

# Symantec™ Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide

Versions 14.6–15.5

Last updated: 21 December 2018



# Symantec™ Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide

Documentation version: 15.5

## Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, CloudSOC, Blue Coat, the Symantec Logo, the Checkmark Logo, the Blue Coat logo, and the Shield Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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 Legal Notice Appendix to this Documentation or TPIP ReadMe File 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 DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. 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>

# Contents

Chapter 1	About this guide .....	6
	About updates to the <i>Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide</i> .....	6
Chapter 2	Preparing to install or upgrade to Oracle 12c Standard Edition 2 Release 2 .....	7
	About installing or upgrading to Oracle 12c Standard Edition 2 Release 2 .....	7
	About deploying Oracle to AWS .....	8
	Before upgrading to Oracle 12c Standard Edition 2 Release 2 .....	8
	Downloading the Oracle 12c SE software .....	9
	Set privileges for the Oracle user .....	10
	Preparing the upgrade software .....	10
	Follow the upgrade path for your hardware profile .....	11
Chapter 3	Installing Oracle 12c Standard Edition 2 Release 2 on Windows .....	12
	Steps to install Oracle 12c SE2 on Windows .....	12
	Installing Oracle 12c SE2 on Windows .....	13
	Installing Oracle 12.2.0.1 on Windows .....	13
	Creating the Symantec Data Loss Prevention database on Windows .....	15
	Creating the TNS Listener on Windows .....	16
	Configuring the local net service name on Windows .....	19
	Creating the Oracle user account for Symantec Data Loss Prevention (Windows) .....	20
	Verifying the Symantec Data Loss Prevention database .....	21
Chapter 4	Installing Oracle 12c Standard Edition 2 Release 2 on Linux .....	23
	Steps to install Oracle 12c SE2 on Linux .....	23
	Performing the preinstallation steps .....	24

	Preparing the Linux environment .....	24
	Installing Oracle 12c SE2 on Linux .....	26
	Installing Oracle 12.2.0.1 on Linux systems .....	26
	Creating the Symantec Data Loss Prevention database on Linux .....	29
	Creating the TNS Listener on Linux .....	30
	Configuring the local net service name on Linux .....	33
	Verifying tnsnames.ora contents .....	34
	Verifying the Symantec Data Loss Prevention database .....	35
	Creating the Oracle user account for Symantec Data Loss Prevention (Linux) .....	36
	Configuring automatic startup and shutdown of the database .....	37
Chapter 5	Upgrading to Oracle 12c Standard Edition 2 Release 2 .....	39
	Upgrading from Oracle 11g SE1 or Oracle 11g SE on servers with two (or fewer) CPU sockets .....	39
	Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation .....	40
	Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation .....	41
	Upgrading to Oracle 12.2.0.1 .....	42
Chapter 6	Migrating the Oracle database to supported hardware .....	46
	About migrating the Oracle database to supported hardware .....	47
	Workflow for migrating the Oracle database to supported hardware .....	47
	Confirm the schema row count before the export (Windows) .....	49
	Exporting a database schema (Windows) .....	50
	Confirm the schema row count before the export (Linux) .....	51
	Exporting a database schema (Linux) .....	52
	Importing a database backup schema on Windows .....	53
	Confirm the schema row count after the import (Windows) .....	54
	Import the database backup schema on Linux .....	55
	Confirm the schema row count after the import (Linux) .....	56
	Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database .....	57

# About this guide

This chapter includes the following topics:

- [About updates to the Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide](#)

## ***About updates to the Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide***

This guide is occasionally updated as new information becomes available. You can find the latest version of the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide* at the following link to the Symantec Support Center article:

<http://www.symantec.com/docs/DOC10713>.

Subscribe to the article at the Support Center to be notified when there are updates.

# Preparing to install or upgrade to Oracle 12c Standard Edition 2 Release 2

This chapter includes the following topics:

- [About installing or upgrading to Oracle 12c Standard Edition 2 Release 2](#)
- [About deploying Oracle to AWS](#)
- [Before upgrading to Oracle 12c Standard Edition 2 Release 2](#)
- [Follow the upgrade path for your hardware profile](#)

## About installing or upgrading to Oracle 12c Standard Edition 2 Release 2

You can use Oracle 12c Standard Edition 2 Release 2 (12c SE2 R2 [12.2.0.1]) with Symantec Data Loss Prevention 14.6 through 15.5 for new installations and upgrades.

---

**Note:** Oracle 12c Standard Edition 1 (12.1.0.2) is not supported.

---

Symantec supports Oracle 11g until December 2020 if you purchased the Extended Support plan through Oracle. If you did not purchase the Extended Support plan, Symantec ended support on 25 September 2018. Symantec recommends that you upgrade to Oracle Database

12c Standard Edition 2 Release 2 to continue to receive bug fixes and security patches in the future.

You can download the Symantec-licensed version of Oracle 12c SE2 and use this guide to install or upgrade based on your Symantec Data Loss Prevention implementation.

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 or 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 12c Database Client software, see the platform-specific documentation from Oracle Corporation, available from the Oracle Documentation Library at <https://docs.oracle.com/database/122/nav/install-and-upgrade.htm>.

---

**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* available here:

<http://www.symantec.com/docs/DOC9261>

---

## About deploying Oracle to AWS

You can deploy the Oracle database server or Oracle RDS on Amazon Web Services (AWS). You do not have to modify the servers or perform any special configurations to deploy the Oracle database Server on AWS. For deploying Oracle RDS on AWS, you need to configure TLS as described in the Support Center article “[About securing communications between the Enforce Server and Amazon RDS for Oracle](https://www.symantec.com/docs/TECH252583)” at <https://www.symantec.com/docs/TECH252583>.

See the *Symantec Data Loss Prevention Deployment Guide for Amazon Web Services* for more information.

<https://www.symantec.com/docs/DOC9520>

## Before upgrading to Oracle 12c Standard Edition 2 Release 2

Prepare for the Oracle upgrade by completing the following:

1. Back up the Oracle database.

If the upgrade fails you can use a backup to restore your system. Refer to the *Symantec Symantec Data Loss Prevention System Maintenance Guide* for instructions on backing up your database, available here:

<http://www.symantec.com/docs/DOC9267>

2. Upgrade to Symantec Data Loss Prevention version 14.6, 15.0, 15.1, or 15.5.

Refer to the *Symantec Data Loss Prevention Upgrade Guide* available here:

<http://www.symantec.com/docs/DOC9258>

3. Download Oracle 12.2.0.1 database files.

See “[Downloading the Oracle 12c SE software](#)” on page 9.

## Downloading the Oracle 12c SE software

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 Support as described at [https://support.symantec.com/en\\_US/contact-support.html](https://support.symantec.com/en_US/contact-support.html).

Go to [Symantec Software Downloads](#) and enter the serial number. Proceed to the list of available downloads and download and extract the appropriate files. [Table 2-1](#) lists the files you download.

**Table 2-1** Oracle 12.2.0.1 files to download

File name	Description
For Windows, 12.2.0.1_64_bit_Installation_Tools.zip	<p>These ZIP files contain the Oracle database template, the database user SQL script, and the response (.rsp) files, which you use during the installation and configuration of Oracle 12.2.0.1.</p> <p>If you are using Symantec Data Loss Prevention 14.6 or 15.0, you can download these ZIP files at Symantec Software Downloads directly.</p> <p>If you are using Symantec Data Loss Prevention 15.1 or 15.5, these files are available in the Platform ZIP files:</p> <ul style="list-style-type: none"> <li>■ Windows: Symantec_DLP_15.5_Platform_Win-IN.zip</li> <li>■ Linux: Symantec_DLP_15.5_Platform_Lin-IN.zip</li> </ul>
For Linux, 12.2.0.1_64_bit_Installation_Tools.tar.gz	

**Table 2-1** Oracle 12.2.0.1 files to download (*continued*)

File name	Description
For Windows, Oracle_12.2.0.1.0_Server_Win64_1of2 and Oracle_12.2.0.1.0_Server_Win64_2of2  For Linux, Oracle_12.2.0.1.0_Server_Lin64_1of2.zip and Oracle_12.2.0.1.0_Server_Lin64_2of2.zip	This ZIP file contains the Oracle server.
For Windows, Oracle_12.2.0.1.0_Client_Win64.zip  For Linux, Oracle_12.2.0.1.0_Client_Lin64.zip	This ZIP file contains the Oracle Client (SQL*Plus and Database Utilities). If you implement a three-tier installation, you must install the Oracle Client on the Enforce Server.  See <a href="#">“About installing or upgrading to Oracle 12c Standard Edition 2 Release 2”</a> on page 7.

## Set privileges for the Oracle user

You must set privileges for the Oracle user if you are currently running Symantec Data Loss Prevention 14.6 MP2 through 15.5. Set privileges before you upgrade Symantec Data Loss Prevention.

**Complete the following to set privileges for the Oracle user on Symantec Data Loss Prevention:**

- 1 Stop all Symantec Data Loss Prevention services.
- 2 Grant select on v\_\$version to protect; (or to your schema user) as sysdba user:

```
sqlplus sys/[sysdba password] as sysdba

Grant select on v_$version to protect;
```

## Preparing the upgrade software

The steps to prepare the Symantec Data Loss Prevention upgrade software if difference depending on the Symantec Data Loss Prevention version.

If you are updating to 15.0 or 15.0 MP1, copy the upgrade file to the `\SymantecDLP\Protect\updates` directory.

The Symantec Data Loss Prevention version 15.0 file is `15.0_Upgrader_Windows.jar`. The Symantec Data Loss Prevention version 15.0 MP1 file is `15.0.01_Upgrader_Windows.jar`.

If you are updating to 15.1 or later, install the new version where the existing version is running. See the *Symantec Data Loss Prevention Upgrade Guide* available at the Symantec Support Center:

<https://www.symantec.com/docs/DOC10602>.

## Follow the upgrade path for your hardware profile

Upgrade paths are unique depending on your database server hardware. [Table 2-2](#) describes scenarios you may be using and provides links where you can go for steps to upgrade to Oracle Database 12c Standard Edition 2.

**Table 2-2** Oracle version and hardware profile

Oracle version	Hardware profile	More information
Oracle 11g SE1 or Oracle 11g SE	Servers with two (or fewer) CPU sockets	See <a href="#">“Upgrading from Oracle 11g SE1 or Oracle 11g SE on servers with two (or fewer) CPU sockets”</a> on page 39.
Oracle 11g SE	Servers with more than two CPU sockets on a two-tier installation	See <a href="#">“Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation”</a> on page 40.
	Servers with more than two CPU sockets on a single-tier installation	See <a href="#">“Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation”</a> on page 41.

# Installing Oracle 12c Standard Edition 2 Release 2 on Windows

This chapter includes the following topics:

- [Steps to install Oracle 12c SE2 on Windows](#)
- [Installing Oracle 12c SE2 on Windows](#)
- [Creating the Symantec Data Loss Prevention database on Windows](#)
- [Creating the TNS Listener on Windows](#)
- [Configuring the local net service name on Windows](#)
- [Creating the Oracle user account for Symantec Data Loss Prevention \(Windows\)](#)
- [Verifying the Symantec Data Loss Prevention database](#)

## Steps to install Oracle 12c SE2 on Windows

[Installing Oracle 12c SE2 on Windows](#) provides the Oracle 12c installation process. You can find additional detail for each step of the process as indicated in the table.

**Table 3-1** Oracle 12c Standard Edition 2 Release 2 installation overview

Step	Action	More information
1	Install Oracle 12c SE2.	See <a href="#">“Installing Oracle 12c SE2 on Windows”</a> on page 13.

**Table 3-1** Oracle 12c Standard Edition 2 Release 2 installation overview (*continued*)

Step	Action	More information
2	Create the Symantec Data Loss Prevention database.	See <a href="#">“Creating the Symantec Data Loss Prevention database on Windows”</a> on page 15.
3	Create the database listener.	See <a href="#">“Creating the TNS Listener on Windows”</a> on page 16.
4	Configure the local net service name.	See <a href="#">“Configuring the local net service name on Windows”</a> on page 19.
5	Create the Symantec Data Loss Prevention database user.	See <a href="#">“Creating the Oracle user account for Symantec Data Loss Prevention (Windows)”</a> on page 20.

## Installing Oracle 12c SE2 on Windows

The Enforce Server uses the Oracle thin driver and the Oracle Client (for three-tier deployments). Symantec Data Loss Prevention packages the JAR files for the Oracle thin driver with the Symantec Data Loss Prevention software.

You must install the Oracle Client if you implement a three-tier system. 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 SQL\*Plus.

See [“About installing or upgrading to Oracle 12c Standard Edition 2 Release 2”](#) on page 7.

---

**Note:** Before starting the installation process, confirm that the Windows host name does not contain invalid characters (for example, underscores [\_]). Using invalid characters causes the Oracle installation to fail. If the Windows host name contains invalid characters, go to **Control Panel > System** and change the host name. Restart the computer for the new host name to take effect.

---

## Installing Oracle 12.2.0.1 on Windows

### To install Oracle 12.2.0.1 on Windows

- Shut down the following services if they are running in Windows Services:
  - All Oracle services: OracleService<ServiceID>, Oracle<HOME\_NAME>TNSListener
  - 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 Extract the two ZIP files containing your Oracle 12c SE2 software into a single temporary directory: `C:\temp\Oracle`. The contents of both extracted `database` directories should be in the temporary directory `C:\temp\Oracle\database`.
- 3 Extract the `12.2.0.1_64_bit_Installation_Tools.zip` file into the temporary directory `C:\temp\Oracle\tools`.
- 4 To install the Oracle software, use the command prompt to navigate to the temporary directory where you extracted the Oracle 12c files. Run the following command, which includes the paths to the temporary directories where you extracted the zip files in steps 2 and 3:

---

**Note:** Line breaks added for legibility.

---

```
C:\temp\Oracle\database\setup.exe -noconfig -responsefile
C:\temp\Oracle\tools\responsefiles
\Oracle_12.2.0.1_Standard_Edition_Installation_WIN.rsp
```

The installation wizard appears with pre-selected values drawn from the installation response file. You can confirm these values and click through the panels without needing to enter information where noted.

- 5 On the **Configure Security Updates** panel, **I wish to receive security updates via My Oracle Support** is selected. Click **Next**.
- 6 On the **Select Installation Options** panel, **Install database software only** is selected. Click **Next**.
- 7 On the **Grid Installation Options** panel, **Single instance database installation** is selected. Click **Next**.
- 8 On the **Select Database Edition** panel, **Standard Edition** is selected. Click **Next**.
- 9 On the **Oracle Home User** panel, enter a user name and password for the Oracle Home User. The default name for the Oracle Home User is *Oracle*.

---

**Note:** The Oracle Home User is the Windows user account that runs Windows services for `%ORACLE_HOME`. It is not the Symantec Data Loss Prevention Oracle user account.

---

Confirm the password, then click **Next**.

- 10 On the **Specify Installation Location** panel, the **Oracle Base** and **Software Location** paths fields are populated. Click **Next**.

**Oracle Base:** c:\oracle

**Software Location:** c:\oracle\product\12.2.0.1\db\_1

- 11 On the **Prerequisite Check** panel, click **Next** to begin the prerequisite check process.
- 12 On the **Summary** panel, click **Install** to begin the installation.  

The installer application installs the Oracle 12c software to your computer. This process may take several minutes to complete.
- 13 On the **Finish** panel, click **Close** to exit the installer application. You can safely ignore the configuration note that displays on this panel.

## Creating the Symantec Data Loss Prevention database on Windows

Follow this procedure to create the Symantec Data Loss Prevention database on Windows systems.

### To create the Symantec Data Loss Prevention database on Windows

- 1 Set the ORACLE\_HOME environment variable for your new installation. Open a command prompt, and enter:

```
set ORACLE_HOME=c:\oracle\product\12.2.0.1\db_1
```

If you installed Oracle 12.2.0.1 into a different location, substitute the correct directory in this command.

- 2 Navigate to the C:\temp\Oracle\tools folder where you extracted the 12.2.0.1\_64\_bit\_Installation\_Tools.zip file.
- 3 Copy the database template file (Oracle\_12.2.0.1\_Template\_for\_64\_bit\_WIN.dbt) from the C:\temp\Oracle\tools folder to the c:\oracle\product\12.2.0.1\db\_1\assistants\dbca\templates folder.
- 4 (Optional) Rename the OraDb12c\_home1 section of the **Windows Start** menu item to Oracle\_12.2.0.1.

- 5 Open a command prompt as the Administrator user, and execute the following command:

---

**Note:** Line breaks added for legibility.

---

```
%ORACLE_HOME%\bin\dbca  
-createDatabase  
-ProgressOnly  
-responseFile C:\temp\Oracle\tools\responsefiles\Oracle_12.2.0.1_DBCA_WIN.rsp
```

- 6 Enter the SYS password when you are prompted.
- 7 Create the SYSTEM password when you are prompted.

Follow these guidelines to create acceptable passwords:

- Passwords cannot contain more than 30 characters.
- Passwords cannot contain double quotation marks, commas, or backslashes.
- Avoid using the & character.
- Passwords are case-sensitive by default. You can change the case sensitivity through an Oracle configuration setting.
- If your password uses special characters other than `_`, `#`, or `$`, or if your password begins with a number, you must enclose the password in double quotes when you configure it.

The progress of the Symantec Data Loss Prevention database creation displays on the terminal window.

- 8 Enter the Oracle Home User password when you are prompted.  
The password you enter here is the same password you created in step 9 of [Installing Oracle 12.2.0.1 on Windows](#).
- 9 If the database services *OracleServicePROTECT* and Distributed Transaction Coordinator are down, start them using Windows Services: **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications > Services**.

## Creating the TNS Listener on Windows

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

Before you create the TNS listener, confirm that the local host name can be resolved using the DNS server name or a hosts file. If no DNS server resolution exists, the Net Configuration Assistant (NETCA) does not start. If you use a host file (at `/etc/hosts`), it must contain

IP-address-to-host-name mappings that point to the DNS server name. Add two entries to the `/etc/hosts` file, one that resolves the static IP and one that resolves the local host IP. For example, use the following:

```
[IP address or DNS] myhost.mydomain.com myhost
127.0.0.1 myhost.mydomain.com myhost
```

Replace *myhost* with the actual host name.

### 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\12.2.0.1\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 running the following command:

```
%ORACLE_HOME%/BIN/NETCA
```

This command assumes that you set the Oracle HOME and PATH to the following:

```
set ORACLE_HOME=c:\oracle\product\12.2.0.1\db_1
set PATH=%ORACLE_HOME%\bin;%PATH%
```

- 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, select the default listener name, **LISTENER**, unless you must use a different name. Enter the password for your Oracle Home User, then click **Next**.
- 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** Configure the Local Net Service Name in the **Oracle Net Configuration Assistant**.

See [“Configuring the local net service name on Windows”](#) on page 19.

---

**Note:** You must click **Finish** to exit the **Oracle Net Configuration Assistant** before continuing with this procedure.

---

**11** On the computer that runs your Oracle database, open a command prompt. The command window must run as Administrator. (See your Microsoft Windows documentation.)**12** Run the following command:

```
lsnrctl stop
```

**13** Open the following file in a text editor:

```
%ORACLE_HOME%\network\admin\listener.ora
```

**14** Locate the following line:

```
(ADDRESS = (PROTOCOL = IPC)(KEY = <key_value>))
```

**15** Change *key\_value* to PROTECT.**16** Add the following line to the end of the file:

```
SECURE_REGISTER_LISTENER = (IPC)
```

**17** Save the file and exit the text editor.**18** Run the following command:

```
lsnrctl start
```

**19** Run the following commands to connect to the database using SQL Plus:

```
sqlplus /nolog  
conn sys/<password> as sysdba
```

**20** Run the following command:

```
ALTER SYSTEM SET local_listener =  
'(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=PROTECT)))' SCOPE=both;
```

**21** Run the following command to register the listener:

```
ALTER SYSTEM REGISTER;
```

22 Exit SQL Plus by running the following command:

```
exit
```

23 Run the following command to verify the change:

```
lsnrctl services
```

The command output should display a message similar to the following:

```
Services Summary...
Service "protect" has 1 instance(s).
Instance "protect", status READY, has 1 handler(s) for this service...
  Handler(s):
    "DEDICATED" established:0 refused:0 state:ready
    LOCAL SERVER
The command completed successfully
```

If you are upgrading from an older Oracle version, continue the upgrade process by referring to one of the following topics that apply to your configuration:

- See [“Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation”](#) on page 41.
- See [“Upgrading from Oracle 11g SE1 or Oracle 11g SE on servers with two \(or fewer\) CPU sockets”](#) on page 39.

## Configuring the local net service name on Windows

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 12.2.0.1 > 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**.

If you are upgrading from an older Oracle version, continue the upgrade process by referring to one of the following topics that apply to your configuration:

- See ["Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation"](#) on page 41.
- See ["Upgrading from Oracle 11g SE1 or Oracle 11g SE on servers with two \(or fewer\) CPU sockets"](#) on page 39.

## Creating the Oracle user account for Symantec Data Loss Prevention (Windows)

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

To create the new Oracle user account named "protect"

- 1 Navigate to the `C:\temp\Oracle\tools` folder.
- 2 Start SQL\*Plus:  

```
sqlplus /nolog
```
- 3 Run the `oracle_create_user.sql` script:  

```
SQL> @oracle_create_user.sql
```
- 4 At the **Please enter the password for sys user** prompt, enter the password for the SYS user.
- 5 At the **Please enter Service Name** prompt, enter `protect`.

- 6 At the **Please enter required username to be created** prompt, enter `protect` for the user name.
- 7 At the **Please enter a password for the new username** prompt, enter a new password. Follow these guidelines to create acceptable passwords:
  - Passwords cannot contain more than 30 characters.
  - Passwords cannot contain double quotation marks, commas, or backslashes.
  - Avoid using the `&` character.
  - Passwords are case-sensitive by default. You can change the case sensitivity through an Oracle configuration setting.
  - If your password uses special characters other than `_`, `#`, or `$`, or if your password begins with a number, you must enclose the password in double quotes when you configure it.

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 available here:

<http://www.symantec.com/docs/DOC9261>

## Verifying the Symantec Data Loss Prevention database

After you create the Symantec Data Loss Prevention database, 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
```

- 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 12.2.0.1.

The output information should read:

BANNER

-----

```
Oracle Database 12c Release 12.2.0.1.0 - 64-bit Production
PL/SQL Release 12.2.0.1.0 - Production
CORE      12.2.0.1.0      Production
TNS for 64-bit Windows: Version 12.2.0.1.0 - Production
NLSRTL Version 12.2.0.1.0 - Production
```

- 5 Exit SQL\*Plus:

```
SQL> exit
```

# Installing Oracle 12c Standard Edition 2 Release 2 on Linux

This chapter includes the following topics:

- [Steps to install Oracle 12c SE2 on Linux](#)
- [Performing the preinstallation steps](#)
- [Installing Oracle 12c SE2 on Linux](#)
- [Creating the Symantec Data Loss Prevention database on Linux](#)
- [Creating the TNS Listener on Linux](#)
- [Configuring the local net service name on Linux](#)
- [Verifying tnsnames.ora contents](#)
- [Verifying the Symantec Data Loss Prevention database](#)
- [Creating the Oracle user account for Symantec Data Loss Prevention \(Linux\)](#)
- [Configuring automatic startup and shutdown of the database](#)

## Steps to install Oracle 12c SE2 on Linux

[Table 4-1](#) provides the Oracle 12c installation process. You can find additional detail for each step of the process as indicated in the table.

**Table 4-1** Oracle 12c SE2 installation steps

Step	Action	More information
1	Perform the preinstallation steps.	See <a href="#">“Preparing the Linux environment”</a> on page 24.
2	Install Oracle 12c SE2.	See <a href="#">“Installing Oracle 12c SE2 on Linux”</a> on page 26.
3	Create the Symantec Data Loss Prevention database.	See <a href="#">“Creating the Symantec Data Loss Prevention database on Linux”</a> on page 29.
4	Create the database listener.	See <a href="#">“Creating the TNS Listener on Linux”</a> on page 30.
5	Configure the local net service name.	See <a href="#">“Configuring the local net service name on Linux”</a> on page 33.
6	Create the Symantec Data Loss Prevention database user.	See <a href="#">“Creating the Oracle user account for Symantec Data Loss Prevention (Linux)”</a> on page 36.
7	Configure your system to start Oracle when the server computer boots.	See <a href="#">“Configuring automatic startup and shutdown of the database”</a> on page 37.

## Performing the preinstallation steps

Perform the following procedure to prepare your Linux environment for installation. The preinstallation requires Python. You can use any Python version from 2.4.6 through 3.6.3.

### Preparing the Linux environment

Follow this procedure to prepare the Linux environment.

## To prepare the Linux environment

- 1 Log on as the root user. Navigate to where the file `12.2.0.1_64_bit_Installation_Tools.tar.gz` is located.
- 2 Copy the file `12.2.0.1_64_bit_Installation_Tools.tar.gz` to the Linux server and extract its contents into the temporary directory (`/tmp`). For example:

```
tar xvfz 12.2.0.1_64_bit_Installation_Tools.tar.gz -C /tmp
```

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

- 3 In the `oracle_install` directory, run the Oracle preparation script:

```
cd /tmp/oracle_install  
./scripts/oracle_prepare.sh
```

- 4 Enter the Oracle User password when prompted.
- 5 After the preparation script has run to completion, switch to the `tmp/oracle_install/scripts` directory and run the verification script:

```
cd /tmp/oracle_install/scripts  
./oracle_verify.py
```

The verification script displays settings (such as RAM, swap space, shared memory, `/tmp` disc space) that do not meet the requirements for Oracle. Adjust any settings to the required values.

If you have mismatched values between kernel parameters and resource limits, run the `oracle_config_kernel_parameters.py` script in the `/tmp/oracle_install/scripts` directory. This script sets the kernel parameters to the required settings.

- 6 Restart the server so that the updated kernel parameters take effect.
- 7 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.
- 8 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, available here:

<http://www.symantec.com/docs/DOC10602>

# Installing Oracle 12c SE2 on 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.

You must install the Oracle Client if you implement a three-tier system. 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 installing or upgrading to Oracle 12c Standard Edition 2 Release 2”](#) on page 7.

The instructions in this section assume that you are logged on locally to the Linux server and running the X Window System. It also assumes that you have the `xorg-x11-apps.x86_64` package installed. 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.

## Installing Oracle 12.2.0.1 on Linux systems

For Symantec Data Loss Prevention installation on Linux systems, follow this procedure to install Oracle 12c SE2.

### To install Oracle 12.2.0.1 on Linux systems

- 1 Log in to the terminal as the root user, then execute the following command:

```
su -l root
xhost +SI:localuser:oracle
```

- 2 Switch to the Oracle user terminal.
- 3 Copy the required software installation file or files to `/home/oracle`.

- 4 From `/home/oracle`, unzip the ZIP files you copied. 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.
- 5 Put the contents of the **database** directory from the ZIP file you extracted to `/home/oracle` into a directory titled **database**. You should now have a directory named `/home/oracle/database`.

- 6 Change directory to:

```
cd /home/oracle/database/stage/cvu/cv/admin
```

- 7 Back up the `cvu_config` file using this command:

```
cp cvu_config backup_cvu_config
```

- 8 Edit the original `cvu_config` file as follows:

Set `CV_ASSUME_DISTID=OEL6` if you are using Linux 6.x

Set `CV_ASSUME_DISTID=OEL7` if you are using Linux 7.x

Save the edited `cvu_config` file.

- 9 Navigate to the `/tmp/oracle_install` directory where you extracted the `12.2.0.1_64_bit_Installation_Tools.tar.gz` file.

Copy the response files `Oracle_12.2.0.1_DBCA_Linux.rsp` and `Oracle_12.2.0.1_Standard_Edition_Installation_Linux.rsp` from `/tmp/oracle_install/responsefiles` to a temporary folder such as `/home/oracle/oracle_install/responsefiles`.

- 10 Provide read and write access to the `/opt` directory for the Oracle user.
- 11 In the Oracle user terminal execute this command:

---

**Note:** Line breaks added for legibility.

---

```
/home/oracle/database/runInstaller -noconfig -responseFile  
/home/oracle/oracle_install/responsefiles  
/Oracle_12.2.0.1_Standard_Edition_Installation_Linux.rsp
```

- 12 On the **Configure Security Updates** panel, **I wish to receive security updates via My Oracle Support** is selected. Click **Next**.
- 13 Click **Yes** to confirm that you have not provided an email address.

- 14 On the **Select Installation Option** panel, **Install database software only** is selected. Click **Next**.
- 15 On the **Grid Installation Options** panel, **Single instance database installation** is selected. Click **Next**.
- 16 On the **Select Database Edition** panel, **Standard Edition** is selected. Click **Next**.
- 17 On the **Specify Installation Location** panel, enter the following paths are specified. Click **Next**:
  - **Oracle Base:** `/opt/oracle`
  - **Software Location:** `/opt/oracle/product/12.2.0.1/db_1`
- 18 If this is the first Oracle installation on the server computer, the installer application displays the **Create Inventory** panel. The inventory path is entered as `/opt/oracle/oraInventory` and the group name is entered as `oinstall`. Click **Next**.

The installer may display a warning message that you placed the central inventory location inside of the Oracle base directory. You can safely ignore this message for Symantec Data Loss Prevention database installations.
- 19 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. Click the **Fix and Check Again** button to correct any warnings or installation errors.
- 20 On the **Summary** panel, click **Install** to begin the installation.

The installer application installs the Oracle 12c software on your computer.
- 21 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/12.2.0.1/db_1/root.sh
```

After you run the `/opt/oracle/product/12.2.0.1/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**. Enter **Y** if the script asks for confirmation to overwrite the following files: `dbhome`, `oraenv` and `coraenv`.

The script displays `Finished product-specific root actions` when it is finished.
- 22 Enter **Y** after the script displays `Do you want to setup oracle trace analyzer`. Entering **Y** finishes the process to create the Oracle trace analyzer.

- 23 Return to the **Execute Configuration scripts** screen and click **OK**.
- 24 On the **Finish** panel, click **Close** to exit the installer application. You can safely ignore the configuration note displayed on this panel.

## Creating the Symantec Data Loss Prevention database on Linux

Follow this procedure to create the Symantec Data Loss Prevention database on a Linux system.

### To create the Symantec Data Loss Prevention database on Linux systems

- 1 Set the `ORACLE_HOME` and `ORACLE_SID` environment variables for your new installation. Open a command prompt as the `Oracle` user and enter:

```
export ORACLE_HOME=/opt/oracle/product/12.2.0.1/db_1
export ORACLE_SID=protect
```

If you installed Oracle 12c 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 Navigate to `/tmp/oracle_install` where you extracted the `12.2.0.1_64_bit_Installation_Tools.tar.gz` file.
- 3 Copy the database template file (`Oracle_12.2.0.1_Template_for_64_bit_LIN.dbt`) to the `$ORACLE_HOME/assistants/dbca/templates` directory.
- 4 At the command prompt, execute the following command (line break added for legibility):

```
$ORACLE_HOME/bin/dbca
-createDatabase
-progressOnly
-responseFile /home/oracle/oracle_install/responsefiles/Oracle_12.2.0.1_DBCA_Linux.rsp
```

- 5 Enter the SYS password when you are prompted.
- 6 Create the SYSTEM password when you are prompted.

Follow these guidelines to create acceptable passwords:

- Passwords cannot contain more than 30 characters.
- Passwords cannot contain double quotation marks, commas, or backslashes.

- Avoid using the **&** character
- Passwords are case-sensitive by default. You can change the case sensitivity through an Oracle configuration setting.
- If your password uses special characters other than **\_**, **#**, or **\$**, or if your password begins with a number, you must enclose the password in double quotes when you configure it.

The progress of the Symantec Data Loss Prevention database creation displays on the terminal window.

## Creating the TNS Listener on Linux

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

---

**Note:** To use the the commands referenced in this procedure, ensure that your working directory is `$ORACLE_HOME/bin`. If SQL\*Plus does not work while following this procedure, set your `$PATH` variable to point to `$ORACLE_HOME/bin`.

---

Before you create the TNS listener, confirm that the local host name can be resolved using the DNS server name or a hosts file. If no DNS server resolution exists, the Net Configuration Assistant (NETCA) does not start. If you use a host file (at `/etc/hosts`), it must contain IP-address-to-host-name mappings that point to the DNS server name. Add two entries to the `/etc/hosts` file, one that resolves the static IP and one that resolves the local host IP. For example, use the following:

```
[IP address or DNS] myhost.mydomain.com myhost
127.0.0.1 myhost.mydomain.com myhost
```

Replace *myhost* with the actual host name.

### To create the TNS Listener

- 1 As the `Oracle` user, confirm that the following environment variables are set before starting **Oracle Net Configuration Assistant**.

Set Oracle HOME to the following:

```
export ORACLE_HOME= /opt/oracle/product/12.2.0.1/db_1
```

Set the Oracle SERVICE\_NAME to the following:

```
export ORACLE_SID=protect
```

Set the path to the following

```
export PATH=$ORACLE_HOME\bin:$PATH$
```

- 2 As the `Oracle` user, start the **Oracle Net Configuration Assistant**:

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

- 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 Configure the Local Net Service Name in the **Oracle Net Configuration Assistant**.  
See [“Configuring the local net service name on Linux”](#) on page 33.

---

**Note:** You must click **Finish** to exit the **Oracle Net Configuration Assistant** before continuing with this procedure.

---

- 11 Log on to the Oracle host computer as the Oracle user.

```
su - oracle
```

- 12** Confirm that the ORACLE\_SID is set to the following:

```
export ORACLE_SID=protect
```

- 13** Run the following command:

```
lsnrctl stop
```

- 14** Open the following file in a text editor:

```
$ORACLE_HOME/network/admin/listener.ora
```

- 15** Locate the following line:

```
(ADDRESS = (PROTOCOL = IPC) (KEY = <key_value>))
```

- 16** Change *key\_value* to PROTECT.

- 17** Add the following line to the end of the file:

```
SECURE_REGISTER_LISTENER = (IPC)
```

- 18** Save the file and exit the text editor.

- 19** Run the following command as a root user:

```
lsnrctl start
```

- 20** Run the following commands to connect to the database using SQL\*Plus:

```
sqlplus /nolog  
conn sys/<password> as sysdba
```

- 21** Run the following command:

```
ALTER SYSTEM SET local_listener =  
'(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc) (KEY=PROTECT)))' SCOPE=both;
```

- 22** Run the following command to register the listener:

```
ALTER SYSTEM REGISTER;
```

23 Exit SQL Plus by running the following command:

```
exit
```

24 Run the following command to verify the change:

```
lsnrctl services
```

The command output should display a message similar to the following:

```
Services Summary...
Service "protect" has 1 instance(s).
Instance "protect", status READY, has 1 handler(s) for this service...
  Handler(s):
    "DEDICATED" established:0 refused:0 state:ready
    LOCAL SERVER
The command completed successfully
```

If you are upgrading from an older Oracle version, continue the upgrade process by referring to one of the following topics that apply to your configuration:

- See [“Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation”](#) on page 41.
- See [“Upgrading from Oracle 11g SE1 or Oracle 11g SE on servers with two \(or fewer\) CPU sockets”](#) on page 39.

## Configuring the local net service name on Linux

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, log on as the `oracle` user and 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 tnsnames.ora contents

Before you create the required Oracle user accounts, verify that the `tnsnames.ora` file contains entries for the `protect` database that you created.

### To verify or update tnsnames.ora file contents

- 1 Using a text editor, open the `tnsnames.ora` file, located in the `$ORACLE_HOME/network/admin` directory.
- 2 Verify that the following lines are present in the file:

```
PROTECT =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP) (HOST = ip_address) (PORT = port_number))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = protect)
    )
  )
```

If these lines do not exist, add them to the file, replacing *ip\_address* and *port\_number* with the correct values for your system.

---

**Note:** Do not copy and paste information to the `tnsnames.ora` file, as it can introduce hidden characters that cannot be parsed.

---

- 3 Save the `tnsnames.ora` file and exit the text editor.

## Verifying the Symantec Data Loss Prevention database

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

### To verify that the database was created correctly

- 1 Open a command prompt as the `Oracle` user 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 12.2.0.1.

The output information should read:

```
BANNER
```

```
-----  
  
Oracle Database 12c Release 12.2.0.1.0 - 64bit Production  
PL/SQL Release 12.2.0.1.0 - Production  
CORE      12.2.0.1.0      Production  
TNS for Linux: Version 12.2.0.1.0 - Production  
NLSRTL Version 12.2.0.1.0 - Production
```

- 5 Exit SQL\*Plus:

```
SQL> exit
```

## Creating the Oracle user account for Symantec Data Loss Prevention (Linux)

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

**To create the new Oracle user account named "protect"**

- 1 Copy the `oracle_create_user.sql` file from `/tmp/oracle_install/scripts` to a local directory.
- 2 Open a command prompt as the `Oracle` user and go to the directory where you copied 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 Service Name** 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.

Follow these guidelines to create acceptable passwords:

- Passwords cannot contain more than 30 characters.
- Passwords cannot contain double quotation marks, commas, or backslashes.
- Avoid using the `&` character.
- Passwords are case-sensitive by default. You can change the case sensitivity through an Oracle configuration setting.
- If your password uses special characters other than `_`, `#`, or `$`, or if your password begins with a number, you must enclose the password in double quotes when you configure it.

Store the password in a secure location for future use. You 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, available here:

<http://www.symantec.com/docs/DOC9261>

## Configuring automatic startup and shutdown of the database

To configure automatic startup and shutdown of the database, follow this procedure:

### To configure the automatic startup and shutdown of the database

- 1 Switch to the root **xterm** window.
- 2 Go to the `oracle_install` directory.

```
cd /tmp/oracle_install
```

- 3 Run the `oracle_post.sh` script from the `oracle_install` directory.

```
./scripts/oracle_post.sh
```

- 4 Verify that the script completed successfully by checking if the very last line of the output is:

```
dbora 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

You may see errors before the last line (for example, `cannot access /var/log/dbora`).

You can ignore these errors.

# Upgrading to Oracle 12c Standard Edition 2 Release 2

This chapter includes the following topics:

- [Upgrading from Oracle 11g SE1 or Oracle 11g SE on servers with two \(or fewer\) CPU sockets](#)
- [Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation](#)
- [Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation](#)
- [Upgrading to Oracle 12.2.0.1](#)

## Upgrading from Oracle 11g SE1 or Oracle 11g SE on servers with two (or fewer) CPU sockets

[Table 5-1](#) describes the steps you complete to upgrade to Oracle 12c SE2 from Oracle 11g SE or SE1 on servers with two (or fewer) CPU sockets.

**Table 5-1** Upgrade path from Oracle 11g SE1 or Oracle 11g SE on servers with two (or fewer) CPU sockets

Step	Action	Information
1	Stop all Symantec Data Loss Prevention services on the Enforce Server except the Symantec DLP Update Service.	For information on stopping services, see the <i>Symantec Data Loss Prevention Upgrade Guide</i> .

**Table 5-1** Upgrade path from Oracle 11g SE1 or Oracle 11g SE on servers with two (or fewer) CPU sockets (*continued*)

Step	Action	Information
2	Upgrade the database to Oracle 12c SE2.	See <a href="#">“Upgrading to Oracle 12.2.0.1”</a> on page 42.
3	Re-create the TNS listener.	See <a href="#">“Creating the TNS Listener on Windows”</a> on page 16. See <a href="#">“Creating the TNS Listener on Linux”</a> on page 30.
4	Re-create the local net services.	See <a href="#">“Configuring the local net service name on Windows”</a> on page 19. See <a href="#">“Configuring the local net service name on Linux”</a> on page 33.
5	Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database.	See <a href="#">“Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database”</a> on page 57.
6	Restart all Symantec Data Loss Prevention services.	For information on starting services, see the <i>Symantec Data Loss Prevention Upgrade Guide</i> .

## Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation

[Table 5-2](#) describes the steps you complete to upgrade to Oracle 12c SE2 from Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation.

It is likely that your license for Oracle 12c SE2 limits CPU sockets to two. You may be running an Oracle 11g database on computers with more than two CPU sockets. If this is the case, you must migrate your database to a new computer with two CPU sockets.

**Table 5-2** Upgrade path for Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation

Step	Action	Information
1	Migrate the database to new hardware with two CPU sockets.	See <a href="#">“About migrating the Oracle database to supported hardware”</a> on page 47.

**Table 5-2** Upgrade path for Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation (*continued*)

Step	Action	Information
2	Stop all Symantec Data Loss Prevention services on the Enforce Server except the Symantec DLP Update Service.	For information on stopping services, see the <i>Symantec Data Loss Prevention Upgrade Guide</i> .
3	Install the Oracle 12c SE2 on new two CPU socket hardware.	See <a href="#">“Steps to install Oracle 12c SE2 on Windows”</a> on page 12. See <a href="#">“Steps to install Oracle 12c SE2 on Linux”</a> on page 23.
4	Re-create the TNS listener.	See <a href="#">“Creating the TNS Listener on Windows”</a> on page 16. See <a href="#">“Creating the TNS Listener on Linux”</a> on page 30.
5	Re-create the local net services.	See <a href="#">“Configuring the local net service name on Windows”</a> on page 19. See <a href="#">“Configuring the local net service name on Linux”</a> on page 33.
6	Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database.	See <a href="#">“Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database”</a> on page 57.
7	Restart all Symantec Data Loss Prevention services.	For information on starting services, see the <i>Symantec Data Loss Prevention Upgrade Guide</i> .

## Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation

[Table 5-3](#) describes the steps you complete to upgrade to Oracle 12c SE2 from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation.

It is likely that your license for Oracle 12c SE2 limits CPU sockets to two. You may be running an Oracle 11g database on computers with more than two CPU sockets. If this is the case, you must migrate your database to a new computer with two CPU sockets.

**Table 5-3** Upgrade path for Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation

Step	Action	Information
1	Migrate the database to new hardware with two CPU sockets.	See <a href="#">“About migrating the Oracle database to supported hardware”</a> on page 47.
2	On your Symantec Data Loss Prevention 14.6 Enforce Server, stop all Symantec Data Loss Prevention services except the Symantec DLP Update Service.	For information on stopping services, see chapter 5 in the <i>Symantec Data Loss Prevention Upgrade Guide</i> .
3	Install the Oracle 12c SE2 on new two CPU socket hardware.	See <a href="#">“Steps to install Oracle 12c SE2 on Windows”</a> on page 12.  See <a href="#">“Steps to install Oracle 12c SE2 on Linux”</a> on page 23.
4	Migrate the Enforce Server to supported hardware.	Refer to the <i>Symantec Symantec Data Loss Prevention System Maintenance Guide</i> .  <a href="http://www.symantec.com/docs/DOC9267">http://www.symantec.com/docs/DOC9267</a> .

## Upgrading to Oracle 12.2.0.1

You use the following steps to upgrade your Oracle 11g SE1 or Oracle 11g SE database running on servers with two (or fewer) CPU sockets. The following steps include details for both Windows and Linux.

---

**Note:** If you upgrade the Oracle database on Linux, you must complete prerequisite steps. See [“Preparing the Linux environment”](#) on page 24.

---

**Complete the following steps to upgrade your version to Oracle 12.2.0.1:**

- 1 Obtain the Oracle 12.2.0.1 installation software.

Go to Symantec Software Downloads to download the installation media.

- 2 Install Oracle 12.2.0.1 under the same folder as Oracle 11g. For example:

`c:\oracle\product\12.2.0.1\db1` for Windows

`/opt/oracle/product/12.2.0.1/db1` for Linux

Refer to the install steps for your particular database server OS to install the Oracle 12.2.0.1 database:

See “[Installing Oracle 12c SE2 on Windows](#)” on page 13.

See “[Installing Oracle 12c SE2 on Linux](#)” on page 26.

- 3 Set ORACLE\_HOME depending on your database server OS:

`set ORACLE_HOME=c:\oracle\product\12.2.0.1\db_1` for Windows

`export ORACLE_HOME=/opt/oracle/product/12.2.0.1/db_1` for Linux

---

**Note:** Clear any errors before starting the Database Upgrade Assistant.

---

- 4 Set the ORACLE\_SID variable:

`set ORACLE_SID=protect` for Windows

`export ORACLE_SID=protect` for Linux

- 5 Set the display variable if you upgrade on Linux by running the following command:

`export DISPLAY=ip_address:display_number`

Where *ip\_address* is the local host.

- 6 Start the Database Upgrade Assistant by running the following command:

`%ORACLE_HOME%/bin/dbua` for Windows

`$ORACLE_HOME/bin/dbua` for Linux

If the Database Upgrade Assistant does not launch and an error message displays, complete the following items in order:

- Open the command prompt window.

- Set ORACLE\_HOME depending on your database server OS:

`set ORACLE_HOME=c:\oracle\product\12.2.0.1\db_1` for Windows

`export ORACLE_HOME= /opt/oracle/product/12.2.0.1/db1` for Linux

- Set the path:

`set PATH=%PATH%;%ORACLE_HOME%\bin` for Windows

`export PATH=$PATH:$ORACLE_HOME/bin` for Linux

■ **Restart the Database Upgrade Assistant:**

`%ORACLE_HOME%/bin/dbua` for Windows

`$ORACLE_HOME/bin/dbua` for Linux

**7** Confirm that the OracleServicePROTECT service is running.

If the service is not running, an error message displays and the upgrade process cannot finish.

**8** Refer to the following table for information on what to enter on each screen of the Database Upgrade Assistant.

Screen	Description
<b>Select Database</b>	Do not enter the sysdba user name and password. You connect to the existing database at a later part of the upgrade.
<b>Prerequisite Checks</b>	Resolve any warnings or errors that display. In some cases, you must drop packages from previous Symantec Data Loss Prevention versions to clear errors. For example, to drop Symantec Data Loss Prevention 14.0 packages, you run the following SQL command:  <pre>SQL&gt; drop package UPGRADESCEHEME_PRELOAD_V14_0_0</pre>
<b>Select Upgrade Options</b>	Leave the settings as default.
<b>Select Recover Options</b>	Select <b>I have my own backup and restore strategy</b> .
<b>Configure Network</b>	Clear the selected listener that displays on the <b>Listener Selection</b> tab. You re-create the listener in a later step. Leave the remaining settings default.
<b>Configure Management</b>	Clear the <b>Configure Enterprise Manager (EM) database express</b> selection.
<b>Summary</b>	The <b>Summary</b> screen lists the settings that are used during the database upgrade. Click <b>Finish</b> .
<b>Progress</b>	The <b>Progress</b> screen displays the details about the upgrade. The upgrade can take around 30 minutes to complete.
<b>Results</b>	The <b>Results</b> screen displays when the upgrade completes.

**9** Re-create the TNS listener.

See [“Creating the TNS Listener on Windows”](#) on page 16.

See [“Creating the TNS Listener on Linux”](#) on page 30.

**10** Re-create the local net services.

See [“Configuring the local net service name on Windows”](#) on page 19.

See [“Configuring the local net service name on Linux”](#) on page 33.

**11** Restart Symantec Data Loss Prevention services.

**12** Log on to the Enforce Server administration platform.

If the Enforce Server logon page does not load and instead displays a 'GLOBAL NOT\_FOUND' message, restart all Symantec Data Loss Prevention services again.

# Migrating the Oracle database to supported hardware

This chapter includes the following topics:

- [About migrating the Oracle database to supported hardware](#)
- [Workflow for migrating the Oracle database to supported hardware](#)
- [Confirm the schema row count before the export \(Windows\)](#)
- [Exporting a database schema \(Windows\)](#)
- [Confirm the schema row count before the export \(Linux\)](#)
- [Exporting a database schema \(Linux\)](#)
- [Importing a database backup schema on Windows](#)
- [Confirm the schema row count after the import \(Windows\)](#)
- [Import the database backup schema on Linux](#)
- [Confirm the schema row count after the import \(Linux\)](#)
- [Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database](#)

# About migrating the Oracle database to supported hardware

Your license requires that you run Oracle 12c SE2 on a two CPU socket system. If you are running an Oracle 11g database on computers with more than two CPU sockets you must migrate your database to a new computer with two CPU sockets running Oracle 12c SE2.

---

**Note:** If you are migrating to a two-CPU socket system and you use a single-tier or a two-tier Symantec Data Loss Prevention implementation, you must migrate the Enforce Server and detection servers to the two-CPU system. See chapter 6 for Windows or chapter 7 for Linux in the *Symantec Data Loss Prevention System Maintenance Guide* available here:

[www.symantec.com/docs/DOC9267](http://www.symantec.com/docs/DOC9267)

---

## Workflow for migrating the Oracle database to supported hardware

[Table 6-1](#) describes the process to migrate the Oracle 12c SE2 database to a server with two CPU sockets.

These steps assume that you have updated Symantec Data Loss Prevention to version 14.6, 15.0, 15.1, or 15.5.

See [“Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a two-tier installation”](#) on page 40.

See [“Upgrading from Oracle 11g SE on servers with more than two CPU sockets on a single-tier installation”](#) on page 41.

---

**Note:** You can use these steps to run the Oracle 12c SE2 database on the same server as the Enforce Server (a single-tier system).

---

**Table 6-1** Steps to migrate the Oracle database to a server with two CPU sockets

Step	Action	Description
1	Stop Symantec Data Loss Prevention services on the Enforce Server.	For information on stopping services, see the <i>Symantec Data Loss Prevention Upgrade Guide</i> available here: <a href="http://www.symantec.com/docs/DOC9258">http://www.symantec.com/docs/DOC9258</a>

**Table 6-1** Steps to migrate the Oracle database to a server with two CPU sockets  
*(continued)*

Step	Action	Description
2	Install Oracle 12c SE2 on the two CPU socket system.	See <a href="#">“Steps to install Oracle 12c SE2 on Windows”</a> on page 12.  See <a href="#">“Steps to install Oracle 12c SE2 on Linux”</a> on page 23.
3	Confirm the database row count.	See <a href="#">“Confirm the schema row count before the export (Windows)”</a> on page 49.  See <a href="#">“Confirm the schema row count before the export (Linux)”</a> on page 51.
4	Export the existing database.	See <a href="#">“Exporting a database schema (Windows)”</a> on page 50.  See <a href="#">“Exporting a database schema (Linux)”</a> on page 52.
4	Create the Oracle user account.	See <a href="#">“Creating the Oracle user account for Symantec Data Loss Prevention (Windows)”</a> on page 20.  See <a href="#">“Creating the Oracle user account for Symantec Data Loss Prevention (Linux)”</a> on page 36.
5	Import the database.	Copy the Oracle <code>export.dmp</code> file from the location on the previous server computer to the same locations on the two CPU socket server computer.  See <a href="#">“Importing a database backup schema on Windows”</a> on page 53.  See <a href="#">“Import the database backup schema on Linux”</a> on page 55.
6	Confirm the schema row count in the imported database.	See <a href="#">“Confirm the schema row count after the import (Windows)”</a> on page 54.  See <a href="#">“Confirm the schema row count after the import (Linux)”</a> on page 56.

**Table 6-1** Steps to migrate the Oracle database to a server with two CPU sockets  
*(continued)*

Step	Action	Description
7	Create the TNS listener on the Oracle 12c SE2 server.	See <a href="#">“Creating the TNS Listener on Windows”</a> on page 16. See <a href="#">“Creating the TNS Listener on Linux”</a> on page 30.
8	Modify the <code>jdbc.properties</code> file on the Enforce Server to point to the Oracle 12c SE2 database.	See <a href="#">“Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database”</a> on page 57.

## Confirm the schema row count before the export (Windows)

Confirm the schema row count before you begin the database export. You use the database row count to compare to the count after you complete the export.

### To confirm the database object count

- 1 Run the command:

```
sqlplus protect/<password>@protect
```

- 2 Run the following command to create a PL/SQL function to generate the row count:

```
SQL>create or replace function
row_count (p_tablename in varchar2)
return number
as
l_count number;
begin execute immediate
'select count(*)
from ' || p_tablename
into l_count;
return l_count;
end;
/
```

- 3 Run the following query to generate the row count for each table in your schema:

```
SQL> spool rowCount_before_export.txt
```

```
SQL> select table_name, row_count(table_name) num_of_rows from user_tables;
```

```
SQL> spool off
```

The `rowCount_before_export.txt` file is generated in the execution directory.

- 4 Save the `rowCount_before_export.txt` file for future use.

## Exporting a database schema (Windows)

Complete the following steps to migrate the necessary Oracle database schemas from an unsupported Oracle installation on Windows.

---

**Note:** Before you begin the process to export database schemas, back up the database. For more information, see the *Symantec Data Loss Prevention System Maintenance Guide*, available here:

<http://www.symantec.com/docs/DOC9267>.

---

### To export the Oracle database on Windows

- 1 Set the `ORACLE_HOME` and `ORACLE_SID` variables using the following commands:

```
set ORACLE_HOME=c:\oracle\product\oracle_version\db_1 where oracle_version is  
the existing Oracle database version. For example, enter 11.2.0.4 if you are running Oracle  
11g Release 2.
```

```
set ORACLE_SID = protect
```

- 2 Log on as the SYS user:

```
sqlplus /nolog
```

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

Where **password** represents the SYS password.

- 3 Run the following command:

```
Select * from dba_directories;
```

Running this command identifies the location of the `DATA_PUMP_DIR` where the `export.dmp` file is created at the end of the database export procedure.

- 4 Run the following command:

```
Grant read,write on directory DATA_PUMP_DIR to protect;
```

- 5 Run the following command:

```
Grant exp_full_database to protect;
```

- 6 Exit SQL\*Plus:

```
SQL> exit
```

- 7 Export the database schema by running the following command from a command prompt:

```
Expdp protect/<protect schema password> DUMPFILE=export.dmp schemas=protect  
DIRECTORY=DATA_PUMP_DIR EXCLUDE=INDEX, STATISTICS
```

- 8 Verify that the `export.dmp` file is created in the `DATA_PUMP_DIR` location.

## Confirm the schema row count before the export (Linux)

Confirm the schema row count before you begin the database export. You use the schema row count to compare to the count after you complete the export.

### To confirm the database object count

- 1 Run the command:

```
sqlplus protect/<password>@protect
```

- 2 Run the following command to create a PL\SQL function to generate the row count:

```
SQL>create or replace function  
row_count (p_tablename in varchar2)  
return number  
as  
l_count number;  
begin execute immediate  
'select count(*)  
from ' || p_tablename  
into l_count;  
return l_count;  
end;  
/
```

- 3 Run the following query to generate the row count for each table in your schema:

```
SQL> spool rowCount_before_export.txt  
  
SQL> select table_name, row_count(table_name) num_of_rows from user_tables;  
  
SQL> spool off
```

The `rowCount_before_export.txt` file is generated in the execution directory.

- 4 Save the `rowCount_before_export.txt` file for future use.

## Exporting a database schema (Linux)

Complete the following steps to export the necessary Oracle database schemas from an unsupported Oracle installation on Linux.

---

**Note:** Before you begin the process to export database schemas, back up the database. For more information, see the *Symantec Data Loss Prevention System Maintenance Guide*, available here:

<http://www.symantec.com/docs/DOC9267>.

---

### To export the Oracle database on Linux

- 1 Set the `ORACLE_HOME` and `ORACLE_SID` variables using the following commands:

```
export ORACLE_HOME=/opt/oracle/product/oracle_version/db_1 where oracle_version  
is the existing Oracle database version. For example, enter 11.2.0.4 if you are running  
Oracle 11g Release 2.
```

```
export ORACLE_SID = protect
```

- 2 Log on as the SYS user:

```
sqlplus /nolog
```

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

Where **password** represents the SYS password.

- 3 Run the following command:

```
Select * from dba_directories;
```

Running this command identifies the location of the `DATA_PUMP_DIR` where the `export.dmp` file is created at the end of the database export procedure.

- 4 Run the following command:

```
Grant read,write on directory DATA_PUMP_DIR to protect;
```

- 5 Run the following command:

```
Grant exp_full_database to protect;
```

- 6 Exit SQL\*Plus:

```
SQL> exit
```

- 7 Switch to the Oracle user by running the following command:

```
su - oracle
```

- 8 Export the database schema by running the following command from Terminal:

```
Expdp protect/<protect schema password> DUMPFILE=export.dmp schemas=protect  
DIRECTORY=DATA_PUMP_DIR EXCLUDE=INDEX, STATISTICS
```

- 9 Verify that the `export.dmp` file is created in the `DATA_PUMP_DIR` location.

## Importing a database backup schema on Windows

Complete the following steps on the two CPU socket Windows server computer.

### Import the database backup schema to Windows

- 1 Set the `ORACLE_HOME` and `ORACLE_SID` variables as follows:

```
set ORACLE_HOME=c:\oracle\product\12.2.0.1\db_1  
set ORACLE_SID = protect
```

- 2 Log on as the SYS user:

```
sqlplus /nolog  
SQL> connect sys/<password>@protect as sysdba
```

Where **password** represents the SYS password.

- 3 Run the following command:

```
Grant read,write on directory DATA_PUMP_DIR to protect;
```

- 4 Run the following command:

```
Grant imp_full_database to protect;
```

- 5 Exit SQL\*Plus:

```
SQL> exit
```

- 6 Import the database schema by running the following command from a command prompt:

```
Impdp 'sys/<password> as sysdba' DUMPFILE=export.dmp schemas=protect  
DIRECTORY=DATA_PUMP_DIR
```

- 7 Regenerate statistics and rebuild indexes after the import completes.
- 8 Verify that the import process was successful by running the following command:

```
sqlplus protect/⟨password⟩@protect
```

Verify that data is present in the schema.

## Confirm the schema row count after the import (Windows)

After importing the database schema, you generate a row count of each table in the schema. You compare the data you generate with the data you generated before the schema export.

### To generate a row count of each table in the schema

- 1 Run the following command:

```
sqlplus protect/⟨password⟩@protect
```

- 2 Run the following command to create a PL\SQL function to generate the row count:

```
SQL>create or replace function  
row_count (p_tablename in varchar2)  
return number  
as  
l_count number;  
begin  
execute immediate  
'select count(*)  
from ' || p_tablename  
into l_count;  
return l_count;  
end;  
/
```

- 3 Run the following query to generate a row count for each table in the schema:

```
SQL>spool rowCount_after_import.txt

SQL>select table_name, row_count(table_name) num_of_rows
from user_tables;

SQL>spool off
```

The `rowCount_after_import.txt` is created in the execution directory.

- 4 Compare the data in `rowCount_after_import.txt` with the `rowCount_before_export.txt` file you created before the export operation.

See [“Confirm the schema row count before the export \(Windows\)”](#) on page 49.

## Import the database backup schema on Linux

Complete the following steps on the two CPU socket Linux server computer.

### Import the database backup schema to Linux

- 1 Set the `ORACLE_HOME` and `ORACLE_SID` variables as follows:

```
export ORACLE_HOME=/opt/oracle/product/12.2.0.1/db_1
export ORACLE_SID = protect
```

- 2 Log on as the SYS user:

```
sqlplus /nolog

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

Where **password** represents the SYS password.

- 3 Run the following command:

```
Grant read,write on directory DATA_PUMP_DIR to protect;
```

- 4 Run the following command:

```
Grant imp_full_database to protect;
```

- 5 Exit SQL\*Plus:

```
SQL> exit
```

- 6 Switch to the Oracle user using the following command:

```
su - oracle
```

- 7 Import the database schema by running the following command from the Terminal:

```
impdp \ 'sys/<password> as sysdba\ ' dumpfile=export.dmp schemas=protect  
DIRECTORY=DATA_PUMP_DIR
```

- 8 Regenerate statistics and rebuild indexes after the import completes.
- 9 Verify that import was successful by running the following command:

```
sqlplus protect/<password>@protect
```

Verify that data is present in the schema.

## Confirm the schema row count after the import (Linux)

After importing the database schema, you generate a row count of each table in the schema. You compare the data you generate with the data you generated before the schema export.

**To generate a row count of each table in the schema**

- 1 Run the following command:

```
sqlplus protect/<password>@protect
```

- 2 Run the following command to create a PL\SQL function to generate the row count:

```
SQL>create or replace function  
row_count (p_tablename in varchar2)  
return number  
as  
l_count number;  
begin  
execute immediate  
'select count(*)  
from ' || p_tablename  
into l_count;  
return l_count;  
end;  
/
```

- 3 Run the following query to generate a row count for each table in the schema:

```
SQL>spool rowCount_ater_import.txt

SQL>select table_name, row_count(table_name) num_of_rows
from user_tables;

SQL>spool off
```

The `rowCount_after_import.txt` is created in the execution directory.

- 4 Compare the data in `rowCount_after_import.txt` with the `rowCount_before_export.txt` file you created before the export operation.

See [“Confirm the schema row count before the export \(Linux\)”](#) on page 51.

## Connect Symantec Data Loss Prevention to the Oracle 12c SE2 database

You update the configuration file `jdbc.properties` on the existing Enforce Server file system to reference the Oracle 12c SE2 database.

**Complete the following steps to update the `jdbc.properties`:**

- 1 Locate the `jdbc.properties` file on the Enforce Server. The following table lists the location based on platform and version:

Windows    `\SymantecDLP\Protect\config` on Symantec Data Loss Prevention version 15.0 through 14.6.

`\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\config` on Symantec Data Loss Prevention version 15.5 and later.

Linux        `/opt/SymantecDLP/Protect/config` on Symantec Data Loss Prevention version 15.0 through 14.6.

`/opt/Symantec/DataLossPrevention/EnforceServer/15.5/Protect/config` on Symantec Data Loss Prevention version 15.5 and later.

- 2 Open the file and locate the **host** line where the `jdbc.dbalias.oracle-thin` value displays the default IP.
- 3 Enter the DNS or IP of the two CPU server computer.
- 4 Save the file.

- 5 Restart the Symantec DLP Manager service on the Enforce Server.
- 6 Log on to the Enforce Server administration console to confirm that the Enforce Server is connected to the database. If you cannot log on, restart all Symantec DLP services and log on again.