Symantec™ Data Loss Prevention Oracle 11g Installation and Upgrade Guide

Version 11.0

Symantec Data Loss Prevention Oracle Installation and Upgrade Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 11.0

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the *Third-Party License Agreements* document accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Installing Oracle 11g on Windows

This chapter includes the following topics:

About the Oracle 11g installation

To use Symantec Data Loss Prevention, install Oracle 11g Release 2 and create a database using the Symantec Data Loss Prevention database template. You must also create an Oracle user account with the correct permissions to access and modify the database. The Enforce Server uses this account to store configuration and incident data for the Symantec Data Loss Prevention deployment.

You can perform a two-tier or single-tier Symantec Data Loss Prevention installation. In both of these cases, the database runs on the same computer as the Enforce Server. Alternatively, you can perform a three-tier Symantec Data Loss Prevention installation. In this case, the database runs on a different computer from the Enforce Server.

If you implement a three-tier installation, you must install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server. Installation of the Oracle Client enables database communications between the Oracle database server and the Enforce Server. The Symantec Data Loss Prevention installer needs SQL*Plus to create tables and views on the Enforce Server. For this reason, the Windows user account that is used to install Symantec Data Loss Prevention needs access to SQL*Plus.

For full details on how to install the Oracle 11g Database Client software, see the platform-specific documentation from Oracle Corporation, available from the Oracle documentation library at http://www.oracle.com/pls/db111/portal.portal_db?selected=11.

Note: After you create the Symantec Data Loss Prevention database and complete the Symantec Data Loss Prevention installation, you can change the database password. To change the database password, you use the Symantec Data Loss Prevention DBPasswordChanger utility.

For more information about the Symantec Data Loss Prevention DBPasswordChanger utility, see the *Symantec Data Loss Prevention Administration Guide*.

About the Oracle 11g Client software for Windows

For full details on how to install the Oracle 11g Database Client software, see the *Oracle Database Client Installation Guide 11g Release 2 (11.2) for Microsoft Windows*. To view this document, see `http://download.oracle.com/docs/cd/E11882_01/install.112/e10844/toc.htm`.

Installing Oracle 11g on Windows

Install Oracle 11g and create the Symantec Data Loss Prevention database by performing the following steps on the server computer that will host the Oracle database.

Table 1-1 Installing Oracle 11g and creating the Symantec Data Loss Prevention database

Step	Action	Description
Step 1	Review the system requirements for the Oracle 11g.	See the Oracle Web pages for the system requirements for Oracle 11g.
Step 2	Download the Oracle 11g software.	See "Downloading the Oracle 11g software for Windows" on page 11.
Step 3	Install Oracle 11g.	See "Installing the Oracle 11g software for Windows" on page 12.
Step 4	Create the Symantec Data Loss Prevention database.	See "Creating the Symantec Data Loss Prevention database" on page 13.
Step 5	Create the database listener.	See "Creating the TNS Listener on Windows" on page 16.
Step 6	Configure the local net service name.	See "Configuring the local net service name" on page 17.
Step 7	Create the Symantec Data Loss Prevention database user.	See "Creating the Oracle user account for Symantec Data Loss Prevention " on page 20.
Step 8	Lock the DBSNMP account for security purposes.	See "Locking the DBSNMP Oracle user account" on page 20.
Step 9	Install the Oracle Critical Patch Update (CPU).	The latest *Oracle 11g Release 2 Critical Patch Update Guide* explains how to download and apply the CPU for Oracle.

Downloading the Oracle 11g software for Windows

You should have received a Symantec Serial Number Certificate with your order that lists a serial number for each of your products. If you did not receive the certificate, contact Symantec Customer Care as described at `http://www.symantec.com/business/support/assistance_care.jsp`. If you have multiple serial numbers , locate the serial number that corresponds to Oracle Standard Edition.

Go to `https://fileconnect.symantec.com` and enter the serial number. Proceed to the list of available downloads and download and extract the following files:

- `Oracle_11.2.0.1.0_Server_Win.zip`
  This ZIP file contains Oracle 11g Release 2 software (`win32_11gR2_database_1of2.zip`, `win32_11gR2_database_2of2.zip`, and `win64_11gR2_database_Complete.zip`).
- `Oracle_11.2.0.1.0_Server_Installation_Tools_Win.zip`
  This ZIP file contains the Symantec Data Loss Prevention Oracle database template and database user SQL script (`11g_r2_32_bit_Installation_Tools.zip` and `11g_r2_64_bit_Installation_Tools.zip`).

Installing the Oracle 11g software for Windows

The Enforce Server uses the Oracle thin driver and the Oracle Client. Symantec Data Loss Prevention packages the JAR files for the Oracle thin driver with the Symantec Data Loss Prevention software. But, you must also install the Oracle Client. The Symantec Data Loss Prevention installer needs SQL*Plus to create tables and views on the Enforce Server. Therefore, the Windows user account that is used to install Symantec Data Loss Prevention must be able to access to SQL*Plus.

See “About the Oracle 11g Client software for Windows” on page 10.

To install Oracle 11g Release 2

1. Shut down the following services if they are running in Windows Services:
   - All Oracle services
   - Distributed Transaction Coordinator service

   To view the services go to **Start > Control Panel > Administrative Tools > Computer Management**, and then expand **Services and Applications** and click **Services**.
2. Unzip the required software installation files and navigate to the database directory:
   - For 32-bit systems, unzip both `win32_11gR2_database_1of2.zip` and `win32_11gR2_database_2of2.zip`.
   - For 64-bit systems, unzip `win64_11gR2_database_Complete.zip`

3. To install the Oracle software, double-click on the Oracle Universal Installer file, `setup.exe`.

4. On the **Configure Security Updates** panel, de-select **I wish to receive security updates via My Oracle Support**, and click **Next**.

   Symantec certifies and provides Oracle Critical Patch Updates for use with Symantec Data Loss Prevention, along with detailed installation instructions. You do not need to receive these updates from Oracle Support.

5. Click **Yes** to confirm that you have not provided an email address.

6. On the **Select Installation Option** panel, select **Install database software only** and click **Next**.

7. On the **Grid Installation Options** panel, select **Single instance database installation** and click **Next**.

8. On the **Select Product Languages** panel, click **Next** to accept English as the default language.

9. On the **Select Database Edition** panel, select **Standard Edition** and click **Next**.

10. On the **Specify Installation Location** panel, enter the following paths in the specified fields, and click **Next**:

    - **Oracle Base**: Enter `c:\oracle`
    - **Software Location**: Enter `c:\oracle\product\11.2.0\db_1`

    Note: All example paths in this document use the installation directory `c:\oracle\product\11.2.0\db_1`. If you specify a different installation directory, substitute the correct path as necessary throughout this document.

    The installer application performs a prerequisite check and displays the results.

11. On the **Summary** panel, click **Finish** to begin the installation.

    The installer application installs the Oracle 11g software to your computer.

12. On the **Finish** panel, click **Close** to exit the installer application.

Creating the Symantec Data Loss Prevention database

Perform the following procedure to create the Symantec Data Loss Prevention database.

Note: If you are installing Oracle 11g on a 64-bit computer in order to migrate an existing 32-bit Symantec Data Loss Prevention database, do not perform this procedure.

See “Migrating from Oracle 10g 32-bit to Oracle 11g 64-bit” on page 58.

To create the Symantec Data Loss Prevention database

1. Set the ORACLE_HOME environment variable for your new installation. Open a command prompt, and enter:

   ```
   set ORACLE_HOME=c:\oracle\product\11.2.0\db_1
   ```

   If you installed Oracle 11g into a different location, substitute the correct directory in this command.

   You may want to configure your Windows system to automatically set the ORACLE_HOME environment variable each time you log on. See your Windows documentation for details about setting environment variables.
2. Extract the database template file (`.dbt` file) from the `11g_r2_32_bit_Installation_Tools.zip` or `11g_r2_64_bit_Installation_Tools.zip` file to the `%ORACLE_HOME%\assistants\dbca\templates` folder. For example, copy `Oracle_11g_Database_for_Vontu_v11.dbt` for 32-bit installations, or copy `Oracle_11g_Database_for_Vontu_v11_64_bit.dbt` for 64-bit installations.
3. Start the Oracle Database Configuration Assistant to create the Symantec Data Loss Prevention database. Choose **Start > All Programs > Oracle - OraDb11g_home1 > Configuration and Migration Tools** > **Database Configuration Assistant**.
4. On the **Welcome** panel, click **Next**.
5. On the **Operations** panel, select **Create a Database** and click **Next**.
6. On the **Database Templates** panel, select **Oracle 11g Database for Vontu v11 32 bit** for 32-bit installations, or select **Oracle 11g Database for Vontu v11 64 bit** for 64-bit installations. Click **Next**.

   Caution: You must use the Symantec Data Loss Prevention template to create the database. Do not use an alternate template or reuse an existing database instance. If you do not use the supplied template, failures can occur when you use Symantec Data Loss Prevention. Failures can also occur later when you try to upgrade the product.

   ---

7. On the **Database Identification** panel, set the database name (Global Database Name) and the Oracle System Identifier (SID) by performing the following steps in this order:
   - Enter **protect** in the **Global Database Name** field.
     The **SID** field is automatically set to **protect**. Keep the SID and the Global Database Name fields as the same value, "protect."
   - Click **Next**.
   - Write down the database name and SID for later use when you install the Symantec Data Loss Prevention software.
8. On the **Management Options** panel, perform the following steps in order:
   - Deselect **Configure Enterprise Manager**.
   - Select the **Automatic Maintenance Tasks** tab and deselect **Enable automatic maintenance tasks**.
   - Click **Next**.
9. On the **Database Credentials** panel, perform the following steps in order:
   - Select **Use the Same Administrative Password for All Accounts**.
   - Enter a password in the **Password** field.
   - Re-enter the same password in the **Confirm Password** field.
   - Click **Next**.

   Follow these guidelines to create acceptable passwords:
   - Passwords cannot contain quotation marks.
   - Passwords are not case-sensitive.
   - Passwords must begin with an alphabetic character.
   - Passwords can only contain alphanumeric characters. Do not use underscore (_), the dollar sign ($), and pound sign (#) for your password, because Oracle interprets these symbols differently than other systems.
   - A password cannot be an Oracle-reserved word such as `SELECT`.

   If you enter a password that does not meet these guidelines, Oracle keeps prompting for a password. You must enter a password. Do not kill the Oracle Database Configuration Assistant.

   Note: You can optionally use different passwords for each user account type. The various user account types are SYS, SYSTEM, DBSNMP, and SYSMAN.

10 On the **Database File Locations** panel, accept the default selection, **Use Database File Locations from Template**, and click **Finish**.

   The Database Configuration Assistant displays a **Confirmation** window with a summary of the database configuration.

11 Click **OK** on the **Confirmation** window to create the database.

   The database creation can take up to 20 minutes to complete. If the database creation process fails or hangs, check the Oracle Database Configuration Assistant logs (located in the `%ORACLE_HOME%\cfgtoollogs\dbca\SID` folder) for errors (for example, `c:\oracle\product\11.2.0\db_1\cfgtoollogs\dbca\protect`).

   When the database creation process is complete, another **Database Configuration Assistant** window opens and displays the database details.

12 Click **Exit**.

13 If the database service (OracleServicePROTECT) is down, start it using Windows Services. To view services, choose **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**, and then open **Services**.

Creating the TNS Listener on Windows

Perform the following procedure to create a TNS listener for the Symantec Data Loss Prevention database.

To create the TNS Listener

1 (Optional) If you logged on as a domain user, you must set the `sqlnet.ora` file `SQLNET.AUTHENTICATION_SERVICES=()` value to `none`. Otherwise, proceed to step 2.

   To set the `sqlnet.ora` file `SQLNET.AUTHENTICATION_SERVICES=()` value, perform the following steps in this order:

   - Open `sqlnet.ora`, located in the `%Oracle_Home%\network\admin` folder (for example, `c:\oracle\product\11.2.0\db_1\NETWORK\ADMIN`), using a text editor.
   - Change the `SQLNET.AUTHENTICATION_SERVICES=(NTS)` value to `none`:

     ```
     SQLNET.AUTHENTICATION_SERVICES=(none)
     ```

- Save and close the `sqlnet.ora` file.

2. Start the Oracle Net Configuration Assistant by selecting **Start > All Programs > Oracle - OraDb11g_home1 > Configuration and Migration Tools > Net Configuration Assistant**.
3. On the **Welcome** panel, select **Listener configuration** and click **Next**.
4. On the **Listener Configuration, Listener** panel, select **Add** and click **Next**.
5. On the **Listener Configuration, Listener Name** panel, enter a listener name and click **Next**.

   Note: Use the default listener name, LISTENER, unless you must use a different name.

6. On the **Listener Configuration, Select Protocols** panel, select the **TCP** protocol and click **Next**.
7. On the **Listener Configuration, TCP/IP Protocol** panel, select **Use the standard port number of 1521** and click **Next**.
8. On the **Listener Configuration, More Listeners?** panel, select **No** and click **Next**.
9. On the **Listener Configuration Done** panel, click **Next**.
10. Leave the Oracle Net Configuration Assistant open to configure the Local Net Service Name.

    See "Configuring the local net service name" on page 17.

Configuring the local net service name

Perform the following procedure to configure the Local Net Service Name for the Symantec Data Loss Prevention database.

To configure the local net service name

1. If the Oracle Net Configuration Assistant is not already running, start it by selecting **Start > All Programs > Oracle - OraDb11g_home1 > Configuration and Migration Tools > Net Configuration Assistant**.
2. On the **Welcome** panel, select **Local Net Service Name configuration** and click **Next**.
3. On the **Net Service Name Configuration** panel, select **Add** and click **Next**.

4 On the **Net Service Name Configuration, Service Name** panel, enter "protect" in the **Service Name** field and click **Next**.

5 On the **Net Service Name Configuration, Select Protocols** panel, select **TCP** and click **Next**.

6 On the **Net Service Name Configuration, TCP/IP Protocol** panel:

- Enter the IP address of the Oracle server computer in the **Host name** field.
- Select **Use the standard port number of 1521** (the default value).
- Click **Next**.

7 On the **Net Service Name Configuration, Test** panel, select **No, do not test** and click **Next**.

Do not test the service configuration, because the listener has not yet started.

8 On the **Net Service Name Configuration, Net Service Name** panel, select accept the default name of "protect" and click **Next**.

9 On the **Net Service Name Configuration, Another Net Service Name?** panel, select **No** and click **Next**.

10 On the **Net Service Name Configuration Done** panel, select **Next**.

11 Click **Finish** to exit the Oracle Net Configuration Assistant.

Verifying the Symantec Data Loss Prevention database

After creating the Symantec Data Loss Prevention database, you should verify that it was created correctly.

To verify that the database was created correctly

1 Open a new command prompt and start SQL*Plus:

```
sqlplus /nolog
```

Using a new command prompt ensures that your Path environment variable includes the SQL*Plus directory.

2 Log on as the SYS user:

```
SQL> connect sys/password@protect as sysdba
```

Where `password` represents the SYS password.

3. Run the following query:

   ```
   SQL> SELECT * FROM v$version;
   ```

4. Make sure that the output from the query contains the following information, which identifies the software components as version 11.2.0.1. For a 32-bit installation, the output should read:

   ```
   BANNER
   -------------------------------------------------------------------------

   Oracle Database 11g Release 11.2.0.1.0 - Production
   PL/SQL Release 11.2.0.1.0 - Production
   CORE    11.2.0.1.0      Production
   TNS for 32-bit Windows: Version 11.2.0.1.0 - Production
   NLSRTL Version 11.2.0.1.0 - Production
   ```

   For a 64-bit installation, the output should read:

   ```
   BANNER
   -------------------------------------------------------------------------

   Oracle Database 11g Release 11.2.0.1.0 - Production
   PL/SQL Release 11.2.0.1.0 - Production
   CORE    11.2.0.1.0      Production
   TNS for 64-bit Windows: Version 11.2.0.1.0 - Production
   NLSRTL Version 11.2.0.1.0 - Production
   ```

5. Run the following command to describe the `dba_tablespaces` view:

   ```
   SQL> describe dba_tablespaces;
   ```

6. Check that the output contains the following information:

   ```
   RETENTION     VARCHAR2(11)
   BIGFILE       VARCHAR2(3)
   ```

7. Exit SQL*Plus:

   ```
   SQL> exit
   ```

Creating the Oracle user account for Symantec Data Loss Prevention

Perform the following procedure to create an Oracle user account and name it “protect.”

To create the new Oracle user account named protect

1. Extract the SQL script file, `oracle_create_user.sql`, from the `11g_r2_32_bit_Installation_Tools.zip` or `11g_r2_64_bit_Installation_Tools.zip` file to a local directory.
2. Open a command prompt and go to the directory where you extracted the `oracle_create_user.sql` file.
3. Start SQL*Plus:

   ```
   sqlplus /nolog
   ```

4. Run the `oracle_create_user.sql` script:

   ```
   SQL> @oracle_create_user.sql
   ```

5. At the **Please enter the password for sys user** prompt, enter the password for the SYS user.
6. At the **Please enter sid** prompt, enter "protect."
7. At the **Please enter required username to be created** prompt, enter "protect" for the user name.
8. At the **Please enter a password for the new username** prompt, enter a new password.

   Store the password in a secure location for future use. You must use this password to install Symantec Data Loss Prevention. If you need to change the password after you install Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention Administration Guide* for instructions.

Locking the DBSNMP Oracle user account

To maintain security, you should lock the Oracle DBSNMP user account.

To lock the Oracle DBSNMP user account

1. Open a command prompt and start SQL*Plus:

   ```
   sqlplus /nolog
   ```

2. Log on as the SYS user:

   ```
   SQL> connect sys/password as sysdba
   ```

   Where `password` is the SYS password.

3. Lock the DBSNMP user account:

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

4. Exit SQL*Plus:

   ```
   SQL> exit
   ```

Chapter 2

Upgrading a Symantec Data Loss Prevention database to Oracle 11g on Windows

This chapter includes the following topics:

Upgrading an Oracle 10g database on Windows

If you have an existing Symantec Data Loss Prevention database that runs on Oracle 10g, you can choose to continue using that database, or you can upgrade the 10g database to use Oracle 11g. Follow these steps, in order, to upgrade an Oracle 10g Symantec Data Loss Prevention database to use Oracle 11g:

Table 2-1 Upgrading a Symantec Data Loss Prevention database from Oracle 10g to Oracle 11g

Step	Action	Description
Step 1	Delete the existing Oracle 10g listener.	See "Removing the Oracle 10g listener on Windows" on page 24.

Table 2-1 Upgrading a Symantec Data Loss Prevention database from Oracle 10g to Oracle 11g *(continued)*

Step	Action	Description
Step 2	Install the Oracle 11g software and use the Oracle Database Upgrade Assistant to upgrade the Symantec Data Loss Prevention database.	See "Upgrading from Oracle 10g to Oracle 11g" on page 25.
Step 3	Modify the configuration of the upgraded Symantec Data Loss Prevention database.	See "Configuring the upgraded 11g database" on page 28.
Step 4	Install the Oracle Critical Patch Update (CPU).	The latest *Oracle 11g Release 2 Critical Patch Update Guide* explains how to download and apply the latest CPU for Oracle.

Removing the Oracle 10g listener on Windows

Perform the following procedure to delete the existing Oracle 10g TNS listener before you upgrade to Oracle 11g.

To remove the Oracle 10g listener on Windows

1. Start the Oracle Net Configuration Assistant by selecting **Start > All Programs > Oracle - OraDb10g_home1 > Configuration and Migration Tools > Net Configuration Assistant**.
2. On the **Welcome** panel, select **Listener configuration** and click **Next**.
3. On the **Listener Configuration, Listener** panel, select **Delete** and click **Next**.
4. On the **Listener Configuration, Select Listener** panel, select the name of the listener you want to delete, and click **Next**.
5. If the listener is running, the Net Configuration Assistant asks if you want to stop and delete the selected listener. Select **Yes**.
6. On the **Listener Configuration, Listener Deleted** panel, select **Next**.
7. On the **Listener Configuration Done** panel, select **Next**.
8. On the **Welcome** panel, select **Finish** to exit the Net Configuration Assistant.

Upgrading from Oracle 10g to Oracle 11g

If you have an existing Symantec Data Loss Prevention database running on Oracle 10g and you want to upgrade that database to run on Oracle 11g, follow these steps to perform the upgrade.

To upgrade an existing Symantec Data Loss Prevention database to Oracle 11g

1. Shut down the Enforce Server that accesses the Oracle 10g database.

   See the *Symantec Data Loss Prevention System Administration Guide* for information about shutting down Symantec Data Loss Prevention servers.

2. Download and unzip the Oracle 11g software to the server computer that is running your Oracle 10g database.

   See "Downloading the Oracle 11g software for Windows" on page 11.

3. Double-click on the Oracle 11g Universal Installer file, `setup.exe`.

4. On the **Configure Security Updates** panel, de-select **I wish to receive security updates via My Oracle Support**, and click **Next**.

5. Click **Yes** to confirm that you have not provided an email address.

6. On the **Select Installation Option** panel, select **Upgrade an existing database** and click **Next**.

7. On the **Select Product Languages** panel, click **Next** to accept English as the default language.

8. On the **Select Database Edition** panel, select **Standard Edition** and click **Next**.

9. On the **Specify Installation Location** panel, enter the following paths in the specified fields, and click **Next**:

   - **Oracle Base**: Enter `c:\oracle`
   - **Software Location**: Enter `c:\oracle\product\11.2.0\db_1`

   Note: All example paths in this document use the installation directory `c:\oracle\product\11.2.0\db_1`. If you specify a different installation directory, substitute the correct path as necessary throughout this document.

   The installer application performs a prerequisite check and displays the results.

10. On the **Summary** panel, click **Finish** to begin the installation.

    The installer application installs the Oracle 11g software to your computer.

11. On the **Finish** panel, click **Close** to exit the installer application.

    The installer upgrades the Oracle 10g software and then starts the Oracle Net Configuration Assistant.

12. On the Oracle Net Configuration Assistant **Welcome** panel, deselect **Perform typical configuration** and click **Next**.
13. On the **Listener Configuration, Listener Name** panel, enter a listener name and click **Next**.

    Note: Use the default listener name, LISTENER, unless you must use a different name.

    ---

14. On the **Listener Configuration, Select Protocols** panel, select the **TCP** protocol and click **Next**.
15. On the **Listener Configuration, TCP/IP Protocol** panel, select **Use the standard port number of 1521** and click **Next**.
16. On the **Listener Configuration, More Listeners?** panel, select **No** and click **Next**.
17. On the **Listener Configuration Done** panel, click **Next**.
18. On the **Naming Methods Configuration** panel, select **No** and click **Next**.
19. Click **Finish** after the network configuration completes.

    The installer loads the Database Upgrade Assistant.

20. On the **Welcome** panel of the Database Upgrade Assistant, click **Next**.
21. On the **Select Database** panel:
    - Select the PROTECT database from the list of available databases.
    - Enter the password to the sys account in the **Password** field.
    - Click **Next** to continue.

    The upgrade assistant gathers information about the PROTECT database.

22. The upgrade assistant may display a **Warnings** window that lists warning conditions that were determined during the upgrade check. If the window indicates that you should purge the recycle bin, start SQL*Plus and enter the `purge dba_recyclebin;` command. Then click **Yes** in the Oracle 11g Universal Installer to continue with the upgrade. You can view review other warning conditions at a later time by examining the `c:\oracle\product\11.2.0\db_1\cfgtoollogs\dbua\protect\upgrade1\PreUpgradeResults.html` file.

23 On the **Upgrade Options** panel, select **Backup database** and specify a backup directory if you do not have a current backup of the PROTECT database. Click **Next** to continue.

24 On the **Move Database Files** panel:

- Select **Move Database Files during Upgrade**.
- Select **File System**.
- Click **Next** to continue.

25 On the **Database File Locations** panel, click **Next** to accept the default location for the database files (`c:\oracle\product\11.2.0\db_1\oradata`).

26 On the **Recovery and Diagnostic Locations** panel, click **Next** to accept the default destinations.

27 On the **Management Options** panel, click **Next** to accept the default configuration.

28 On the **Summary** panel, click **Finish** to begin the database upgrade.

The Database Upgrade Assistant displays a **Progress** window while it performs the upgrade.

At the **Progress** window you may see the error, `Identifier SYS.DBMS_JAVA must be declared`. You can safely ignore this error by clicking **Ignore**.

29 On the **Upgrade Result** panel, click **Close**. The Database Upgrade Assistant displays a document summary. Depending on your database environment, the summary may display errors such as `00201: identifier SYS.DBMS_JAVA must be declared`, which can be ignored.

30 After you finish upgrading the Oracle 10g database to Oracle 11g, change the ORACLE_HOME environment variable to point to your new installation. Open a command prompt, and enter:

```
set ORACLE_HOME=c:\oracle\product\11.2.0\db_1
```

If you installed Oracle 11g into a different location, substitute the correct directory in this command.

Also update your Windows system to automatically set the ORACLE_HOME environment variable each time you log on . See your Windows documentation for details about setting environment variables.

Configuring the upgraded 11g database

After you finish upgrading the Oracle 10g database to Oracle 11g, perform these steps to alter the database password lifetime and disable certain automated maintenance tasks.

To configure the upgraded database

1. Copy the SQL script file, `post_v11_upgrade_11gr2.sql`, from the `c:\Vontu\Protect\install\sql` directory of a Symantec Data Loss Prevention version 11 installation to a local directory.

2. Open a terminal prompt and go to the directory where you extracted the `post_v11_upgrade_11gr2.sql` script.

3. Start SQL*Plus:

   ```
   sqlplus /nolog
   ```

4. Log on as the SYS user:

   ```
   SQL> connect sys/password as sysdba
   ```

   Where *password* represents the SYS password.

5. Execute the following command to remove the password lifetime limit:

   ```
   alter profile default limit password_life_time unlimited;
   ```

6. Enter the following commands to disable automated maintenance tasks:

```
begin
   dbms_auto_task_admin.disable(
      client_name => 'auto optimizer stats collection',
      operation => NULL,
      window_name => NULL
   );

   dbms_auto_task_admin.disable(
      client_name => 'auto space advisor',
      operation => null,
      window_name => null
   );

   dbms_auto_task_admin.disable(
      client_name => 'sql tuning advisor',
      operation => null,
      window_name => null
   );
end;
```

7. Verify that the automated maintenance tasks are disabled by executing the following command:

```
select client_name, status from dba_autotask_client;
```

8. Execute these commands to modify the database initialization parameters:

```
alter system set memory_target = 1536m scope=spfile;
alter system set memory_max_target = 1536m scope=spfile;
alter system set sga_max_size = 0 scope=spfile;
alter system set sga_target = 0 scope=spfile;
alter system set compatible = '11.2.0.1.0' scope=spfile;
```

9. Execute the `utlrp.sql` script to recompile any invalid objects:

```
@%ORACLE_HOME%\rdbms\admin\utlrp.sql
```

10. Execute the post upgrade script for the Symantec Data Loss Prevention database:

    ```
    @post_v11_upgrade_11gr2.sql
    ```

    If the post upgrade script is not in the current working directory, specify the full path to the script.

11. Exit SQL*Plus:

    ```
    exit
    ```

12. Restart the Enforce Server.

Chapter 3

Installing Oracle 11g on Linux

This chapter includes the following topics:

About the Oracle 11g installation

To use Symantec Data Loss Prevention, you must install Oracle 11g and create a database using the Symantec Data Loss Prevention database template. You must also create an Oracle user account with the correct permissions to access and modify the database. The Enforce Server uses this account to store configuration and incident data for the Symantec Data Loss Prevention deployment.

You can perform a two-tier or single-tier Symantec Data Loss Prevention installation. In both of these cases, the database runs on the same computer as the Enforce Server. Alternatively, you can perform a three-tier Symantec Data Loss Prevention installation. In this case, the database runs on a different computer from the Enforce Server.

In a three-tier installation, your organization’s database administration team installs, creates, and maintains the Symantec Data Loss Prevention database. If your organization already has other databases that run on Oracle 11g, consider using your organization’s existing Oracle 11g installation. For information about how to set up the Symantec Data Loss Prevention database in a three-tier environment, contact your Symantec representative.

If you implement a three-tier installation, you must install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server. Installation of the Oracle Client enables database communications between the Oracle database server and the Enforce Server. The Symantec Data Loss Prevention installer needs SQL*Plus to create tables and views on the Enforce Server. For this reason, the Linux user account that is used to install Symantec Data Loss Prevention needs access to SQL*Plus.

For full details on how to install the Oracle 11g Database Client software, see the platform-specific documentation from Oracle Corporation, available from the Oracle documentation library at http://www.oracle.com/pls/db111/portal.portal_db?selected=11.

Note: After you create the Symantec Data Loss Prevention database and complete the Symantec Data Loss Prevention installation, you can change the database password. To change the database password, you use the Symantec Data Loss Prevention DBPasswordChanger utility.

For more information about the Symantec Data Loss Prevention DBPasswordChanger utility, see the *Symantec Data Loss Prevention Administration Guide*.

About the Oracle 11g Client software for Linux

For full details on how to install the Oracle 11g Database Client software, see the *Oracle® Database Client Installation Guide 11g Release 2 (11.2) for Linux*. To view this document, see `http://download.oracle.com/docs/cd/E11882_01/install.112/e16765/toc.htm`.

Installing Oracle 11g on Linux

Install Oracle 11g and create the Symantec Data Loss Prevention database by performing the following steps on the server computer that will host the Oracle database.

Table 3-1 Installing Oracle 11g and creating the Symantec Data Loss Prevention database

Step	Action	Description
Step 1	Review the system requirements for the Oracle 11g.	See the Oracle Web pages for the system requirements for Oracle 11g.
Step 2	Download the Oracle 11g software.	See "Downloading the Oracle 11g software for Linux" on page 37.
Step 3	Perform the preinstallation steps.	See "Performing the preinstallation steps" on page 34.
Step 4	Install Oracle 11g.	See "Installing the Oracle 11g software for Windows" on page 12.
Step 5	Create the Symantec Data Loss Prevention database.	See "Creating the Symantec Data Loss Prevention database" on page 13.
Step 6	Create the database listener.	See "Creating the TNS Listener on Windows" on page 16.
Step 7	Configure the local net service name.	See "Configuring the local net service name" on page 17.
Step 8	Create the Symantec Data Loss Prevention database user.	See "Creating the Oracle user account for Symantec Data Loss Prevention " on page 20.
Step 9	Lock the DBSNMP account for security purposes.	See "Locking the DBSNMP Oracle user account" on page 20.

Table 3-1 Installing Oracle 11g and creating the Symantec Data Loss Prevention database *(continued)*

Step	Action	Description
Step 10	Install the Oracle Critical Patch Update (CPU).	The latest *Oracle 11g Release 2 Critical Patch Update Guide* explains how to download and apply the latest CPU for Oracle.

Performing the preinstallation steps

Perform the following steps to prepare your Linux environment for installation.

To prepare the Linux environment

1. Log on as the root user. Copy the `11g_r2_32_bit_Installation_Tools.tar.gz` file (for 32-bit platforms) or `11g_r2_64_bit_Installation_Tools.tar.gz` file (for 64-bit platforms) to the Linux server and extract its contents into the temporary directory (`/tmp`). For example:

   ```
   tar xvfz 11g_r2_32_bit_Installation_Tools.tar.gz
   ```

   Extracting creates a subdirectory that is called `oracle_install` in the `/tmp` directory and extracts the files into that subdirectory.

2. Go to the `oracle_install` directory and run the verification script to verify the requirements for the database.

   ```
   cd oracle_install
   ./scripts/oracle_verify.sh
   ```

   Note: You must run this script in the `oracle_install` directory. Do not change directory to the `scripts` directory.

   The script displays the following items that you need to verify:

   - Physical memory
     The system must have at least 1024 MB of physical RAM.
   - Swap space
     The following list shows the relationship between the available RAM and the required swap space.

- When the available RAM is between 1024 MB and 2048 MB, Oracle requires swap space 1.5 times the size of RAM.
- When the available RAM is between 2049 MB and 8192 MB, Oracle requires swap space equal to the size of RAM.
- When the available RAM is more than 8192 MB. Oracle requires swap space 75% of the size of RAM.

If the system does not have the required swap space, you can add temporary swap space to your system. You create a temporary swap file instead of using a raw device. You should create swap space only after you restart the server. If you create the swap space and then restart the server, then the swap space is removed when the server is restarted.

3. Verify that there is at least 400 MB under `/tmp`.
4. Verify that the Red Hat Enterprise Linux version is the version that Symantec requires for running Symantec Data Loss Prevention. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*.
5. Verify that the following rpm packages with the required version (or higher) have been installed:

```
binutils-2.17.50.0.6-6.el5
compat-db-4.2.52-5.1
compat-libstdc++-296-2.96-138
control-center-2.16.0-16.el5
gcc-4.1.2-42.el5
gcc-c++-4.1.2-42.el5
glibc-2.5-24
glibc-common-2.5-24
glibc-devel-2.5-24
glibc-headers-2.5-24
libstdc++-4.1.2-42.el5
libgomp-4.1.2-42.el5
libstdc++-devel-4.1.2-42.el5
libXp-1.0.0-8.1.el5
make-3.81-3.el5
sysstat-7.0.2-1.el5
libaio-0.3.106-3.2
unixODBC-devel-2.2.11
```

If any of these packages are not installed, then the script returns a message saying that packet is not installed. For example, `package gnome-libs is not installed`. Install any missing packages.

6. Run the oracle_prepare.sh script:

   ```
   ./scripts/oracle_prepare.sh
   ```

   If the Oracle user does not already exist, you are prompted for the password for the new Oracle user. The Oracle user is used to install and manage the Oracle database. This script sets proper kernel parameters for the Oracle database.

   oracle_prepare.sh overwrites certain kernel parameters in the `/etc/sysctl.conf` file. Oracle recommends the settings for these parameters. However, you may want certain parameters to be set to higher values than those suggested by Oracle. In that case, you can edit `/etc/sysctl.conf` file after running oracle_prepare.sh. The original values are commented out by the shell script. The new values are those recommended by Oracle. If you choose to manually edit this file, make sure that you do not make the values lower than those recommended by Oracle.

7. Restart the server so that the updated kernel parameters take effect.

8. If the server does not have enough swap space (as determined in the verification process), add more, temporarily:

   ```
   dd if=/dev/zero of=tmpswap bs=1k count=4194304
   chmod 600 tmpswap
   mkswap tmpswap
   swapon tmpswap
   ```

   This command can take several minutes to complete.

   The foregoing example creates 4 GB (1K * 4,194,304) of additional swap space, thereby avoiding the need to use a raw device.

   After installing the Oracle software, you can remove any temporary swap space you previously created by entering the following commands:

   ```
   swapoff tmpswap
   rm tmpswap
   ```

9 Verify that there is enough space under `/var`. For a small to medium enterprise, `/var` should have at least 15 GB. For a large enterprise, `/var` should have at least 30 GB. For a very large enterprise, `/var` should have at least 45 GB of free space. As your organization's traffic expands, these figures should increase, and you must allocate more free space.

10 Verify that the `/opt` and `/boot` file systems have the required free space for your Symantec Data Loss Prevention installation. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for more information.

Downloading the Oracle 11g software for Linux

You should have received a Symantec Serial Number Certificate with your order that lists a serial number for each of your products. If you did not receive the certificate, contact Symantec Customer Care as described at `http://www.symantec.com/business/support/assistance_care.jsp`. If you have multiple serial numbers , locate the serial number that corresponds to Oracle Standard Edition.

Go to `https://fileconnect.symantec.com` and enter the serial number. Proceed to the list of available downloads and download and extract the following files:

- `Oracle_11.2.0.1.0_Server_Lin.zip`
  This ZIP file contains Oracle 11g Release 2 software (`linux_11gR2_database_1of2.zip`, `linux_11gR2_database_2of2.zip`, and `linux.x64_11gR2_database_Complete.zip`).
- `Oracle_11.2.0.1.0_Server_Installation_Tools_Lin.zip`
  This ZIP file contains the Symantec Data Loss Prevention Oracle database template and database user SQL script (`11g_r2_32_bit_Installation_Tools.tar.gz` and `11g_r2_64_bit_Installation_Tools.tar.gz`).

Installing the Oracle 11g software for Linux

The Enforce Server uses the Oracle thin driver and the Oracle Client. Symantec Data Loss Prevention packages the JAR files for the Oracle thin driver with the Symantec Data Loss Prevention software. But, you must also install the Oracle Client. The Symantec Data Loss Prevention installer needs SQL*Plus to create tables and views on the Enforce Server. Therefore, the Linux user account that is used to install Symantec Data Loss Prevention must be able to access to SQL*Plus.

See "About the Oracle 11g Client software for Linux" on page 32.

Although you install Oracle 11g as the Oracle user, you also need to perform some tasks as the root user. You might find it easier to switch to a dedicated root xterm window instead of changing users. Open two terminal windows; the first is for the Oracle user, the second for the root user. Enter `su - oracle` in the first window; enter `su - root` in the second window. Keep these separate windows open throughout the Oracle installation.

The instructions in this section assume that you are logged on locally to the Linux server and running the X Window System. If you connect to the server remotely, you need a terminal emulator. You also need to set the location where the GUI tools can display their output; you use the export display command to do that. For example:

```
export DISPLAY=ip_address:display_number
```

Note: Refer to the configuration information in the X server management program for the IP address and display number. Typically, the display number is 0.

As you run the GUI tools later, you might get a response similar to the following:

```
X connection to localhost:10.0 broken (explicit kill or server shutdown)
```

Run the export display command again.

To install Oracle 11g Release 2

1. Log on as the Oracle user.

   ```
   su - oracle
   ```

2. Copy the required software installation files or file to `/home/oracle`:

   - For 32-bit systems, copy both `linux_11gR2_database_1of2.zip` and `linux_11gR2_database_2of2.zip`.
   - For 64-bit systems, copy `linux.x64_11gR2_database_Complete.zip`.

3. From `/home/oracle`, unzip the files you copied. For example:

   ```
   unzip linux.x64_11gR2_database_Complete.zip
   ```

   For 32-bit systems, unzip both files.

   You must run the `unzip` command as the Oracle user. If you run it as the root user, then the Oracle user is not able to view the extracted files unless you change the permissions. However, changing the permissions is not advisable from a security standpoint.

4 Go to `/home/oracle/database` and run the installer:

```
./runInstaller -ignoresysprereqs
```

5 On the **Configure Security Updates** panel, de-select **I wish to receive security updates via My Oracle Support**, and click **Next**.

Symantec certifies and provides Oracle Critical Patch Updates for use with Symantec Data Loss Prevention, along with detailed installation instructions. You do not need to receive these updates from Oracle Support.

6 Click **Yes** to confirm that you have not provided an email address.

7 On the **Select Installation Option** panel, select **Install database software only** and click **Next**.

8 On the **Grid Installation Options** panel, select **Single instance database installation** and click **Next**.

9 On the **Select Product Languages** panel, click **Next** to accept English as the default language.

10 On the **Select Database Edition** panel, select **Standard Edition** and click **Next**.

11 On the **Specify Installation Location** panel, enter the following paths in the specified fields, and click **Next**:

- **Oracle Base**: Enter `/opt/oracle`
- **Software Location**: Enter `/opt/oracle/product/11.2.0/db_1`

Note: All example paths in this document use the installation directory `/opt/oracle/product/11.2.0/db_1`. If you specify a different installation directory, substitute the correct path as necessary throughout this document.

12 If this is the first Oracle installation on the server computer, the installer application displays the **Create Inventory** panel. Enter `/opt/oracle/oraInventory` as the inventory path and `oinstall` as the group name, and click **Next**.

The installer may display a warning message recommending that you place the central inventory location outside of the Oracle base directory. You can safely ignore this message for Symantec Data Loss Prevention database installations.

13 On the **Privileged Operating System Groups** panel, click **Next** to grant the Database Administrator and Database Operator privileges to the default dba group.

The installer application performs a prerequisite check and displays the results.

14 On the **Summary** panel, click **Finish** to begin the installation.

The installer application installs the Oracle 11g software on your computer.

15 The installer displays the **Execute Configuration scripts** window, which instructs you to execute two scripts as the root user. From the root xterm window, run the following two scripts:

```
/opt/oracle/oraInventory/orainstRoot.sh
/opt/oracle/product/11.2.0/db_1/root.sh
```

After you run the `/opt/oracle/product/11.2.0/db_1/root.sh` script, you are prompted to enter the full pathname to the local binary directory. Accept the default `/usr/local/bin` directory and press **Enter**.

16 Return to the **Execute Configuration scripts** screen and click **OK**.

17 On the **Finish** panel, click **Close** to exit the installer application.

Creating the Symantec Data Loss Prevention database

Perform the following procedure to create the Symantec Data Loss Prevention database.

Note: If you are installing Oracle 11g on a 64-bit computer in order to migrate an existing 32-bit Symantec Data Loss Prevention database, do not perform this procedure.

See "Migrating from Oracle 10g 32-bit to Oracle 11g 64-bit" on page 58.

To create the Symantec Data Loss Prevention database

1. Set the ORACLE_HOME and ORACLE_SID environment variables for your new installation. Open a command prompt, and enter:

   ```
   export ORACLE_HOME=/opt/oracle/product/11.2.0/db_1
   export ORACLE_SID=protect
   ```

   If you installed Oracle 11g into a different location, substitute the correct directory in this command.

   You may want to add these commands to your user profile configuration so that the ORACLE_HOME and ORACLE_SID environment variables are defined each time you log on. See your Linux documentation for details about setting environment variables.

2. Extract the database template file (`.dbt` file) from the `11g_r2_32_bit_Installation_Tools.tar.gz` or `11g_r2_64_bit_Installation_Tools.tar.gz` file to the `$ORACLE_HOME/assistants/dbca/templates` directory. For example, extract `v11_32_bit_Lnx.dbt` for 32-bit systems or `v11_64_bit_Lnx.dbt` for 64-bit systems.

3. Start the Oracle Database Configuration Assistant to create the Symantec Data Loss Prevention database:

   ```
   $ORACLE_HOME/bin/dbca
   ```

4. On the **Welcome** panel, click **Next**.

5. On the **Operations** panel, select **Create a Database** and click **Next**.

6. On the **Database Templates** panel, select **Oracle 11g Database for Vontu v11 32 bit Lnx** for 32-bit installations, or select **Oracle 11g Database for Vontu v11 64 bit Lnx** for 64-bit installations. Click **Next**.

   Caution: You must use the Symantec Data Loss Prevention template to create the database. Do not use an alternate template or reuse an existing database instance. If you do not use the supplied template, failures can occur when you use Symantec Data Loss Prevention. Failures can also occur later when you try to upgrade the product.

7. On the **Database Identification** panel, set the database name (Global Database Name) and the Oracle System Identifier (SID) by performing the following steps in this order:

   - Enter **protect** in the **Global Database Name** field.

The **SID** field is automatically set to **protect**. Keep the SID and the Global Database Name fields as the same value, "protect."

- Click **Next**.
- Write down the database name and SID for later use when you install the Symantec Data Loss Prevention software.

8. On the **Management Options** panel, perform the following steps in order:
   - Deselect **Configure Enterprise Manager**.
   - Select the **Automatic Maintenance Tasks** tab and deselect **Enable automatic maintenance tasks**.
   - Click **Next**.
9. On the **Database Credentials** panel, perform the following steps in order:
   - Select **Use the Same Administrative Password for All Accounts**.
   - Enter a password in the **Password** field.
   - Re-enter the same password in the **Confirm Password** field.
   - Click **Next**.

   Follow these guidelines to create acceptable passwords:

   - Passwords cannot contain quotation marks.
   - Passwords are not case-sensitive .
   - Passwords must begin with an alphabetic character.
   - Passwords can only contain alphanumeric characters. Do not use underscore (_), the dollar sign ($), and pound sign (#) for your password, because Oracle interprets these symbols differently than other systems.
   - A password cannot be an Oracle-reserved word such as `SELECT`.

   If you enter a password that does not meet these guidelines, Oracle keeps prompting for a password. You must enter a password. Do not kill the Oracle Database Configuration Assistant.

   Note: You can optionally use different passwords for each user account type. The various user account types are SYS, SYSTEM, DBSNMP, and SYSMAN.

10 On the **Database File Locations** panel, accept the default selection, **Use Database File Locations from Template**, and click **Finish**.

The Database Configuration Assistant displays a **Confirmation** window with a summary of the database configuration.

11 Click **OK** on the **Confirmation** window to create the database.

The database creation can take up to 20 minutes to complete. If the database creation process fails or hangs, check the Oracle Database Configuration Assistant logs (located in the `$ORACLE_HOME/cfgtoollogs/dbca/`*`SID`* directory) for errors (for example, `/opt/oracle/product/11.2.0/db_1/cfgtoollogs/dbca/protect`).

When the database creation process is complete, another **Database Configuration Assistant** window opens and displays the database details.

12 Click **Exit**.

Creating the TNS Listener on Linux

Perform the following procedure to create a TNS listener for the Symantec Data Loss Prevention database.

To create the TNS Listener

1 Start the Oracle Net Configuration Assistant:

```
$ORACLE_HOME/bin/netca
```

2 On the **Welcome** panel, select **Listener configuration** and click **Next**.

3 On the **Listener Configuration, Listener** panel, select **Add** and click **Next**.

4 On the **Listener Configuration, Listener Name** panel, enter a listener name and click **Next**.

Note: Use the default listener name, LISTENER, unless you must use a different name.

5 On the **Listener Configuration, Select Protocols** panel, select the **TCP** protocol and click **Next**.

6 On the **Listener Configuration, TCP/IP Protocol** panel, select **Use the standard port number of 1521** and click **Next**.

7 On the **Listener Configuration, More Listeners?** panel, select **No** and click **Next**.

8. On the **Listener Configuration Done** panel, click **Next**.
9. Leave the Oracle Net Configuration Assistant open to configure the Local Net Service Name.

Configuring the local net service name

Perform the following procedure to configure the Local Net Service Name for the Symantec Data Loss Prevention database.

To configure the local net service name

1. If the Oracle Net Configuration Assistant is not already running, start it:

   ```
   $ORACLE_HOME/bin/netca
   ```

2. On the **Welcome** panel, select **Local Net Service Name configuration** and click **Next**.
3. On the **Net Service Name Configuration** panel, select **Add** and click **Next**.
4. On the **Net Service Name Configuration, Service Name** panel, enter "protect" in the **Service Name** field and click **Next**.
5. On the **Net Service Name Configuration, Select Protocols** panel, select **TCP** and click **Next**.
6. On the **Net Service Name Configuration, TCP/IP Protocol** panel:
   - Enter the IP address of the Oracle server computer in the **Host name** field.
   - Select **Use the standard port number of 1521** (the default value).
   - Click **Next**.
7. On the **Net Service Name Configuration, Test** panel, select **No, do not test** and click **Next**.

   Do not test the service configuration, because the listener has not yet started.
8. On the **Net Service Name Configuration, Net Service Name** panel, select accept the default name of "protect" and click **Next**.
9. On the **Net Service Name Configuration, Another Net Service Name?** panel, select **No** and click **Next**.
10. On the **Net Service Name Configuration Done** panel, select **Next**.
11. Click **Finish** to exit the Oracle Net Configuration Assistant.

Verifying the Symantec Data Loss Prevention database

After creating the Symantec Data Loss Prevention database, you should verify that it was created correctly.

To verify that the database was created correctly

1. Open a command prompt and start SQL*Plus:

   ```
   $ORACLE_HOME/bin/sqlplus /nolog
   ```

2. Log on as the SYS user:

   ```
   SQL> connect sys/password@protect as sysdba
   ```

   Where `password` represents the SYS password.

3. Run the following query:

   ```
   SQL> SELECT * FROM v$version;
   ```

4. Make sure that the output from the query contains the following information, which identifies the software components as version 11.2.0.1.0. For a 32-bit installation, the output should read:

```
BANNER
---------------------------------------------------------------------------

Oracle Database 11g Release 11.2.0.1.0 - 32bit Production
PL/SQL Release 11.2.0.1.0 - Production
CORE    11.2.0.1.0      Production
TNS for Linux: Version 11.2.0.1.0 - Production
NLSRTL Version 11.2.0.1.0 - Production
```

   For a 64-bit installation, the output should read:

```
BANNER
---------------------------------------------------------------------------

Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
PL/SQL Release 11.2.0.1.0 - Production
CORE    11.2.0.1.0      Production
TNS for Linux: Version 11.2.0.1.0 - Production
NLSRTL Version 11.2.0.1.0 - Production
```

5. Run the following command to describe the `dba_tablespaces` view:

```
SQL> describe dba_tablespaces;
```

6. Check that the output contains the following information:

```
RETENTION     VARCHAR2(11)
BIGFILE       VARCHAR2(3)
```

7. Exit SQL*Plus:

```
SQL> exit
```

Creating the Oracle user account for Symantec Data Loss Prevention

Perform the following procedure to create an Oracle user account and name it “protect.”

To create the new Oracle user account named protect

1. Extract the SQL script file, `oracle_create_user.sql`, from the `11g_r2_32_bit_Installation_Tools.tar.gz` or `11g_r2_64_bit_Installation_Tools.tar.gz` file to a local directory.
2. Open a command prompt and go to the directory where you extracted the `oracle_create_user.sql` file.
3. Start SQL*Plus:

   ```
   sqlplus /nolog
   ```

4. Run the `oracle_create_user.bat` script:

   ```
   SQL> @oracle_create_user.sql
   ```

5. At the **Please enter the password for sys user** prompt, enter the password for the SYS user.
6. At the **Please enter sid** prompt, enter "protect."
7. At the **Please enter required username to be created** prompt, enter "protect."
8. At the **Please enter a password for the new username** prompt, enter a new password.

   Store the password in a secure location for future use. You will need this password to install Symantec Data Loss Prevention. If you need to change the password after you install Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention Administration Guide* for instructions.

Locking the DBSNMP Oracle user account

To maintain security, you should lock the Oracle DBSNMP user account.

To lock the Oracle DBSNMP user account

1. Open a command prompt and start SQL*Plus:

   ```
   sqlplus /nolog
   ```

2. Log on as the SYS user:

   ```
   SQL> connect sys/password as sysdba
   ```

   Where `password` is the SYS password.

3. Lock the DBSNMP user account:

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

4. Exit SQL*Plus:

   ```
   SQL> exit
   ```

Chapter 4

Upgrading a Symantec Data Loss Prevention database to Oracle 11g on Linux

This chapter includes the following topics:

- Upgrading an Oracle 10g database on Linux
- Removing the Oracle 10g listener on Linux
- Upgrading from Oracle 10g to Oracle 11g
- Configuring the upgraded 11g database

Upgrading an Oracle 10g database on Linux

If you have an existing Symantec Data Loss Prevention database that runs on Oracle 10g, you can choose to continue using that database, or you can upgrade the 10g database to use Oracle 11g. Follow these steps, in order, to upgrade an Oracle 10g Symantec Data Loss Prevention database to use Oracle 11g:

Table 4-1 Upgrading a Symantec Data Loss Prevention database from Oracle 10g to Oracle 11g

Step	Action	Description
Step 1	Delete the existing Oracle 10g listener.	See "Removing the Oracle 10g listener on Linux" on page 50.

Table 4-1 Upgrading a Symantec Data Loss Prevention database from Oracle 10g to Oracle 11g *(continued)*

Step	Action	Description
Step 2	Install the Oracle 11g software and use the Oracle Database Upgrade Assistant to upgrade the Symantec Data Loss Prevention database.	See "Upgrading from Oracle 10g to Oracle 11g" on page 25.
Step 3	Modify the configuration of the upgraded Symantec Data Loss Prevention database.	See "Configuring the upgraded 11g database" on page 28.
Step 4	Install the Oracle Critical Patch Update (CPU).	The latest *Oracle 11g Release 2 Critical Patch Update Guide* explains how to download and apply the latest CPU for Oracle.

Removing the Oracle 10g listener on Linux

Perform the following procedure to delete the existing Oracle 10g TNS listener before you upgrade to Oracle 11g.

To remove the Oracle 10g listener on Linux

1. Start the Oracle Net Configuration Assistant:

   ```
   $ORACLE_HOME/bin/netca
   ```

2. On the **Welcome** panel, select **Listener configuration** and click **Next**.
3. On the **Listener Configuration, Listener** panel, select **Delete** and click **Next**.
4. On the **Listener Configuration, Select Listener** panel, select the name of the listener you want to delete, and click **Next**.
5. If the listener is running, the Net Configuration Assistant asks if you want to stop and delete the selected listener. Select **Yes**.
6. On the **Listener Configuration, Listener Deleted** panel, select **Next**.
7. On the **Listener Configuration Done** panel, select **Next**.
8. On the **Welcome** panel, select **Finish** to exit the Net Configuration Assistant.

Upgrading from Oracle 10g to Oracle 11g

If you have an existing Symantec Data Loss Prevention database running on Oracle 10g and you want to upgrade that database to run on Oracle 11g, follow these steps to perform the upgrade.

To upgrade an existing Symantec Data Loss Prevention database to Oracle 11g

1. Shut down the Enforce Server that accesses the Oracle 10g database.

   See the *Symantec Data Loss Prevention System Administration Guide* for information about shutting down Symantec Data Loss Prevention servers.

2. Download and unzip the Oracle 11g software to the server computer that is running your Oracle 10g database.

   See "Downloading the Oracle 11g software for Linux" on page 37.

3. Log on as the Oracle user.

   ```
   su - oracle
   ```

4. Go to `/home/oracle/database` and run the Oracle 11g installer:

   ```
   ./runInstaller -ignoresysprereqs
   ```

5. On the **Configure Security Updates** panel, de-select **I wish to receive security updates via My Oracle Support**, and click **Next**.
6. Click **Yes** to confirm that you have not provided an email address.
7. On the **Select Installation Option** panel, select **Upgrade an existing database** and click **Next**.
8. On the **Select Product Languages** panel, click **Next** to accept English as the default language.
9. On the **Select Database Edition** panel, select **Standard Edition** and click **Next**.
10. On the **Specify Installation Location** panel, enter the following paths in the specified fields, and click **Next**:
    - **Oracle Base**: Enter `/opt/oracle`
    - **Software Location**: Enter `/opt/oracle/product/11.2.0/db_1`

    Note: All example paths in this document use the installation directory `/opt/oracle/product/11.2.0/db_1`. If you specify a different installation directory, substitute the correct path as necessary throughout this document.

11 On the **Privileged Operating System Groups** panel, click **Next** to grant the Database Administrator and Database Operator privileges to the default dba group.

12 The installer application performs a prerequisite check and displays the results. If the installer indicates that the system failed when checking kernel parameters, click **Fix and Check again** and run the indicated scripts as the root user.

13 On the **Summary** panel, click **Finish** to begin the installation.

The installer application installs the Oracle 11g software to your computer.

14 On the **Finish** panel, click **Close** to exit the installer application.

The installer upgrades the Oracle 10g software and then starts the Oracle Net Configuration Assistant.

15 On the Oracle Net Configuration Assistant **Welcome** panel, deselect **Perform typical configuration** and click **Next**.

16 On the **Listener Configuration, Listener Name** panel, enter a listener name and click **Next**.

Note: Use the default listener name, LISTENER, unless you must use a different name.

17 On the **Listener Configuration, Select Protocols** panel, select the **TCP** protocol and click **Next**.

18 On the **Listener Configuration, TCP/IP Protocol** panel, select **Use the standard port number of 1521** and click **Next**.

19 On the **Listener Configuration, More Listeners?** panel, select **No** and click **Next**.

20 On the **Listener Configuration Done** panel, click **Next**.

21 On the **Naming Methods Configuration** panel, select **No** and click **Next**.

22 Click **Finish** after the network configuration completes.

The installer loads the Database Upgrade Assistant.

23 On the **Welcome** panel of the Database Upgrade Assistant, click **Next**.

24 On the **Select Database** panel:

- Select the PROTECT database from the list of available databases.
- Enter the password to the sys account in the **Password** field.

- Click **Next** to continue.

The upgrade assistant gathers information about the PROTECT database.

25 The upgrade assistant may display a **Warnings** window that lists warning conditions that were determined during the upgrade check. If the window indicates that you should purge the recycle bin, start SQL*Plus and enter the `purge dba_recyclebin;` command. Then click **Yes** to continue with the upgrade. You can view review other warning conditions at a later time by examining the `$ORACLE_HOME/cfgtoollogs/dbua/protect/upgrade1/PreUpgradeResults.html` file.

26 On the **Upgrade Options** panel:

- Select **Backup database** and specify a backup directory if you do not have a current backup of the PROTECT database.
- Ensure that **Recompile invalid objects at the end of the upgrade** is selected.
- Click **Next** to continue.

27 On the **Move Database Files** panel:

- Select **Move Database Files during Upgrade**.
- Select **File System**.
- Click **Next** to continue.

28 On the **Database File Locations** panel, click **Next** to accept the default location for the database files.

29 On the **Recovery and Diagnostic Locations** panel, click **Next** to accept the default destinations.

30 On the **Management Options** panel, click **Next** to accept the default configuration.

31 On the **Summary** panel, click **Finish** to begin the database upgrade.

The Database Upgrade Assistant displays a **Progress** window while it performs the upgrade.

At the **Progress** window you may see the error, `Identifier SYS.DBMS_JAVA must be declared`. You can safely ignore this error by clicking **Ignore**.

32 On the **Upgrade Result** panel, click **Close**. The Database Upgrade Assistant displays a document summary. Depending on your database environment, the summary may display errors such as `00201: identifier SYS.DBMS_JAVA must be declared`, which can be ignored.

33 The Database Upgrade Assistant displays the **Execute Configuration scripts** window, which instructs you to execute scripts as the root user. From the root xterm window, run the following script:

```
/opt/oracle/product/11.2.0/db_1/root.sh
```

When you run `/opt/oracle/product/11.2.0/db_1/root.sh`, the script finds that the `dbhome`, `oraenv`, and `coraenv` files already exist in the `/usr/local/bin` directory. Press `Y` to overwrite each file in its location.

34 After you finish upgrading the Oracle 10g database to Oracle 11g, change the ORACLE_HOME environment variable to point to your new installation. Open a command prompt, and enter:

```
export ORACLE_HOME=/opt/oracle/product/11.2.0/db_1
```

If you installed Oracle 11g into a different location, substitute the correct directory in this command.

Also update your user profile configuration to automatically set the ORACLE_HOME environment variable each time you log on.

Configuring the upgraded 11g database

After you finish upgrading the Oracle 10g database to Oracle 11g, perform these steps to alter the database password lifetime and disable certain automated maintenance tasks.

To configure the upgraded database

1 Copy the SQL script file, `post_v11_upgrade_11gr2.sql`, from the `/opt/Vontu/Protect/install/sql` directory of a Symantec Data Loss Prevention version 11 installation to a local directory.

2 Open a command prompt and go to the directory where you extracted the `post_v11_upgrade_11gr2.sql` script.

3 Start SQL*Plus:

```
$ORACLE_HOME/bin/sqlplus /nolog
```

4 Log on as the SYS user:

```
SQL> connect sys/password as sysdba
```

Where *`password`* represents the SYS password.

5. Execute the following command to remove the password lifetime limit:

   ```
   alter profile default limit password_life_time unlimited;
   ```

6. Enter the following commands to disable automated maintenance tasks:

   ```
   begin
      dbms_auto_task_admin.disable(
         client_name => 'auto optimizer stats collection',
         operation => NULL,
         window_name => NULL
      );

      dbms_auto_task_admin.disable(
         client_name => 'auto space advisor',
         operation => null,
         window_name => null
      );

      dbms_auto_task_admin.disable(
         client_name => 'sql tuning advisor',
         operation => null,
         window_name => null
      );
   end;
   ```

7. Verify that the automated maintenance tasks are disabled by executing the following command:

   ```
   select client_name, status from dba_autotask_client;
   ```

8. Execute these commands to modify the database initialization parameters:

   ```
   alter system set memory_target = 1536m scope=spfile;
   alter system set memory_max_target = 1536m scope=spfile;
   alter system set sga_max_size = 0 scope=spfile;
   alter system set sga_target = 0 scope=spfile;
   alter system set compatible = '11.2.0.1.0' scope=spfile;
   ```

9. Execute the `utlrp.sql` script to recompile any invalid objects:

   ```
   @$ORACLE_HOME/rdbms/admin/utlrp.sql
   ```

10 Execute the post upgrade script for the Symantec Data Loss Prevention database:

```
@post_v11_upgrade_11gr2.sql
```

If the post upgrade script is not in the current working directory, specify the full path to the script.

11 Exit SQL*Plus:

```
exit
```

12 Restart the Enforce Server.

Chapter 5

Migrating from a 32-bit Oracle 10g to 64-bit Oracle 11g database

This chapter includes the following topics:

- About migrating Oracle from a 32-bit to 64-bit Oracle database
- Migrating from Oracle 10g 32-bit to Oracle 11g 64-bit
- Migrating 32-bit Oracle database files

About migrating Oracle from a 32-bit to 64-bit Oracle database

Migrating from Oracle 10g (32-bit) to Oracle 11g (64-bit) requires that you use two separate server computers during the migration process. You begin using the existing 32-bit server computer, where you install a 32-bit version of Oracle 11g and upgrade the Oracle 10g database files. On the 64-bit server computer, you install Oracle 11g without creating a dedicated Symantec Data Loss Prevention database. The migration process is completed by copying the upgraded database files from the 32-bit computer to the correct locations on the 64-bit computer.

See “Migrating from Oracle 10g 32-bit to Oracle 11g 64-bit” on page 58.

Oracle migration is frequently performed as part of a larger process to migrate the Enforce Server to a new computer. If you are migrating the Enforce Server from a 32-bit computer to a 64-bit computer, also refer to the *Symantec Data Loss Prevention System Administration Guide* for additional steps that you must perform to migrate Enforce Server configuration data.

Migrating from Oracle 10g 32-bit to Oracle 11g 64-bit

The instructions for migrating the Oracle database from a 32-bit server computer to a 64-bit server computer apply to both Windows and Linux systems. During the migration process, you will use many of the same instructions provided earlier in this document. For example, you will use earlier instructions to perform the database upgrade on the 32-bit server computer. The migration instructions direct you to the correct procedures.

Table 5-1 Migrating from Oracle 10g 32-bit to Oracle 11g 64-bit

Step	Action	Description
Step 1	Upgrade Oracle 10g to Oracle 11g on the 32-bit server computer.	On the same 32-bit server computer that hosts your Oracle 10g installation, install Oracle 11g and upgrade the Oracle 10g database. Make sure that you install Oracle 11g in its own, dedicated Oracle home directory. Accepting the default Oracle 11g installation location creates an Oracle home directory that is separate from the home directory that was used with Oracle 10g. See "Upgrading an Oracle 10g database on Windows" on page 23. See "Upgrading an Oracle 10g database on Linux" on page 49.

Table 5-1 Migrating from Oracle 10g 32-bit to Oracle 11g 64-bit *(continued)*

Step	Action	Description
Step 2	Install Oracle 11g on the 64-bit server computer.	On the 64-bit server computer, install Oracle 11g without creating a database. Follow the instructions in this guide for installing Oracle 11g on your platform, but do not perform Step 4: Create the Symantec Data Loss Prevention database. See "Installing the Oracle 11g software for Windows" on page 12. See "Installing the Oracle 11g software for Linux" on page 37. If you already installed Oracle 11g with a database on the 64-bit server computer, use the Oracle Database Configuration Assistant to remove the database.
Step 3	Create the TNS listener on the 64-bit server computer.	See "Creating the TNS Listener on Windows" on page 16. See "Creating the TNS Listener on Linux" on page 43.
Step 4	Migrate 32-bit database files to the 64-bit server computer.	On the 32-bit server computer, generate an Oracle 11g `pfile` from the `spfile`. Then copy all Oracle 11g database files from their locations on the 32-bit server computer to the same locations on the 64-bit server computer. See "Migrating 32-bit Oracle database files" on page 60.
Step 5	Install the Oracle Critical Patch Update (CPU) on the 64-bit server computer.	The latest *Oracle 11g Release 2 Critical Patch Update Guide* explains how to download and apply the latest CPU for Oracle.

Migrating 32-bit Oracle database files

Follow this procedure to migrate the necessary Oracle database files from the 32-bit Oracle 11g installation to the 64-bit Oracle 11g installation.

Migrating 32-bit Oracle database files

1. On the 32-bit server computer, open a command prompt and start SQL*Plus:

   ```
   sqlplus /nolog
   ```

2. Log on as the SYS user:

   ```
   SQL> connect sys/password as sysdba
   ```

   Where *password* represents the SYS password.

3. Create a `pfile` from the `spfile`. On Windows platforms, enter:

```
SQL> create pfile='c:\oracle\admin\protect\pfile\init.ora' from spfile;
```

   On Linux, platforms, enter:

```
SQL> create pfile='/opt/oracle/admin/protect/pfile/init.ora' from spfile;
```

4. Shut down the Oracle database before copying files:

   ```
   SQL> shutdown immediate
   ```

5. Exit SQL*Plus:

   ```
   SQL> exit
   ```

6 Copy the Oracle database files from the 32-bit server computer to the 64-bit server computer. Always ensure that you copy the files to the same directory location on the 64-bit server destination.

For Windows platforms, copy the following files and directories to the corresponding directory on the 64-bit server computer.

Location	**Description**
`c:\oracle\oradata`	Copy the entire `oradata` directory to migrate database, log, and control files.
`c:\oracle\product\11.2.0\db_1\database\PWDprotect.ora`	Copy the remote password file.
`c:\oracle\admin`	Copy the entire `admin` directory to migrate the `pfile` directory struture.
`flash_recovery_area\*`	If you configured disk-based backup and recovery for Oracle, copy the complete contents of the `flash_recovery_area\` directory.

If you installed into a different directory, replace `c:\oracle\product\11.2.0\db_1` with the correct installation directory.

For Linux platforms, copy the following files and directories to the corresponding directories on the 64-bit server computer:

Location	**Description**
`/opt/oracle/oradata`	Copy the entire `oradata` directory to migrate database, log, and control files.
`/opt/oracle/product/11.2.0/db_1/dbs/orapwprotect`	Copy the remote password file.
`/opt/oracle/admin`	Copy the entire `admin` directory to migrate the `pfile` directory struture.
`flash_recovery_area/*`	If you configured disk-based backup and recovery for Oracle, copy the complete contents of the `flash_recovery_area/` directory.

For Linux platforms, also ensure that the copied files have the same permissions as the source files, and that they are owned by the same “oracle” user and “oinstall” group as the source files.

7. If 64-bit server computer uses a different directory structure for the Oracle installation, you must manually edit the `init.ora` file that your created to specify the correct location for directories on the 64-bit server computer. For example, if the 32-bit Oracle software was installed on the `c:\` drive and the 64-bit Oracle software was installed on the `d:\` drive, edit `c:\oracle\product\11.2.0\db_1\admin\protect\pfile\init.ora` and change all drive references from `c:\` to `d:\`.

8. On the 64-bit server computer, open a command prompt or terminal window and set the ORACLE_HOME and ORACLE_SID environment variables. For example, on Windows enter:

   ```
   set ORACLE_HOME=c:\oracle\product\11.2.0\db_1
   set ORACLE_SID=protect
   ```

   On Linux enter:

   ```
   export ORACLE_HOME=/opt/oracle/product/11.2.0/db_1
   export ORACLE_SID=protect
   ```

9. If you did not re-create the TNS listener on the 64-bit server computer, you must do so now.

   See “Creating the TNS Listener on Windows” on page 16.

   See “Creating the TNS Listener on Linux” on page 43.

10 On the 64-bit server computer, create a new Oracle service using the `pfile` that you migrated. The method for completing this step is different for Windows and Linux platforms.

For Windows platforms only, create a new Oracle service on the 64-bit server computer using the `oradim` utility. Enter the following from a command prompt:

```
oradim -new -sid protect -startmode auto
     -pfile c:\oracle\admin\protect\pfile\init.ora
```

For Linux platforms, start SQL*Plus and enter the commands as follows to use the migrated `pfile`:

```
sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> shutdown immediate
SQL> startup pfile=/opt/oracle/admin/protect/pfile/init.ora
```

The `shutdown immediate` command may display the error, `ORA-01034: ORACLE not available`. You can ignore this error. Starting up the database using the above command connects to an idle database instance.

11 Start SQL*Plus if it is not already running, and generate a `spfile`. For Windows platforms, enter:

```
sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> create spfile from pfile='c:\oracle\admin\protect\pfile\init.ora';
```

For Linux platforms, enter:

```
sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> create spfile from pfile='/opt/oracle/admin/protect/pfile/init.ora';
```

12 Shutdown the database and start it in upgrade mode:

```
SQL> shutdown immediate
SQL> startup upgrade
```

13 Run the `utlip.sql` and `utlrp.sql` scripts. For Windows, enter:

```
SQL> @c:\oracle\product\11.2.0\db_1\rdbms\admin\utlip.sql
SQL> @c:\oracle\product\11.2.0\db_1\rdbms\admin\utlrp.sql
```

For Linux, enter:

```
SQL> @/opt/oracle/product/11.2.0/db_1/rdbms/admin/utlip.sql
SQL> @/opt/oracle/product/11.2.0/db_1/rdbms/admin/utlrp.sql
```

14 Restart Oracle using the commands:

```
SQL> shutdown immediate
SQL> startup
```

15 Exit SQL*Plus:

```
SQL> exit
```

Index