREAM LISTENING 3364817 23725/dis4pr /tmp/orb_23725_0
```

FORMS AND DISCOVERER OPEN PORTS

Open the following ports for the Forms and Discoverer components:

```
$ netstat -ltuxpn
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:1632 0.0.0.0:* LISTEN 24896/tnslsnr
tcp 0 0 0.0.0.0:9006 0.0.0.0:* LISTEN 24955/f60srvm
tcp 0 0 127.0.0.1:5966 0.0.0.0:* LISTEN 2442/Xvnc
tcp 0 0 0.0.0.0:6066 0.0.0.0:* LISTEN 2442/Xvnc
udp 0 0 130.35.84.112:32778 0.0.0.0:* 24975/d21c60
udp 0 0 0.0.0.0:32779 0.0.0.0:* 24992/d21s60
udp 0 0 0.0.0.0:32780 0.0.0.0:* 24992/d21s60
udp 0 0 0.0.0.0:9106 0.0.0.0:* 24992/d21s60
udp 0 0 0.0.0.0:9206 0.0.0.0:* 24992/d21s60
```

```
Active UNIX domain sockets (only servers)
Proto RefCnt Flags Type State I-Node PID/Program name Path
unix 2 [ ACC ] STREAM LISTENING 1215 - /tmp/.font-unix/fs7100
unix 2 [ ACC ] STREAM LISTENING 2852 2442/Xvnc /tmp/.X11-unix/X66
unix 2 [ ACC ] STREAM LISTENING 59477400 24896/tnslsnr /var/tmp/.oracle/s#24896.1
```

CONCURRENT MANAGER AND REPORTS TIER OPEN PORTS

Open the following ports for the Concurrent Manager and Report tier components:

```
$ netstat -ltuxpn
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:1632 0.0.0.0:* LISTEN 1129/tnslsnr
tcp 0 0 0.0.0.0:7006 0.0.0.0:* LISTEN 1247/rwmmts60
tcp 0 0 127.0.0.1:5966 0.0.0.0:* LISTEN 2442/Xvnc
tcp 0 0 0.0.0.0:6066 0.0.0.0:* LISTEN 2442/Xvnc
```

```
Active UNIX domain sockets (only servers)
Proto RefCnt Flags Type State I-Node PID/Program name Path
unix 2 [ ACC ] STREAM LISTENING 1215 - /tmp/.font-unix/fs7100
unix 2 [ ACC ] STREAM LISTENING 2852 2442/Xvnc /tmp/.X11-unix/X66
unix 2 [ ACC ] STREAM LISTENING 313930 1129/tnslsnr /var/tmp/.oracle/s#1129.1
```


Appendix F: References & More Resources

The table below contains references consulted in the preparation of this document as well as other resource material useful for securing E-Business Suite.

DocID	Document
CIS	The Center for Information Security: Oracle Benchmark Tools
DK	“Effective Oracle Database 10g Security by Design”, David Knox
IntA	“ Guide to Auditing in Oracle Applications ”, Integrity Corporation
IntB	“ Oracle Applications 11i Security Quick Reference ”, Integrity Corporation
MTAN	“Oracle Security Handbook : Implement a Sound Security Plan in Your Oracle Environment”, Marlene L. Theriault, Aaron Newman
NGSS	“ Hackproofing Oracle Application Server (A Guide to Securing Oracle 9) ”, Next Generation Security Software, Ltd.
PF	“Oracle Security - Step by Step”, Pete Finnigan

