Oracle® Default Password Scanner

User's Guide

Release 1.0

B28036-01

April 2006

ORACLE®

Oracle Default Password Scanner User's Guide, Release 1.0

B28036-01

Primary Author: Patricia Huey

Contributor: Robert Armstrong, Jim Benge, Norman Bock, Mark Fallon, Tami Gallupe, Erik Graversen, Ray Hachem, Dave Kerr, Rajan Modi, Kant C. Patel, Ranga Polisetti, Karthik Rajan, Rajiv Sharma, Vera So, Yuru Stamas, Venu Surakanti, Darius Wiles, Jose Wong

Contents

5 Troubleshooting Oracle Default Password Scanner

Preface

This guide explains how you can secure Oracle default database accounts by using Oracle Default Password Scanner. This section covers the following topics:

Audience

This document is intended for database administrators or other personnel who are responsible for maintaining security for Oracle products.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction

This chapter explains why you need to check Oracle default database accounts for default passwords, and how you can use Oracle Default Password Scanner to help secure these accounts. It covers the following topics:

What Are Oracle Default Database Accounts and Default Passwords?

Oracle provides a set of default database accounts with most Oracle products. For example, when you install Oracle Database, the `SYS` and `SYSTEM` administrative accounts are created so that database administrators can create user accounts, assign privileges, and perform other database administrative tasks, as required. Sample user accounts are created as well.

During installation, Oracle Universal Installer (or other Oracle installer) allows you either to create individual passwords for each account or use the default password generated by the installation process.

When you upgrade an Oracle database, the upgrade preserves the default accounts from the earlier version. Default accounts for upgraded and migrated databases are cumulative. Release 10*g* databases that have been upgraded from Oracle 7, Oracle8*i*, and Oracle9*i* may also have these older default accounts, which could have default passwords or accounts not locked.

Oracle strongly recommends that you do the following:

- Assign each default account a new password, to better safeguard and secure your databases. You increase the risk of unauthorized access to your database if you do not lock these accounts or change their passwords.
- Run Oracle Default Password Scanner on every database instance to determine if any default accounts remain unlocked with a default password.

Oracle recommends that you adhere to Oracle best practices for security in order to protect your database systems. The Oracle Default Password Scanner assists in identifying Oracle default database accounts with default passwords that need to be secured, but does not replace the need to implement other best practices. "Additional Oracle Security Information" on page 1-2 lists best practices documentation, in addition to other security-related resources.

Third Party Products that Depend on Oracle Default Accounts

For Oracle Database default accounts that are used by customized or third-party products that may depend on the Oracle Database default accounts, refer to the product's documentation for information on securing the products.

What Is Oracle Default Password Scanner?

Oracle Default Password Scanner is a SQL script that queries your Oracle database for accounts that are unlocked (open) and have default passwords. It then generates a report listing these accounts. Afterwards, you can use the instructions in this guide to secure the accounts listed in this report.

You can run Oracle Default Password Scanner without adversely impacting your system's performance, even during normal operational hours.

You will follow these general steps:

1. In Chapter 2, "Installing and Running Oracle Default Password Scanner", install and run Oracle Default Password Scanner to generate a report listing the accounts you need to secure.
2. In Chapter 3, "List of Default Database Accounts", check Table 3–1 to find out which of your Oracle products use or provide the accounts listed in the Oracle Default Password Scanner report. The security solution you use depends on the product that uses the account.
3. In Chapter 4, "Security Solutions for Oracle Default Database Accounts", implement the security solution listed for your Oracle products that contain unsecured accounts.

If you encounter problems with the procedures in this guide, see Chapter 5, "Troubleshooting Oracle Default Password Scanner" for troubleshooting advice.

Additional Oracle Security Information

For more information on managing Oracle security:

- Oracle Security Technology Center:

  `http://www.oracle.com/technology/deploy/security/index.html`

- Oracle Database security-specific information on OTN:

  `http://www.oracle.com/technology/deploy/security/db_security/index.html`

- Oracle Security Checklist whitepaper on OTN:

  `http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf`

- *Security Vulnerability Fixing Policy and Process* whitepaper on OTN:

  `http://www.oracle.com/technology/deploy/security/pdf/securityfixlifecycle.html`

- Oracle*MetaLink*: This site provides a variety of resources such as forums, a customer knowledge base, and certification information. In addition, you can download the latest security patches and file service requests from Oracle*MetaLink*. The URL is:

  `http://metalink.oracle.com/`

Patches and notes specific to Oracle Default Password Scanner are as follows:

- 4926128: Executable download for Oracle Default Password Scanner. Includes this guide, *Oracle Default Password Scanner User's Guide*, with the file name of `B28036_01.pdf`.
- 361482.1: Frequently Asked Questions about Oracle Default Password Scanner

- Oracle Security documentation (OTN):

  `http://www.oracle.com/technology/documentation/index.html`

  To view the library for a particular product, select the product name, and then in the product's documentation page, under Link, either click **View Library** or select the manual's **PDF** or **HTML** link. In particular, you may want to view the following manuals:

  - *Oracle Database Security Guide 10g Release 2 (10.2)* on OTN:

    `http://download-west.oracle.com/docs/cd/B19306_01/network.102/b14266.pdf`

  - *Oracle Database Security Guide 10g Release 1 (10.1)* on OTN:

    `http://download-west.oracle.com/docs/cd/B14117_01/network.101/b10773.pdf`

  - *Oracle Application Server Security Guide 10g Release 2 (10.1.2)* on OTN:

    `http://download-west.oracle.com/docs/cd/B14099_09/core.1012/b13999/toc.htm`

  - *Oracle Application Server 10g Security Guide 10g (9.0.4)* on OTN:

    `http://download-west.oracle.com/docs/cd/B10464_05/core.904/b10377/toc.htm`

- Depending on your Oracle product, install and use password policies. You can find more information from both Oracle*MetaLink* and your Oracle product administrator's guide.
- *Configuring A Secure Oracle9i Application Server Environment* whitepaper on OTN:

  `http://www.oracle.com/technology/deploy/security/oracle9iAS/pdf/securingias.pdf`

- *Best Practices for Securing Oracle E-Business Suite* whitepaper Oracle*MetaLink*. Search for Note 189367.1.

2

Installing and Running Oracle Default Password Scanner

This chapter explains how to install and run Oracle Default Password Scanner. You will follow these general steps:

- Step 1: Install Oracle Default Password Scanner
- Step 2: Run Oracle Default Password Scanner
- Step 3: Check the Oracle Default Accounts

Step 1: Install Oracle Default Password Scanner

To install Oracle Default Password Scanner:

1. Go to the OracleMetaLink Web site:

   `http://metalink.oracle.com/`

2. If you are not registered with OracleMetaLink, follow the instructions online to register. Then log in to Oracle *MetaLink*.
3. Click **Patches & Updates** on the main OracleMetaLink page.
4. Select **Simple Search**.
5. Enter patch number 4943798, and then click **Go**.

   To ensure that you have the latest version of this guide, search for and download patch note 361483.1. For frequently asked questions about Oracle Default Password Scanner, search for and download patch note 361482.1.
6. Download patch 4943798, which is entitled Oracle Default Password Scanner.
7. Unzip the `4943798.zip` file into an empty directory. The unzipped file that appears is the SQL script `dfltpass.sql`.

   If you do not have an unzip or decompression utility, you can download UnZip, which is available from the following location:

   `http://www.info-zip.org/pub/infozip/UnZip.html`

Step 2: Run Oracle Default Password Scanner

This section covers the following topics:

- Running Oracle Default Password Scanner
- Customizing the Oracle Default Password Scanner dfltpass.sql Script

Running Oracle Default Password Scanner

You should run Oracle Default Password Scanner on a periodic basis, for example, after you have installed an Oracle product or applied a patch update to an existing Oracle installation.

To run Oracle Default Password Scanner:

1. Go to the directory where you unzipped the `4943798.zip` file.
2. Log onto the Oracle database locally with administrative privileges and run Oracle Default Password Scanner. For example:

```
$ sqlplus system
Enter password: password
SQL> SPOOL default_passwords_database_timestamp.txt
SQL> @dfltpass
SQL> SPOOL OFF
```

   In this example:

   - *database* refers to the SID or database instance name on which you are running the report.
   - *timestamp* refers to the date when you run the report.

3. Store the report in a safe place.

   When you are finished securing your accounts, you may want to delete the report.

If the database has no default accounts that are unlocked and use default passwords, the output will be as follows:

```
no rows selected
```

Otherwise, the output contains the account name and status of each default account with a default password whose the account is unlocked. An example of the generated output is as follows:

```
Default Database Accounts With Default Passwords

Account Name                   Account Status
------------------------------ --------------------------------
CTXSYS                         OPEN
ORDCOMMON                      OPEN
OUTLN                          OPEN
SCOTT                          OPEN
SYSTEM                         OPEN
```

If this happens, follow the instructions under "Step 3: Check the Oracle Default Accounts" on page 2-4 to begin securing these accounts.

If you encounter problems running Oracle Default Scanner, see Chapter 5, "Troubleshooting Oracle Default Password Scanner" for troubleshooting advice.

Customizing the Oracle Default Password Scanner dfltpass.sql Script

Oracle Default Password Scanner is a simple SQL script that includes only Oracle default accounts. If you want to add default accounts released by other software vendors or deployed by your organization, you can customize the Oracle Default Password Scanner `dfltpass.sql` script to include additional default usernames and passwords specific to your environment.

The main part of the Oracle Default Password Scanner script is a `SELECT` statement that compares a list of known usernames and hashed passwords with records in the `SYS.DBA_USERS` view. Matching usernames are sorted and output. The `WHERE` clause for the statement contains pairs of usernames and hashed passwords, one per line, in the following format:

```
('USERNAME',  'HASHED PASSWORD'),
```

To customize the script, you need first to find the hashed passwords for the default accounts you want to add, and then add this information to a customized version of the script.

Follow these steps:

1. Go to the directory where you unzipped the `4943798.zip` file, which contains the `dfltpass.sql` script.
2. Copy the `dfltpass.sql` script to a file with a different name to ensure that future versions of the `dfltpass.sql` script that you download do not overwrite your customized version.
3. Log into SQL*Plus with database administrative privileges:

   ```
   $ sqlplus / as sysdba
   ```

   You will use the database to create the default accounts and record password hashes to add to the script.
4. Determine the hashed passwords for the username/password pairs you want to add to the script.

   To determine the hashed password for an account not currently on the system, first create the user. For example:

   ```
   SQL> CREATE USER MYUSERNAME IDENTIFIED BY MYPASSWORD;
   User created.
   ```

   Obtain the password for the new account:

   ```
   SQL> SELECT USERNAME, PASSWORD FROM DBA_USERS WHERE USERNAME='MYUSERNAME';

   USERNAME                       PASSWORD
   ------------------------------ ------------------------------
   MYUSERNAME                     41C2510A47994810
   ```
5. Clean up by dropping the users you have just created, for example:

   ```
   SQL> DROP USER MYUSERNAME;
   ```
6. Exit SQL*Plus:

   ```
   SQL> EXIT;
   ```
7. Use a text editor to edit the copy of the `dfltpass.sql` file that you created in step 2.

   For each user name/password pair, add a new row to the script using the following format:

   ```
   ('USERNAME',  'HASHED PASSWORD'),
   ```

   For example:

   ```
   ('MYUSERNAME',  '41C2510A47994810'),
   ```

You can add the rows to the script in any order. Also, you can add the same user name multiple times to check for different passwords.

8. Install and run the script on your site's servers to check for default user names and passwords, similar to the procedure for the `dfltpass.sql` script under "Running Oracle Default Password Scanner" on page 2-2.

Step 3: Check the Oracle Default Accounts

Now that you have a list of Oracle default accounts that are unlocked and use default passwords, you are ready to secure them.

Follow these steps:

1. Test changing the default accounts in a test environment before trying to change them in a production environment.
2. Check for any Oracle or non-Oracle applications that are dependent on the default accounts you plan to change.

   For example, if the default account was created through an Oracle application, you may need to change the password through that application, not through SQL*Plus, or you may need to change the password through both SQL and in the application.
3. Go to Chapter 3 and check Table 3–1 to find the products that use the accounts listed in your report.

   The security solution that you perform depends on the products that use the account. Chapter 4 provides instructions for securing the accounts, based on the products listed in Table 3–1.

   For example, suppose the report you generate lists the `ABM` account, which is used in Oracle E-Business Suite. In this case, you would follow the instructions in "Securing Oracle E-Business Suite Application Default Accounts" on page 4-9.

   Some products share the same account. For example, the MDSYS account is present in Oracle Application Server, Oracle Database, and Oracle E-Business Suite. Unless otherwise instructed in Chapter 4, follow the instructions for the highest level application and then "go down the stack" if no advice was given at the higher level. For example, if your database is an Oracle E-Business Suite database, you would be using the Oracle database, the Application Server, and E-Business Suite. In this case, you would look for the product's security solution in the following order:

   1. Secure the open accounts according to the Oracle E-Business Suite instructions.
   2. For any remaining, open accounts, secure according to the Oracle Application Server instructions.
   3. For any remaining, open accounts, secure according to the Oracle Database instructions.

3

List of Default Database Accounts

Table 3–1 lists in alphabetical order the accounts that Oracle Default Password Scanner checks and the products use these accounts. After you find the products that are using the accounts listed in your report, you can implement the security solution in Chapter 4 for that product.

Table 3–1 Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
AASH					X	
ABA1					X	
ABM			X			
AD_MONITOR			X			
ADAMS	X					
ADS			d			
ADSEUL_US			d			
AHL			X			
AHM			X			
AK			X			
AL					X	
ALA1					X	
ALLUSERS					X	
ALR			X			
AMA1					X	
AMA2					X	
AMA3					X	
AMA4					X	
AMF			X			
AMS			X			
AMS1					X	
AMS2					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
AMS3					X	
AMS4					X	
AMSYS					X	
AMV			X			
AMW			X			
ANNE					X	
ANONYMOUS		X				
AOLDEMO			d			
AP			X			
APA1					X	
APA2					X	
APA3					X	
APA4					X	
APPLEAD						X
APPLSYS			X			
APPLSYSPUB			X			
APPS			X			
APS1					X	
APS2					X	
APS3					X	
APS4					X	
AQDEMO	X					
AQJAVA	X					
AQUSER	X					
AR			X			
ARA1					X	
ARA2					X	
ARA3					X	
ARA4					X	
ARS1					X	
ARS2					X	
ARS3					X	
ARS4					X	
ART					X	
ASF			X			
ASG			X			
ASL			X			

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
ASN			X			
ASO			X			
ASP			X			
AST			X			
AUC_GUEST					X	
AURORAJISUTILITY$	X					
AURORAORBUNAUTHENTICATE	X					
AURORAORBUNAUTHENTICATED	X					
AUTHORIA	X		d			
AX			X			
AZ			X			
B2B		X				
BAM		X				
BCA1					X	
BCA2					X	
BEN			X			
BI	X					
BIL			X			
BIM			X			
BIS			X			
BIV			X			
BIX			X			
BLAKE	X					
BMEADOWS					X	
BNE			X			
BOM			X			
BP01					X	
BP02					X	
BP03					X	
BP04					X	
BP05					X	
BP06					X	
BSC			X			
BUYACCT					X	
BUYAPPR1					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
BUYAPPR2					X	
BUYAPPR3					X	
BUYER					X	
BUYMTCH					X	
CAMRON					X	
CANDICE					X	
CARL					X	
CARLY					X	
CARMEN					X	
CARRIECONYERS					X	
CATADMIN					X	
CE			X			
CEASAR					X	
CENTRA						
CFD			d			
CHANDRA					X	
CHARLEY					X	
CHRISBAKER					X	
CHRISTIE					X	
CINDY					X	
CLARK	X				X	
CLAUDE					X	
CLINT					X	
CLN			X			
CN			X			
CNCADMIN						X
CONNIE					X	
CONNOR					X	
CORY					X	
CRM1					X	
CRM2					X	
CRP			X			
CRPB733						X
CRPCTL						X
CRPDTA						X
CS			X			
CSADMIN					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
CSAPPR1					X	
CSC			X			
CSD			X			
CSDUMMY			d			
CSE			X			
CSF			X			
CSI			X			
CSL			X			
CSM			X			
CSMIG			d			
CSP			X			
CSR			X			
CSS			X			
CTXDEMO	X					
CTXSYS	X		X			
CTXTEST			d			
CUA			X			
CUE			X			
CUF			X			
CUG			X			
CUI			X			
CUN			X			
CUP			X			
CUS			X			
CZ			X			
DAVIDMORGAN					X	
DBSNMP	X		X	X		
DCM		X				
DD7333						X
DD7334						X
DD810						X
DD811						X
DD812						X
DD9						X
DDB733						X
DDD			X			
DES		X				

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
DES2K		X				
DEV2000_DEMOS		X				
DEVB733						X
DEVUSER						X
DGRAY			d			
DIP		X				
DISCOVERER5		X				
DKING					X	
DLD			d			
DMADMIN	X					
DMATS					X	
DMS			d			
DMSYS	X	X				
DOM			X			
DPOND					X	
DSGATEWAY		X				
DV7333						X
DV7334						X
DV810						X
DV811						X
DV812						X
DV9						X
DVP1					X	
EAA			X			
EAM			X			
EC			X			
ECX			X			
EDR			X			
EDWEUL_US			d			
EDWREP			d			
EGC1					X	
EGD1					X	
EGM1					X	
EGO			X			
EGR1					X	
END1					X	
ENG			X			

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
ENI			X			
ENM1					X	
ENS1					X	
ENTMGR_CUST					X	
ENTMGR_PRO					X	
ENTMGR_TRAIN					X	
EOPP_PORTALADM					X	
EOPP_PORTALMGR					X	
EOPP_USER					X	
EUL_US			d			
EVM			X			
EXA1					X	
EXA2					X	
EXA3					X	
EXA4					X	
EXFSYS	X	X				
EXS1					X	
EXS2					X	
EXS3					X	
EXS4					X	
FA			X			
FEM			X			
FIA1					X	
FII			X			
FNI1					X	
FNI2					X	
FLM			X			
FNI1					X	
FNI2					X	
FPA			X			
FPT			X			
FRM			X			
FTA1					X	
FTE			X			
FUN			X			
FV			X			
FV1					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
GALLEN					X	
GCA1					X	
GCA2					X	
GCA3					X	
GCA9					X	
GCMGR1					X	
GCMGR2					X	
GCMGR3					X	
GCS			X			
GCS1					X	
GCS2					X	
GCS3					X	
GEORGIAWINE					X	
GL			X			
GLA1					X	
GLA2					X	
GLA3					X	
GLA4					X	
GLS1					X	
GLS2					X	
GLS3					X	
GLS4					X	
GMA			X			
GMD			X			
GME			X			
GMF			X			
GMI			X			
GML			X			
GMP			X			
GMS			X			
GM_AWDA					X	
GM_COMH					X	
GM_COPI					X	
GM_DPHD					X	
GM_MLCT					X	
GM_PLADMA					X	
GM_PLADMH					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
GM_PLCCA					X	
GM_PLCCH					X	
GM_PLCOMA					X	
GM_PLCONA					X	
GM_PLADMA					X	
GM_PLCONH					X	
GM_PLNSCA					X	
GM_PLNSCH					X	
GM_PLCOMA					X	
GM_PLSCTA					X	
GM_PLVET					X	
GM_SPO					X	
GR			X			
GUEST					X	
HCC			d			
HHCFO					X	
HR	X		X			
HRI			X			
HXC			X			
HXT			X			
IA			X			
IBA			X			
IBC			X			
IBE			X			
IBP			X			
IBU			X			
IBY			X			
ICX			X			
IEB			X			
IEC			X			
IEM			X			
IEO			X			
IES			X			
IEU			X			
IEX			X			
IGC			X			
IGF			X			

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
IGI			X			
IGS			X			
IGW			X			
IMC			X			
IMT			X			
INS1					X	
INS2					X	
INTERNET_ APPSERVER_REGISTRY		X				
INV			X			
IP		X				
IPA			X			
IPD			X			
ISC			X			
ISTEWARD					X	
ITG			X			
IX	X					
JA			X			
JD7333						X
JD7334						X
JD9						X
JDE						X
JDEDBA						X
JE			X			
JG			X			
JL			X			
JOHNINARI					X	
JONES	X					
JTF			X			
JTI			d			
JTM			X			
JTR			d			
JTS			X			
JUNK_PS			X			
JUSTOSHUM					X	
KELLYJONES					X	
KEVINDONS					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
KPN					X	
LADAMS					X	
LBA					X	
LBACSYS	X					
LDQUAL					X	
LHILL					X	
LNS			X			
LQUINCY					X	
LSA					X	
MDDATA		X				
MDSYS	X	X	X			
ME			X			
MFG			X			
MGR1					X	
MGR2					X	
MGR3					X	
MGR4					X	
MIKEIKEGAMI					X	
MJONES					X	
MLAKE					X	
MM1					X	
MM2					X	
MM3					X	
MM4					X	
MM5					X	
MMARTIN					X	
MOBILEADMIN			d			
MRP			X			
MSC			X			
MSD			X			
MSO			X			
MSR			X			
MST			X			
MWA			X			
NEILKATSU					X	
OBJ7333						X
OBJ7334						X

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
OBJB733						X
OCA		X				
ODM	X		X			
ODM_MTR	X		X			
ODS		X				
ODSCOMMON		X				
OE	X		X			
OKB			X			
OKC			X			
OKE			X			
OKI			X			
OKL			X			
OKO			X			
OKR			X			
OKS			X			
OKX			X			
OL810						X
OL811						X
OL812						X
OL9						X
OLAPSYS	X	X				
ONT			X			
OPI			X			
ORABAM		X				
ORABAMSAMPLES		X				
ORABPEL		X				
ORAESB		X				
ORAOCA_PUBLIC		X				
ORASAGENT		X				
ORASSO		X				
ORASSO_DS		X				
ORASSO_PA		X				
ORASSO_PS		X				
ORASSO_PUBLIC		X				
ORDPLUGINS	X		X			
ORDSYS	X		X			
OSM			X			

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
OTA			X			
OUTLN	X	X	X			
OWAPUB			X			
OWF_MGR		X				
OZF			X			
OZP			X			
OZS			X			
PA			X			
PABLO					X	
PAIGE					X	
PAM					X	
PARRISH					X	
PARSON					X	
PAT					X	
PATORILY					X	
PATRICKSANCHEZ					X	
PATSY					X	
PAUL					X	
PAULA					X	
PAXTON					X	
PCA1					X	
PCA2					X	
PCA3					X	
PCA4					X	
PCS1					X	
PCS2					X	
PCS3					X	
PCS4					X	
PD7333						X
PD7334						X
PD810						X
PD811						X
PD812						X
PD9						X
PDA1					X	
PEARL					X	
PEG					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
PENNY					X	
PEOPLE					X	
PERCY					X	
PERRY					X	
PETE					X	
PEYTON					X	
PHIL					X	
PJI			X			
PJM			X			
PMI	X		X			
PN			X			
PO			X			
POA			X			
POLLY					X	
POM			X			
PON			X			
PORTAL		X				
PORTAL_APP		X				
PORTAL_DEMO		X				
PORTAL_PUBLIC		X				
PORTAL30		X	X			
PORTAL30_DEMO		X	X			
PORTAL30_PUBLIC		X	X			
PORTAL30_SSO		X	X			
PORTAL30_SSO_PS		X	X			
PORTAL30_SSO_ PUBLIC		X	X			
POS			X			
PPM1					X	
PPM2					X	
PPM3					X	
PPM4					X	
PPM5					X	
PRISTB733						X
PRISTCTL						X
PRISTDTA						X
PRODB733						X

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
PRODCTL						X
PRODDTA						X
PRODUSER						X
PROJMFG			d			
PRP			X			
PS					X	
PS810						X
PS810CTL						X
PS810DTA						X
PS811						X
PS811CTL						X
PS811DTA						X
PS812						X
PS812CTL						X
PS812DTA						X
PSA			X			
PSB			X			
PSBASS					X	
PSEM					X	
PSFT						X
PSFTDBA						X
PSP			X			
PTADMIN					X	
PTCNE					X	
PTDMO					X	
PTE			d			
PTESP					X	
PTFRA					X	
PTG			d			
PTGER					X	
PTJPN					X	
PTUKE					X	
PTUPG					X	
PTWEB					X	
PTWEBSERVER					X	
PV			X			
PY7333						X

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
PY7334						X
PY810						X
PY811						X
PY812						X
PY9						X
QA			X			
QOT			X			
QP			X			
QRM			X			
QS	X					
QS_ADM	X					
QS_CB	X					
QS_CBADM	X					
QS_CS	X					
QS_ES	X					
QS_OS	X					
QS_WS	X					
RENE					X	
REPADMIN	X		d			
REPORTS		X				
REPORTS_USER		X				
RESTRICTED_US			d			
RG			X			
RHX			X			
RLA			X			
RLM			X			
RM1					X	
RM2					X	
RM3					X	
RM4					X	
RM5					X	
RMAN	X					
ROB					X	
RPARKER					X	
RWA1					X	
SALLYH					X	
SAM					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
SARAHMANDY					X	
SCM1					X	
SCM2					X	
SCM3					X	
SCM4					X	
SCOTT	X	X	X			
SDAVIS					X	
SECDEMO						
SEDWARDS					X	
SELLCM					X	
SELLER					X	
SELLTREAS					X	
SERVICES			d			
SETUP					X	
SH	X					
SI_INFORMTN_SCHEMA		X				
SID					X	
SKAYE					X	
SKYTETSUKA					X	
SLSAA					X	
SLSMGR					X	
SLSAA					X	
SLSMGR					X	
SLSREP					X	
SRABBITT					X	
SRALPHS					X	
SRAY					X	
SRIVERS					X	
SSA1					X	
SSA2					X	
SSA3					X	
SSC1					X	
SSC2					X	
SSC3					X	
SSOSDK			X			
SSP			X			
SSS1					X	

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
SUPPLIER					X	
SVM7333						X
SVM7334						X
SVM810						X
SVM811						X
SVM812						X
SVM9						X
SVMB733						X
SVP1					X	
SY810						X
SY811						X
SY812						X
SY9						X
SYS	X		X			
SYS7333						X
SYS7334						X
SYSADMIN						X
SYSB733						X
SYSMAN				X		
SYSTEM	X		X			
TDEMARCO					X	
TDOS_ICSAP						
TESTCTL						X
TESTDTA						X
TRA1					X	
TRACESVR			d	X		
TRBM1					X	
TRCM1					X	
TRDM1					X	
TRRM1					X	
TWILLIAMS					X	
UDDISYS		X				
VEA			X			
VEH			X			
VIDEO31		X				
VIDEO4		X				
VIDEO5		X				

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
VP1					X	
VP2					X	
VP3					X	
VP4					X	
VP5					X	
VP6					X	
WAA1					X	
WAA2					X	
WCRSYS		X				
WEBDB	X					
WEBSYS			d			
WEBDB						
WEBSYS						
WENDYCHO					X	
WH			d			
WIP			X			
WIRELESS		X	d			
WK_TEST		X				
WKPROXY		X				
WKSYS		X				
WMS			X			
WMSYS	X	X				
WPS			X			
WSH			X			
WSM			X			
XDB	X	X				
XDO			X			
XDP			X			
XLA			X			
XLE			X			
XNB			X			
XNC			X			
XNI			X			
XNM			X			
XNP			X			
XNS			X			
XTR			X			

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

Table 3–1 (Cont.) Default Accounts Oracle Default Password Scanner Checks

Account	Oracle Database	Oracle Application Server	Oracle E-Business Suite (See Legend 1)	Oracle Enterprise Manager	PeopleSoft (See Legend 2)	JD Edwards (See Legend 3)
YCAMPOS					X	
YSANCHEZ					X	
ZFA			X			
ZPB			X			
ZSA			X			
ZX			X			

1. For Oracle E-Business Suite, accounts that are only present in the demo databases are indicated with a "d".
2. For a list of accounts across different releases of PeopleSoft products, see "List of PeopleSoft Default Accounts Per Release" on page 4-18.
3. For a list of common and unique accounts across different releases of JD Edwards products, see "List of JD Edwards Database Accounts Per Release" on page 4-22.

4

Security Solutions for Oracle Default Database Accounts

In Chapter 2, you generated a report listing Oracle default accounts that you need to secure. In Chapter 3, you checked Table 3–1 for the products that use the accounts in your report. Use the instructions in this chapter to secure those accounts, based on the products in which the accounts are used.

This chapter covers the following topics:

Securing Oracle Database Default Accounts

If your Oracle database is not used by any of the other Oracle products described in this guide (Oracle Application Server, Oracle E-Business Suite Application, PeopleSoft, and so on), then log into the database with administrative privileges and lock the account. For example:

```
$ sqlplus username
Enter password: password
SQL> ALTER USER ACCOUNT ACCOUNT LOCK;
```

However, if the Oracle database is used by the other Oracle products covered in this guide, then follow the instructions described in this chapter to secure the account for each of these products.

For Oracle Database default accounts that are used by customized or third-party products that may depend on the Oracle Database default accounts, refer to the product's documentation for information on securing the products.

Securing Oracle Application Server Default Accounts

Depending on the Oracle Application Server default account, you either need to lock the account, or you need to change the account's password.

This section covers the following topics:

Oracle Application Server Accounts That Need to be Locked and Expired

In order for Oracle Application Server to function correctly, the following accounts are created in Oracle Database and registered with Oracle Internet Directory Server with a random password. However, if you had created the accounts with a default password, the creation process locks and expires the accounts but does not register the account with Oracle Internet Directory Server. If Oracle Default Password Scanner finds any of the accounts in this list, then it means that someone has unlocked the account. As a result, Oracle Application Server cannot use the account. In this case, you need to lock the account again.

Oracle Application Server default accounts that you need to lock and expire are as follows:

ANONYMOUS	MDSYS	PORTAL
B2B	OCA	PORTAL_APP
CTXSYS	ODS	PORTAL_DEMO
DCM	OLAPSYS	PORTAL_PUBLIC
DES	ORAOCA_PUBLIC	SCOTT
DES2K	ORASSO	SI_INFORMTN_SCHEMA
DIP	ORASSO_DS	UDDISYS
DISCOVERER5	ORASSO_PA	WCRSYS
DMSYS	ORASSO_PS	WIRELESS
DSGATEWAY	ORASSO_PUBLIC	WKPROXY
EXFSYS	ORDPLUGINS	WKSYS
INTERNET_APPSERVER_REGISTRY	ORDSYS	WK_TEST
IP	OUTLN	WMSYS
MDDATA	OWF_MGR	XDB

If Oracle Default Password Scanner lists these accounts as `OPEN`, then lock them and expire the password using administrative privileges in SQL*Plus. For example

```
$ sqlplus username
Enter password: password
SQL> ALTER USER ACCOUNT PASSWORD EXPIRE ACCOUNT LOCK;
```

Oracle Application Server Accounts That Need Their Passwords Changed

If the following Oracle Application Server default accounts are listed as OPEN, then you need to change their passwords:

BAM	PORTAL30	REPORTS
DEV2000_DEMOS	PORTAL30_DEMO	REPORTS_USER
ORABPEL	PORTAL30_PUBLIC	VIDEO31
ORABAM	PORTAL30_SSO	VIDEO4
ORASAGENT	PORTAL30_SSO_PS	VIDEO5
ORABAMSAMPLES	PORTAL30_SSO_PUBLIC	

Changing the Integration Product Passwords

The accounts used in the Integration Products are:

BAM	ORABAM	ORABAMSAMPLES
ORABPEL	ORASAGENT	

Changing the BAM Account Password

Log into SQL*Plus with database administrative privileges and change the BAM password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD BAM;
Changing password for BAM
New password: new_password
Retype new password: new_password
```

Changing the ORABPEL Account Password

For a standalone installation of Oracle Business Process Execution Language (BPEL), follow these steps:

1. Log into SQL*Plus with database administrative privileges and change the ORABPEL password:

   ```
   $ sqlplus username
   Enter password: password
   SQL> PASSWORD ORABPEL;
   Changing password for ORABPEL
   New password: new_password
   Retype new password: new_password
   ```

2. In the Data-Sources.xml file, search for password and replace its setting with the password that you created in Step 1.

   By default, Data-Sources.xml is located in *ORACLE_HOME*/integration/orabpel/system/appserver/oc4j/j2ee/home/config.

3. Restart BPEL Server.

For a mid-tier installation of BPEL, follow these steps:

1. Stop the mid-tier BPEL Server.

2. Log into SQL*Plus with database administrative privileges and change the ORABPEL password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD ORABPEL;
Changing password for ORABPEL
New password: new_password
Retype new password: new_password
```

3. In the jazn-data.xml file, search for the credentials-clear setting enter the password that you created in Step 2.

   In the following example, xyzABCD is the password you would change:

```
<user>
<name>pwForOrabpel</name>
<credentials clear="true">xyzABCD</credentials>
</user>
```

   By default, jazn-data.xml is located in ORACLE_HOME/j2ee/OC4J_BPEL/config.

4. Restart the mid-tier BPEL Server.

   Oracle Containers for J2EE (OC4J) reads the jazn-data.xml file and then rewrites it with obfuscated (encrypted) versions of the password. For more information password obfuscation in the jazn-data.xml file, refer to *Oracle Application Server Containers for J2EE Security Guide*.

For Oracle Identity Management-based installations of BPEL, you do not need to change the passwords. In this type of BPEL installation, all passwords are randomized.

Changing the ORABAM Account Password

Follow these steps:

1. Log into SQL*Plus with database administrative privileges and change the ORABAM password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD ORABAM;
Changing password for ORABAM
New password: new_password
Retype new password: new_password
```

2. At a Windows command prompt, enter pwencrypt to start Password Encryption utility, and then do the following:

   a. In the Password Encryption dialog box, enter the following settings:

      User name: ORABAM

      Password and Confirm password: Enter the same password as you created in Step 1.

      Data source: oraclebam

      Select Oracle database credentials: Enable this button.

   b. Click the **Encrypt** button.

   c. When prompted, click **Save to .config file**.

d. Save each of the following files to the BAM directory, overwriting the original version of each file.

```
adcVersionChecker.exe.config

CacheInit.exe.config

ICommand.exe.config

morpheus.exe.config

OracleBAMActiveDataCache.exe.config
```

e. Click **Exit**.

3. Restart the BAM services.

Changing the ORASAGENT Account Password

Follow these steps:

1. Log into SQL*Plus with database administrative privileges and change the ORASAGENT password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD ORASAGENT;
Changing password for ORASAGENT
New password: new_password
Retype new password: new_password
```

2. Start Oracle BAM Enterprise Link Design Studio and do the following:
   a. Click the **Advanced** button.
   b. On the right side, under the Repository section, enter the new password you created in Step 1.
   c. At the bottom, select the **Save these Data Flow Service and Repository settings as my default login settings** checkbox.
   d. Click **OK** to log into the repository. Subsequent logins will retain the new database password.
3. Restart BPEL Server.

Changing the ORABAMSAMPLES Account Password

Log into SQL*Plus with database administrative privileges and change the ORABAMSAMPLES password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD ORABAMSAMPLES;
Changing password for ORABAMSAMPLES
New password: new_password
Retype new password: new_password
```

Changing the DEV2000_DEMOS Password

Log into SQL*Plus with database administrative privileges and change the DEV2000_DEMOS password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD DEV2000_DEMOS;
```

```
Changing password for DEV2000_DEMOS
New password: new_password
Retype new password: new_password
```

Changing the PORTAL30 and PORTAL30_SSO Passwords

The following sections explain how to change the PORTAL30 and PORTAL30_SSO passwords for Oracle9*i*AS Release 1 and Oracle 9*i*AS Release 2 and later.

Changing the PORTAL30 and PORTAL30_SSO Passwords for Oracle9*i*AS Release 1

Follow these steps:

1. Log onto SQL*Plus with database administrative privileges and then change the PORTAL30 and PORTAL30_SSO passwords.

   ```
   $ sqlplus username
   Enter password: password
   SQL> PASSWORD PORTAL30
   Changing password for PORTAL30
   New password: new_password
   Retype new password: new_password
   SQL> PASSWORD PORTAL30_SSO
   Changing password for PORTAL30_SSO
   New password: new_password
   Retype new password: new_password
   ```

2. Update the corresponding modplsql Database Access Descriptor (DAD) for Oracle9*i*AS Release 1, called wdbsvr.app, which is used to access these schemas.

   In a default installation, wdbsvr.app is located in *ORACLE_HOME*/Apache/modplsql/cfg. In this file, search for the following lines:

   ```
   password =
   username =
   ```

   The username setting will be either PORTAL30 or PORTAL30_SSO. Change its corresponding password setting to the password you set in Step 1.

3. Restart Apache.

   - On Windows:

     ```
     SYSTEM_DRIVE:\> ORACLE_HOME_9\Apache\Apache\apache -k shutdown
     SYSTEM_DRIVE:\> ORACLE_HOME_9\Apache\Apache\apache -k startup
     ```

   - On UNIX:

     ```
     $ ORACLE_HOME_9/Apache/Apache/bin/apachectl stop
     $ ORACLE_HOME_9/Apache/Apache/bin/apachectl start
     ```

Changing the PORTAL30 and PORTAL30_SSO Passwords for Oracle9*i*AS Release 2 and Later

Follow these steps:

1. Log onto SQL*Plus with database administrative privileges and then change the PORTAL30 and PORTAL30_SSO passwords.

   ```
   $ sqlplus username
   Enter password: password
   SQL> PASSWORD PORTAL30
   Changing password for PORTAL30
   ```

```
New password: new_password
Retype new password: new_password
SQL> PASSWORD PORTAL30_SSO
Changing password for PORTAL30_SSO
New password: new_password
Retype new password: new_password
```

2. Update the corresponding `modplsql` Database Access Descriptor (DAD) for Oracle9*i*AS Release 2 (and later), called `dads.conf`, which is used to access these schemas.

   In a default installation, `dads.conf` is located in *ORACLE_HOME*`/Apache/modplsql/conf`. In this file, search for the following lines:

   ```
   PlsqlDatabaseUsername <username>
   PlsqlDatabasePassword <password>
   ```

   The `username` setting will be either `PORTAL30` or `PORTAL30_SSO`. Change its corresponding `password` setting to the password you set in Step 1.

3. Update the `oradav.conf` file, which is located in *ORACLE_HOME*`/Apache/modplsql/conf`.

   Look for the following lines:

   ```
   DAVParam ORAUSER <username>
   DAVParam ORAPASSWORD <password>
   ```

   The `username` setting will be `PORTAL30` or `PORTAL30_SSO`. Change its corresponding `password` setting to the password you set in Step 1.

4. Restart Oracle HTTP Server.

   - On Windows:

     ```
     SYSTEM_DRIVE:\> ORACLE_HOME\dcm\bin\dcmctl stop -ct ohs
     SYSTEM_DRIVE:\> ORACLE_HOME\dcm\bin\dcmctl start -ct ohs
     ```

   - On UNIX:

     ```
     $ ORACLE_HOME/dcm/bin/dcmctl stop -ct ohs
     $ ORACLE_HOME/dcm/bin/dcmctl start -ct ohs
     ```

Changing the PORTAL30_DEMO–PORTAL30_SSO_PUBLIC Passwords

These accounts are:

```
PORTAL30_DEMO     PORTAL30_PUBLIC      PORTAL30_SSO_PUBLIC
```

Log onto SQL*Plus with database administrative privileges and then change the passwords as follows:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD ACCOUNT;
Changing password for ACCOUNT
New password: new_password
Retype new password: new_password
```

Changing the PORTAL30_SSO_PS Password

Follow these steps:

1. Log into SQL*Plus with database administrative privileges and then change the PORTAL30_SSO_PS password.

```
$ sqlplus username
Enter password: password
SQL> PASSWORD PORTAL30_SSO_PS;
Changing password for PORTAL30_SSO_PS
New password: new_password
Retype new password: new_password
```

2. If your login server is on a database instance that is separate from the portal instance, run the ssodatax script.

   The ssodatax script updates the Partner Application's enabler configuration table, WWSSO_PAPP_CONFIGURATION_INFO$. By default, ssodatax is located in *ORACLE_HOME*/portal30/admin/plsql, where *ORACLE_HOME* is where your Oracle Portal installation is located.

   The syntax for ssoddatax is:

```
ssodatax -i portal_site_id -t portal_site_token -k encryption_key -w portal_url
-l login_server_url -s portal_schema -p portal_password -v cookie_version -o
sso_schema -e pstore_schema -r pstore_password -b pstore_dblink -c connect_
string -n ps_connect_string
```

   For example:

```
ssodatax -i 1234 -t A1B2C3 -k X9Y8Z7 -w
http://webdbsvr.us.oracle.com:3000/pls/portal30/ -l
http://webdbsvr.us.oracle.com:3000/pls/portal30_sso/ -s portal30 -p portal30 -v
v1.1 -o portal30_sso -e portal30_sso_ps -r portal30_sso_ps -b portal30_dblink
-c orcl -n orcl01
```

Changing the REPORTS Password

Log into SQL*Plus with database administrative privileges and then change the REPORTS password.

```
$ sqlplus username
Enter password: password
SQL> PASSWORD REPORTS;
Changing password for REPORTS
New password: new_password
Retype new password: new_password
```

Changing the REPORTS_USER Password

Follow these steps:

1. Log into the Oracle Enterprise Manager Console.
2. From the **Configuration** menu, choose **Manage Administrators**.
3. In the Manage Administrators Accounts dialog box, select REPORTS_USER from the list.
4. Click the **Edit** button.
5. In the Edit Administrator Preferences property sheet, enter the new password in the **Password** field. Then retype the new password in the **Confirm Password** field.

Changing the VIDEO31, VIDEO4, and VIDEO5 Account Passwords

Log into SQL*Plus with database administrative privileges and change the passwords for VIDEO31, VIDEO4, and VIDEO5. For example:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD VIDEO31;
Changing password for VIDEO31
New password: new_password
Retype new password: new_password
```

Securing the ODSCOMMON Account

The ODSCOMMON account was used in Oracle Internet Directory Server releases 9.0.2 and earlier. Oracle no longer supports it. If you are still using one of these earlier releases, Oracle strongly recommends that you upgrade to the latest release.

Log into SQL*Plus with database administrative privileges and lock the ODSCOMMON account. Locking it will not affect newer releases of Oracle Internet Directory Server, but it may affect the earlier releases of Oracle Internet Directory Server.

```
$ sqlplus username
Enter password: password
SQL> ALTER USER ODSCOMMON ACCOUNT LOCK;
```

Securing Oracle E-Business Suite Application Default Accounts

This section covers the following topics:

Securing an Oracle E-Business Suite Database Instance

Oracle recommends that you secure an Oracle E-Business Suite database instance by following these steps:

1. Run Oracle Default Password Scanner to generate the report as described in "Running Oracle Default Password Scanner" on page 2-2.
2. Use FNDCPASS in ALLORACLE mode to change the password for all the base product schemas. Use the following syntax:

   ```
   $ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd ALLORACLE new_pwd
   ```

   This removes approximately 200 schema accounts from the report for a default installation.

   See "Securing the ABM–ZX Accounts" on page 4-11 for instructions.
3. Re-run Oracle Default Password Scanner.

   To secure the products listed in the new report, follow the instructions in this order:

   a. Specific instructions for Oracle E-Business Suite ("Securing Oracle E-Business Suite Application Default Accounts" on page 4-9). If none are given, use:

   b. Instructions for Oracle Application Server ("Securing Oracle Application Server Default Accounts" on page 4-2), or:

   c. Instructions for Oracle Database ("Securing Oracle Database Default Accounts" on page 4-1).

When you have completed this procedure, if you still have some accounts listed in the report, and if these are marked with a "d" in the Oracle E-Business Suite column in Table 3–1 on page 3-1, then your database may have been based on a Vision demo database. In this case, lock any remaining schemas listed in he report unless you know you use them.

Log into SQL*Plus with administrative privileges and enter the following commands:

```
$ sqlplus username
Enter password: password
SQL> ALTER USER ACCOUNT ACCOUNT LOCK;
```

Using FNDCPASS to Secure Oracle E-Business Suite Application Accounts

For Oracle E-Business Suite applications, Oracle recommends that you use the FNDCPASS utility to find and change database passwords, unless instructed differently in this guide. In addition to changing the password, this utility re-encrypts it.

You can download the latest version of FNDCPASS from Oracle*MetaLink* (`http://metalink.oracle.com/`) by selecting patch 5080487).

Securing the AD_MONITOR Account

`AD_MONITOR` is used by Oracle Applications Manager (OAM) to monitor patching progress. This schema is created locked and expired. You do not need to further secure this account.

Securing the ABM–ZX Accounts

These accounts, which belong to individual APPS base products, are:

ABM	BIM	CUA	FLM	IBA	IPD	OKE	POS	XDP
AHL	BIS	CUE	FPA	IBC	ISC	OKI	PRP	XLA
AHM	BIV	CUF	FPT	IBE	ITG	OKL	PSA	XLE
AK	BIX	CUG	FRM	IBP	JA	OKO	PSB	XNB
ALR	BNE	CUI	FTE	IBU	JE	OKR	PSP	XNC
AMF	BOM	CUN	FUN	IBY	JG	OKS	PV	XNI
AMS	BSC	CUP	FV	ICX	JL	OKX	QA	XNM
AMV	CCT	CUS	GCS	IEB	JTF	ONT	QOT	XNP
AMW	CE	CZ	GL	IEC	JTM	OPI	QP	XNS
AP	CLN	DDD	GMA	IEM	JTS	OSM	QRM	XTR
AR	CN	DOM	GMD	IEO	LNS	OTA	RG	ZFA
ASF	CRP	EAA	GME	IES	ME	OZF	RHX	ZPB
ASG	CS	EAM	GMF	IEU	MFG	OZP	RLA	ZSA
ASL	CSC	EC	GMI	IEX	MRP	OZS	RLM	ZX
ASN	CSD	ECX	GML	IGC	MSC	PA	SSP	VEH
ASO	CSE	EDR	GMP	IGF	MSD	PJI	VEA	
ASP	CSF	EGO	GMS	IGI	MSO	PJM	VEH	
AST	CSI	ENG	GR	IGS	MSR	PMI	WIP	
AX	CSL	ENI	HR	IGW	MST	PN	WMS	
AZ	CSM	EVM	HRI	IMC	MWA	PO	WPS	
BEN	CSP	FA	HXC	IMT	OE	POA	WSH	
BIC	CSR	FEM	HXT	INV	OKB	POM	WSM	
BIL	CSS	FII	IA	IPA	OKC	PON	XDO	

Changing the password for these schemas does not affect any configuration files.

You can secure all of these accounts by using a single invocation of FNDCPASS. Before running FNDCPASS, make sure that you have the most recent version that supports the ALLORACLE mode. "Using FNDCPASS to Secure Oracle E-Business Suite Application Accounts" on page 4-10 explains how to download FNDCPASS.

To secure all the accounts with a single invocation of FNDCPASS, use the following syntax:

```
$ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd ALLORACLE new_pwd
```

Note that FNDCPASS finds all registered base product schema accounts, including those added after the code freeze of Oracle Default Password Scanner (for example, the IZU schema).

Oracle recommends that you run FNDCPASS command in the ALLORACLE mode for the accounts listed in this section as your first step to secure an Oracle E-Business Suite database. Afterwards, re-run Oracle Default Password Scanner. Doing so provides a much shorter and more manageable list for your remaining work.

Securing the APPLSYSPUB Account

APPLSYSPUB has sufficient privileges to authenticate an Applications User (that is, an FND user), which includes running PL/SQL packages to verify the username/password combination and the privilege to record the success or failure of a login attempt.

You do not need to change the password for APPLSYSPUB. However, if you do change it, follow these steps:

Follow these steps:

1. Run FNDCPASS as follows:

   ```
   $ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd ORACLE APPLSYSPUB new_pwd
   ```

2. Run Autoconfig (or a manual procedure) to propagate the change to the following application tier configuration files:

   - *FND_TOP*/resource/appsweb.cfg
   - *OA_HTML*/bin/appsweb.cfg
   - *FND_TOP*/secure/*host_name_dbname*.dbc

   If you are using any Application Desktop Integration (ADI) Products other than WebADI, re-configure each client to know the new APPLSYSPUB password.

   See Oracle*MetaLink* note 277535.1 for recommended deployment of Client Server products.

3. Restart all application tier processes (Apaches).

Securing the APPLSYS, APPS, and APPS_mrc Accounts

APPLSYS contains shared APPS foundation objects. APPS_*mrc* is an optional, additional APPS schema for the (now obsolete) Multiple Reporting Currencies (MRC) feature. The default for APPS_*mrc* is APPS_MRC, but country code suffixes can be used, for example. APPS_UK, APPS_JP.

APPLSYS, APPS, and any additional APPS_mrc schema share the same password. APPS is the shared runtime schema for all E-Business Suite products. APPS_MRC is an obsolete account, although it may be used in older versions of E-Business Suite. FNDCPASS synchronizes the password across these schema: when you use FNDCPASS to change one of these accounts, all are changed. Use a long (12 or more characters), secure password for these schema.

To secure these accounts:

1. Run FNDCPASS on one of the three APPLSYS, APPS, and APPS_*mrc* accounts. For example:

   ```
   $ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd SYSTEM APPLSYS new_pwd
   ```

2. Run Autoconfig to propagate the changed passwords into the following application server configuration files:

   - *ORACLE_HOME*/reports60/server/CGIcmd.dat
   - *iAS_TOP*/Apache/modplsql/cfg/wdbsvr.app

3. Restart all application tier processes (for example, Apache, CCM, Report Server).

Securing the CTXSYS Account

For E-Business Suite 11.5.5 and earlier versions, you can lock the CTXSYS account. For example:

```
SQL> ALTER USER CTXSYS ACCOUNT LOCK;
```

For E-Business Suite 11.5.8, some patch scripts assume the password for CTXSYS is CTXSYS. When patching these versions, set the CTXSYS password to CTXSYS and then change it back to a secure password after you complete the patching.

E-Business Suite Maintenance Packs 11.5.9, 11.5.7, 11.5.6, 11.5.5, 11.5.4, 11.5.,3 and 11.5.2 provided file that resets the CTXSYS password to CTXSYS. This file is:

$ad_top/patch/115/sql/adgrnctx.sql (versions 115.11 and lower)

After applying a Maintenance Pack, use SQL*Plus to change the CTXSYS password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD CTXSYS
Changing password for CTXSYS
New password:
Retype new password:
```

Securing the DBSNMP Account

The DBSNMP account is not used by EBS. The DBSNMP account is typically used by monitoring software such as Oracle Enterprise Manager. If you are using Oracle Enterprise Manager, secure the account according to instructions in"Securing the Oracle Enterprise Manager Default DBSNMP Account" on page 4-15.

If you are not using Oracle Enterprise Manager (or any other third party monitoring tool using this schema account) you may lock this account. Log on to SQL*Plus with administrative privileges and lock the DBSNMP account as follows:

```
$ sqlplus username
Enter password: password
SQL> ALTER USER DBSNMP ACCOUNT LOCK;
```

Securing the EDWREP Account

To secure EDWREP, use FNDCPASS to change the password as follows:

```
$ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd ORACLE EDWREP new_pwd
```

Securing the JUNK_PS–SYSTEM Accounts

These accounts are:

JUNK_PS	ORDPLUGINS	SYS
MDSYS	ORDSYS	SYSTEM
ODM_MTR	OUTLN	
OLAPSYS	OWAPUB	

To secure these accounts, log on to SQL*Plus with administrative privileges and change the password:

```
$ sqlplus username
Enter password: password
```

```
SQL> PASSWORD ACCOUNT
Changing password for ACCOUNT
New password: new_password
Retype new password: new_password
```

Securing the ODM Account

ODM is used for the Oracle Data Manager.

Use FNDCPASS to change the password as follows:

```
$ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd ORACLE ODM new_pwd
```

Securing the PORTAL30*x* Accounts

These accounts are used for Oracle Portal 3.0.9 and Portal (3.0.9) Single Sign On.

If you are not using Oracle Login Server and Portal 3.0.9 with E-Business Suite 11*i* as documented in Oracle*MetaLink* Note 146469.1, then log into SQL*Plus with administrative privileges and lock these schema:

```
$ sqlplus username
Enter password: password
SQL> ALTER USER PORTAL30 ACCOUNT LOCK;
SQL> ALTER USER PORTAL30_SSO ACCOUNT LOCK;
SQL> ALTER USER PORTAL30_DEMO ACCOUNT LOCK;
SQL> ALTER USER PORTAL30_PUBLIC ACCOUNT LOCK;
SQL> ALTER USER PORTAL30_SSO_PS ACCOUNT LOCK;
SQL> ALTER USER PORTAL30_SSO_PUBLIC ACCOUNT LOCK;
```

Alternatively, if you are not using any PORTAL30 integration, you may remove the PORTAL30*x* schemas by following instructions in Oracle*MetaLink* Note 312349.1 "Remove Oracle Portal 3.0.9 from E-Business Suite 11*i*."

If you are using Oracle Login Server and Portal 3.0.9 with E-Business Suite 11*i* as documented in Oracle*MetaLink* Note 146469.1, you must use FNDCPASS to change the PORTAL30 and PORTAL30_SSO passwords:

```
$ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd PORTAL30 ORACLE new_pwd
$ FNDCPASS APPS/apps_pwd 0 Y SYSTEM/system_pwd PORTAL30_SSO ORACLE new_pwd
```

For the PORTAL30_PUBLIC, PORTAL30_SSO_PS, PORTAL30_SSO_PUBLIC accounts, log into SQL*Plus with administrative privileges and then change their passwords:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD PORTAL30_ACCOUNT;
Changing password for PORTAL30_ACCOUNT
New password: new_password
Retype new password: new_password
```

Lock the PORTAL30_DEMO schema, because it is not needed:

```
SQL> ALTER USER PORTAL30_DEMO ACCOUNT LOCK;
```

Afterward you change the PORTAL30 and PORTAL30_SSO passwords, run AutoConfig as documented in Oracle*MetaLink* Note 165195.1 "Using AutoConfig to Manage System Configurations with Oracle Applications 11*i*." For more information, refer to ATG Oracle*MetaLink* note 146469.1, which describes the Portal 3.0.9 installation.

Securing the SCOTT Account

To secure the SCOTT account, log on to SQL*Plus with administrative privileges and change the password:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD SCOTT
Changing password for SCOTT
New password: new_password
Retype new password: new_password
```

Securing the SSOSDK Account

To secure the SSOSDK account, log on to SQL*Plus with administrative privileges and lock the account:

```
$ sqlplus username
Enter password: password
SQL> ALTER USER SSOSDK ACCOUNT LOCK;
```

Securing Other Default Accounts

When you install Oracle E-Business Suite, including using the RapidInstall database, the default accounts from Oracle Database are also installed. To secure these accounts, see "Securing Oracle Database Default Accounts" on page 4-1 for instructions.

Securing the Oracle Enterprise Manager Default DBSNMP Account

The following products use the Oracle Enterprise Manager default account, which is DBSNMP:

- Oracle Enterprise Manager Intelligent Agent (release 9.2)
- Oracle Enterprise Manager Database Control (releases 10.1–10.2)
- Oracle Enterprise Manager Grid Control (releases 10.1–10.2)

This section covers the following topics:

Securing DBSNMP in Oracle Enterprise Manager Intelligent Agent (Release 9.2)

To secure the DBSNMP password for Oracle Enterprise Manager Intelligent Agent (release 9.2):

First, change the password at the database level by using Enterprise Manager Console:

1. Use administrative privileges to connect database in Enterprise Manager Console.
2. Expand the database item from the top tree.
3. Expand **Security** item, and then expand **Users** to list all accounts in this database.
4. Click **DBSNMP** from the tree.

   The General tab should display on the right side of the window.

5. Enter the new password in **Enter Password** and **Confirm Password** fields.
6. In the General tab, click **Apply**.

Next, modify the following line for the `snmp.connect.`*`service_name`*`.password` property in the `snmp_rw.ora` file:

1. Open the `snmp_rw.ora` file in a text editor.

   By default, this file is located in the *`ORACLE_HOME`*`/network/admin` directory.
2. Add the following line (if it does not already exist):

   ```
   snmp.connect.service_name.password=password
   ```
3. Replace *`service_name`* with the name of the database instance and *`password`* with the password used for `DBSNMP`.
4. From `$ORACLE_HOME/bin`, reststart Oracle Enterprise Manager Intelligent Agent:

   ```
   $ oemctl stop agent
   $ oemctl start agent
   ```

Securing DBSNMP in Oracle Enterprise Manager Database Control (Releases 10.1–10.2)

You do not need to modify `DBSNMP` for these releases because the password is changed at installation time.

Securing DBSNMP in Oracle Enterprise Manager Grid Control (Releases 10.1–10.2)

First, change the `DBSNMP` password in SQL*Plus:

```
$ sqlplus username
Enter password: password
SQL> PASSWORD DBSNMP;
Changing password for DBSNMP
New password: new_password
Retype new password: new_password
```

Next, follow these steps to complete securing `DBSNMP`:

1. Click the **Targets** tab in the Grid Control Console.
2. Click the **Database** subtab to list the database targets you are monitoring.
3. Select the database and click **Configure**. The Configure Database: Properties page appears.
4. Enter the new password for the `DBSNMP` account in the **Monitor Password** field.
5. Click **Test Connection** to confirm that the monitoring credentials are correct.

   This confirms the connection to the database from Oracle Management Server but not to the agent.
6. In the Configure Database Instance: Properties page, to change the password in Oracle Enterprise Manager Intelligent Agent, click the **Change DBSNMP Password** button.

   (If the **Change DBSNMP Password** button does not appear, click **Cancel** to exit the wizard, and then click **Configure** to display the Configure Database: Properties page.)

   The Properties page appears.

7. In the **Username** and **Password** fields, enter the Oracle Management Server super user's credentials.
8. In the **New DBSNMP Password** and **Confirm New DBSNMP Password** fields, enter the new `DBSNMP` password.
9. Click **OK**.

   The following message appears:

```
Success
The DBSNMP passsword has been successfully changed for both the database and
the agent. This new password has also been set below as the Monitor Password.
The DBSNMP user is unlocked in the database. You may now proceed with any
additional configuration. Otherwise, to exit the wizard, click Cancel
```

For more information on user-configurable parameters, see *Oracle Intelligent Agent User's Guide*.

Securing Oracle Collaboration Suite Default Accounts

Oracle Collaboration Suite does not create additional default accounts. However, Oracle Collaboration Suite uses other Oracle products, such as Oracle Database and Oracle Application Server, which may use default accounts. For instructions on how to secure open default accounts, refer to the instructions for those specific products.

Securing PeopleSoft Default Accounts

This section covers the following topics:

Securing PeopleSoft 8.x and Later Releases

Starting in PeopleSoft 8, and in all subsequent releases, PeopleTools requires only the following account types:

- **Connect ID:** Has read-only access to a handful of PeopleTools tables and is used during certain authentication processes
- **Access ID:** Has full access to all PeopleSoft tables

In earlier PeopleSoft releases, individual User IDs (formerly known as Operator IDs) could also have a corresponding database user account. The upgrade process from one release of PeopleSoft to the next should have removed these earlier accounts. However, if Oracle Default Password Scanner finds any database user accounts from these earlier releases, you should remove the older accounts.

It is important to choose a strong password for your Connect ID. If Oracle Default Password Scanner detects that you are using the default Connect ID and Password ("people/peop1e"), change it immediately. Keep in mind that this ID and password is stored in multiple locations. For 2-tier users, it is specified in Configuration Manager and stored in an encrypted format in the Windows Registry. It is also specified in the PSADMIN utility and stored, optionally encrypted, in the application server and Process Scheduler configuration files.

For PeopleSoft installations on the Oracle database platform, there is no default Access ID. The Access ID and Password are user-specified during the installation process. Even though there is no default Access ID or Password, you should still verify that you are using a strong password for your Access ID.

For more information on Configuration Manager and the PSADMIN utility, refer to PeopleBooks.

Securing Releases Earlier Than PeopleSoft 8

In releases prior to PeopleSoft 8, individual Operator Ids could have a corresponding database user account. PeopleSoft applications were also shipped with several default Operator IIs with matching passwords.

If Oracle Default Password Scanner detects any default Operator IDs and passwords, use one of the following methods to secure the PeopleSoft release:

- **If the Operator ID is not being used:** Delete the account by using the Security Administrator tool. Verify that the PeopleSoft Operator ID has been deleted, along with the corresponding database user account.
- **If the Operator ID is being used:** Change the password by using the Security Administrator tool. Choose a strong password that cannot be easily guessed.

For more information on the Security Administrator tool, refer to PeopleBooks.

List of PeopleSoft Default Accounts Per Release

This section lists the default database accounts that are used in PeopleSoft products. After you run Oracle Default Password Scanner, refer to this list for the accounts the scanner's report lists as `OPEN`.

Accounts from the PeopleTools 7.5 Demo Database

INS1	PTCNE	PTJPN
INS2	PTDMO	PTUKE
MGR1	PTESP	PTUPG
PS	PTFRA	PTWEB
PTADMIN	PTGER	VP1

Account from PeopleTools 8.x and Later

PEOPLE

Accounts That Are Used in the EPM Database

AASH	EOPP_USER	LDQUAL	SEDWARDS
ABA1	FIA1	LQUINCY	SETUP
ALA1	FNI1	MMARTIN	SKAYE
ALLUSERS	FNI2	PPM1	SLSAA
BCA1	FTA1	PPM2	SLSMGR
BCA2	GCA1	PPM3	SLSREP

BP01	GCA2	PPM4	SRABBITT
BP02	GCA3	PPM5	SRALPHS
BP03	GCA9	PSBASS	SRAY
BP04	GCMGR1	PSEM	SVP1
BP05	GCMGR2	PTWEBSERVER	TDEMARCO
BP06	GCMGR3	RPARKER	VP1
CRM1	GCS1	RWA1	WAA1
CRM2	GCS2	SCM1	WAA2
DVP1	GCS3	SCM2	
EOPP_PORTALADM	HHCFO	SCM3	
EOPP_PORTALMGR	ISTEWARD	SCM4	

Accounts That Are Used in the FSCM 8.9 EP890DMO Demo Database

AL	CONNOR	GM_PLNSCA	PENNY
AMA1	CORY	GM_PLNSCH	PERCY
AMA2	CSADMIN	GM_PLSCTA	PERRY
AMA3	CSAPPR1	GM_PLSCTH	PETE
AMA4	DAVIDMORGAN	GM_PLVET	PEYTON
AMS1	DKING	GM_SPO	PHIL
AMS2	DMATS	GM_STKH	POLLY
AMS3	DPOND	GUEST	PSBASS
AMS4	DVP1	JOHNINARI	PSEM
AMSYS	EGC1	JUSTOSHUM	PTWEBSERVER
ANNE	EGD1	KELLYJONES	RENE
APA1	EGM1	KEVINDONS	RM1
APA2	EGR1	KPN	RM2
APA3	END1	LADAMS	RM3
APA4	ENM1	LBA	RM4
APS1	ENS1	LHILL	RM5
APS2	ENTMGR_CUST	LSA	ROB
APS3	ENTMGR_PRO	MGR1	SALLYH
APS4	ENTMGR_TRAIN	MGR2	SAM
ARA1	EOPP_PORTALADM	MGR3	SARAHMANDY
ARA2	EOPP_PORTALMGR	MGR4	SDAVIS
ARA3	EOPP_USER	MIKEIKEGAMI	SELLCM
ARA4	EXA1	MJONES	SELLER
ARS1	EXA2	MLAKE	SELLTREAS
ARS2	EXA3	MM1	SID
ARS3	EXA4	MM2	SKYTETSUKA

ARS4	EXS1	MM3	SRIVERS
ART	EXS2	MM4	SSA1
AUC_GUEST	EXS3	MM5	SSA2
BMEADOWS	EXS4	NEILKATSU	SSA3
BUYACCT	FVP1	PABLO	SSC1
BUYAPPR1	GALLEN	PAIGE	SSC2
BUYAPPR2	GEORGIAWINE	PAM	SSC3
BUYAPPR3	GLA1	PARRISH	SSS1
BUYER	GLA2	PARSON	SUPPLIER
BUYMTCH	GLA3	PAT	SVP1
CAMRON	GLA4	PATORILY	TRA1
CANDICE	GLS1	PATRICKSANCHEZ	TRBM1
CARL	GLS2	PATSY	TRCM1
CARLY	GLS3	PAUL	TRDM1
CARMEN	GLS4	PAULA	TRRM1
CARRIECONYERS	GM_AWDA	PAXTON	TWILLIAMS
CATADMIN	GM_COPI	PCA1	VP1
CEASAR	GM_DPHD	PCA2	VP2
CHANDRA	GM_MLCT	PCA3	VP3
CHARLEY	GM_PLADMA	PCA4	VP4
CHRISBAKER	GM_PLADMH	PCS1	VP5
CHRISTIE	GM_PLCCA	PCS2	VP6
CINDY	GM_PLCCH	PCS3	WENDYCHO
CLARK	GM_PLCOMA	PCS4	YCAMPOS
CLAUDE	GM_PLCOMH	PDA1	YSANCHEZ
CLINT	GM_PLCONA	PEARL	
CONNIE	GM_PLCONH	PEG	

Securing JD Edwards Default Accounts

Depending on the JD Edwards default account, you either need to lock the account, or you need to change the account's password.

This section covers the following topics:

- Accounts That Need to be Locked
- Accounts That Need Their Passwords Changed
- List of JD Edwards Database Accounts Per Release

Accounts That Need to be Locked

For accounts that are listed as OPEN and not in use, log into SQL*Plus with database administrative privileges and lock them as follows:

```
$ sqlplus username
Enter password: password
SQL> ALTER USER ACCOUNT ACCOUNT LOCK;
```

Refer to "List of JD Edwards Database Accounts Per Release" on page 4-22 for a listing of accounts used in each release.

Accounts That Need Their Passwords Changed

For accounts that are listed as OPEN in the Oracle Default Password Scanner report and being used by your current installation of a JD Edwards product, follow the guidelines below to change the password of these accounts.

> **Note:** Oracle Database allows you to set more than 10 characters for the password. However, JD Edwards database accounts have 10 character length limitation for the password.

Follow these steps:

1. If the account is being used in the [SECURITY] section of jde.ini on Enterprise Server, then use P98OWSEC [User Security] Application to change the password of the equivalent user account in EnterpriseOne.

   This password should be exactly same as the one you will set for the database account in step 3.

2. If the account is being used as a system user for User Security in EnterpriseOne, ERP 8, and Xe, then change the system password using the following methods:

   - **P980001 [Work With System Users] Application for EnterpriseOne release:** Refer to the "Working With Signon Security" chapter in *EnterpriseOne Install and Upgrade Guide*.
   - **P98OWSEC [User Security] Application for ERP 8 and OneWorld Xe release:** Refer to the "Working With User Security" chapter in *ERP 8 and OneWorld Xe System Administration Guide*. To change the system user's password for multiple users, refer to the latest documentation update of System Administration Guide for ERP8 and OneWorld Xe.

3. In Oracle Database, change the account's password. Be sure to create a password that has 10 or fewer characters.

   For example, log into SQL*Plus with database administrative privileges at a command prompt and enter the following commands:

   ```
   $ sqlplus username
   Enter password: password
   SQL> PASSWORD ACCOUNT;
   Changing password for ACCOUNT
   New password: new_password
   Retype new password: new_password
   ```

4. If account is being used in the [SECURITY] section of the jde.ini file on Enterprise Server, follow these steps

a. Modify the Password setting in jde.ini with the new password.

b. Restart the EnterpriseOne enterprise server instance.

5. If necessary, modify the jde.ini file in the deployment server.

   If you are installing a new release, upgrading from previous release, or applying a software update, the Installation Planner and Installation Workbench assume that the table owner's password is the same as the table owner, unless they find the override in the jde.ini file on the Deployment Server. Download and install the latest Planner update from the Update Center (http://www.peoplesoftcustomer.com)for the release you are using. Once database passwords have been changed, login to the deployment server with the new password. You will need to add this information to the jde.ini file.

   Follow these steps:

   a. Add the following section to the jde.ini file:

      ```
      [DSPWD]
      Datasource_owner=new_password
      ```

      For example, if you changed the passwords for PRODDTA and PRODCTL to password1 and password2, your section would look like this:

      ```
      [DSPWD]
      PRODDTA=password1
      PRODCTL=password2
      ```

   b. Secure the jde.ini file.

      Only JD Edwards Operating System accounts should have full access.

      In the Windows Explorer on the deployment server, right-click the jde.ini file under the WINDOWS directory and change the file permission on the **Security** tab.

   c. Log into the deployment server with the new password that you created in step 3.

   d. Run Installation Planner from the deployment server to create Plan.

   e. Run Installation Workbench from the deployment server to continue the installation, upgrade, or software update.

   f. Remove the [DSPWD] section from the jde.ini file.

List of JD Edwards Database Accounts Per Release

This section lists the default database owner accounts that are used in different releases of JD Edwards products. Some accounts are unique per release other are common across releases. After you run Oracle Default Password Scanner, refer to this list for the accounts the scanner's report lists as OPEN.

Accounts Common to EnterpriseOne 8.12, EnterpriseOne 8.11, EnterpriseOne 8.10, EnterpriseOne 8.9, ERP 8, OneWorld Xe, OneWorld B7332, OneWorld B7331

APPLEAD	DEVUSER	PRODUSER
CRPCTL	PRODCTL	TESTCTL
CRPDTA	PRODDTA	TESTDTA

Accounts Common to EnterpriseOne 8.9, ERP 8, OneWorld Xe

CNCADMIN PRISTCTL PRISTDTA

Accounts Common to EnterpriseOne 8.12, EnterpriseOne 8.9, ERP 8, OneWorld Xe, OneWorld B7332, OneWorld B7331

JDE JDEDBA

Accounts Common to EnterpriseOne 8.12, EnterpriseOne 8.11, EnterpriseOne 8.10

SYSADMIN

Accounts Common to EnterpriseOne 8.11, EnterpriseOne 8.10

PSFT PSFTDBA

Accounts Unique to EnterpriseOne 8.12

DD812	PS812	SVM812
DV812	PS812CTL	SY812
OL812	PS812DTA	
PD812	PY812	

Accounts Unique to EnterpriseOne 8.11

DD811	PS811	SVM811
DV811	PS811CTL	SY811
OL811	PS811DTA	
PD811	PY811	

Accounts Unique to EnterpriseOne 8.10

DD810	PS810	SVM810
DV810	PS810CTL	SY810
OL810	PS810DTA	
PD810	PY810	

Accounts Unique to EnterpriseOne 8.9

DD9	OL9	SVM9
DV9	PD9	SY9
JD9	PY9	

Accounts Unique to ERP 8

DD7334	OBJ7334	SVM7334

DV7334	PD7334	SYS7334
JD7334	PY7334	

Accounts Unique to OneWorld Xe

DD7333	OBJ7333	SVM7333
DV7333	PD7333	SYS7333
JD7333	PY7333	

Accounts Common to OneWorld B7332, OneWorld B7331

CRPB733	OBJB733	SVMB733
DDB733	PRISTB733	SYSB733
DEVB733	PRODB733	

5

Troubleshooting Oracle Default Password Scanner

This chapter covers the following topics:

Connection Errors

The following common connection errors can occur. For information on other types of errors, see *Oracle Database Error Messages*.

"ORA-12162: TNS:net service name is incorrectly specified"

Possible reasons:

- `ORACLE_HOME` environment variable is not set.
- `ORACLE_SID` environment variable is not set.

In addition, check the `tnsnames.ora` file to ensure it is correctly configured.

"ORA-01031: insufficient privileges"

You may not belong to the DBA group. Please refer to the platform specific requirements to enable this. In most UNIX operating systems, you must typically be a member of the DBA group. In Microsoft Windows, you must be a member of the `ORA_DBA` group.

"ORA-09925: Unable to create audit trail file" (and other permission denied errors)

You do not have permissions to access the database. Log on using a valid user (such as the oracle user) to connect to the database.

"Connected to an idle instance" Error

The database may not be running. To start the database, issue a `STARTUP` command in SQL*Plus. For more information, see *Oracle Database Administrator's Guide*.

"ORA-28000: the account is locked"

The account you are trying to log onto is locked. To unlock the account, log on with administrative privileges and enter the following command:

```
$ sqlplus username
Enter password: password
```

```
SQL> ALTER USER ACCOUNT ACCOUNT UNLOCK;
```

"ORA-01017: invalid username/password; logon denied"

The user name or password is incorrect. Check that the user name and password you are trying to use are correct.

Troubleshooting Patches That Require Default Passwords

Some applications or patches may require a predefined account in order to install successfully. If the application or patch you apply requires a specific account, then unlock the account. If the application or patch also requires a predefined password, then unlock the account and refer to the application or patch documentation for the required password. Once you have completed the installation, you should secure the account by following the instructions in this guide.

To unlock an account, log into SQL*Plus using administrative privileges and enter the following commands:

```
$ sqlplus username
Enter password: password
SQL> ALTER USER ACCOUNT ACCOUNT UNLOCK;
```