Evaluated Configuration Guide for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406

Issue	:	0.8	
Date	:	02 June 2009	
Status	:	Definitive	
Distribution	:		
Prepared by	:	.....	Rizwan Arshad
Reviewed by	:	.....	Hugh Griffin
Authorised by	:	.....	Peter Goatly

==========

Evaluated Configuration Guide for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406

June 2009

Author: Rizwan Arshad

Contributors: Hugh Griffin, Ann Craig and Joel Crisp

==========

Document History

Version	Date	Notes
0.1	12 June 2008	Initial draft
0.8	2 June 2009	Definitive

Table Of Contents

Abbreviations

CC	Common Criteria
CEM	Common Evaluation Methodology
CI	Configuration Item
EAL	Evaluation Assurance Level
ECG	Evaluated Configuration Guide
ETR	Evaluation Technical Report
ISO	International Standards Organisation
IT	Information Technology
OR	Observation Report
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

1 Introduction

1.1 Purpose

This document is the Evaluated Configuration Guide (ECG) for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406.

Title: Evaluated Configuration Guide for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406

Target of Evaluation (TOE): Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406

Release: 10.1.3.3.2 with Quick Fix 090406

Operating System Platform: Oracle Enterprise Linux, Version 4 Update 5 operating system platform with the capp-eal4-config-oracle package

Database Platform: Oracle Database Server 10*g* Release 2 (10.2.0.3.0)

LDAP Directory Platform: Oracle Internet Directory 10*g* (10.1.4.0.1)

Web Server Platform: Oracle HTTP Server 10g Release 2 (10.1.2)

OC4J Platform: Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0)

Keywords: Oracle Business Intelligence Enterprise Edition, EAL3.

1.2 TOE Overview

The TOE is hosted on Oracle Enterprise Linux Version 4 Update 5 operating system platform and uses Oracle Application Server 10g Release 3 (10.1.3.1.0) to serve content and Oracle Client 10g Release 2 (10.2.0.3.0) to connect to the database platform.

This document explains the manner in which the TOE must be configured along with the host operating system so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The assumptions and procedures stated in the document are intended to remove potential vulnerabilities or attack paths from the TOE in its environment. They do not have any impact on the correct implementation of the TOE's SFs.

The Evaluation Assurance Level for the TOE is EAL3. The Security Target used for the evaluation of the TOE is [ST].

1.3 Document Structure

This ECG is divided into 7 sections, as follows:

- Section 1 (this section) provides an introduction to the ECG.
- Section 2 provides the preparatory actions to be undertaken before installing the software for the evaluated configuration.
- Section 3 provides the installation of the software for the evaluated configuration.
- Section 4 provides the post-installation actions to complete the evaluated configuration.
- Section 5 provides the supporting procedures to ensure that the TOE is operated in a way that upholds the security objectives defined in [ST].

1.4 Format

Assertions for the physical, host, and Oracle configurations are given identifiers to the left of each evaluation configuration requirement in bold Arial font, e.g. **[A-1]**.

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “should” in each assertion.

2 Preparation

This part of the ECG provides the preparatory actions to be undertaken before installing the software for the evaluated configuration of Oracle Business Intelligence Enterprise Edition (Oracle BIEE).

2.1 Machine Configuration

In the configuration used for the evaluation testing of Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406, the TOE was installed on virtual machines hosted on two Dell Optiplex 745 MT – Core 2 Duo E6400 (2.13 GHz) machines with 4GB of memory.

It is recommended that Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 be used on physically separate servers. Time synchronisation issues may occur on virtual machine setups and they should be checked for and resolved before the system is put into production. If problems are found the virtualisation vendor should be consulted to resolve the issue[1].

The virtual machines allocated for the installation of the TOE were:

Machines	vm1, vm2
Specification	Dell Optiplex 745 MT – Core 2 Duo E6400 (2.13 GHz) 1GB Memory Oracle Enterprise Linux 4 Update 5 x86_64
Products to be installed	Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) Oracle Client 10*g* Release 2 (10.2.0.3.0) Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406

Table 2.1: Configuration of machines 1 and 2

Machine	vm3
Specification	Dell Optiplex 745 MT – Core 2 Duo E6400 (2.13 GHz) 1GB Memory

[1] The work around used on the test machines during the evaluation was to use `cron` jobs to have each virtual machine synchronise time every 10 minutes with the host physical machine. These in turn were synchronised with the UK pool of NTP servers using an NTP service.

	Oracle Enterprise Linux 4 Update 5 x86_64
Products to be installed	Oracle Database 10*g* Release 2 (10.2.0.3.0)

Table 2.2: Configuration of machine 3

Machine	vm4
Specification	Dell Optiplex 745 MT – Core 2 Duo E6400 (2.13 GHz) 1GB Memory Oracle Enterprise Linux 4 Update 5 x86_64
Products to be installed	Oracle Internet Directory 10*g* Release 4 (10.1.4.0.1)

Table 2.3: Configuration of machine 4

Machine	vm5
Specification	Optiplex 745 MT – Core 2 Duo E6400 (2.13 GHz) 1GB Memory Oracle Enterprise Linux 4 Update 5 x86_64
Products to be installed	Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) Oracle HTTP Server 10*g* Release 2 (10.1.2) Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Presentation Services Plug-In

Table 2.4: Configuration of machine 5

Machine	vm6
Specification	Optiplex 745 MT – Core 2 Duo E6400 (2.13 GHz) 1GB Memory Microsoft Windows XP SP2
Products to be installed	JDK 5 Update 16 Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) Client Tools

Table 2.5: Configuration of machine 6

Machine	vm7
Specification	Optiplex 745 MT – Core 2 Duo E6400 (2.13 GHz) 384MB Memory Oracle Enterprise Linux 4 Update 5 x86_64
Products to be installed	None

Table 2.6: Configuration of machine 7

2.2 System Architecture

The diagram below illustrates the physical and logical architecture of the TOE:

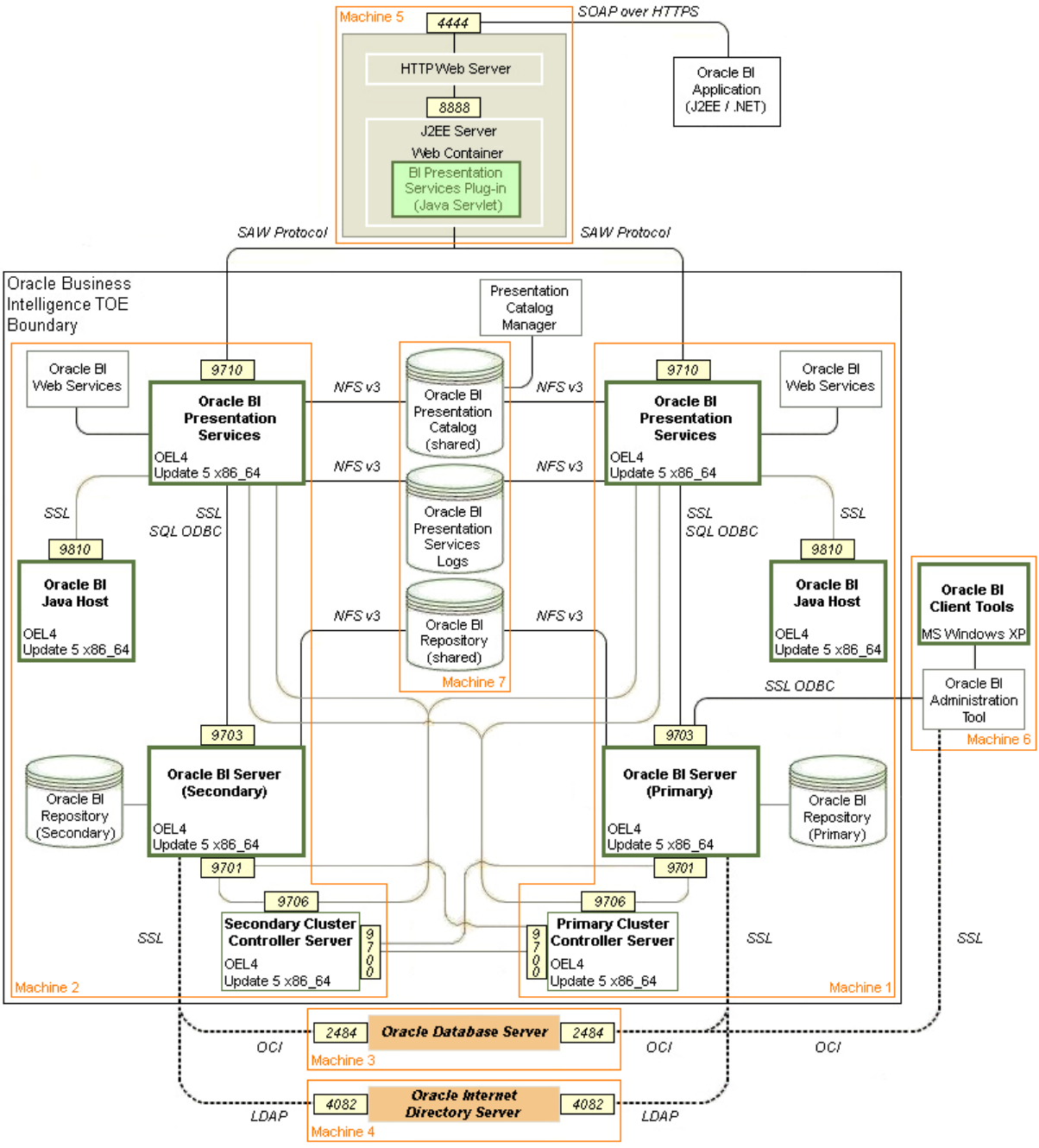


Figure 1: TOE Configuration

2.3 Physical Environmental Assumptions

This section describes physical requirements on the server machine so that the security of the TOE can be maintained.

[DI.A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorized physical access to the TOE by unprivileged users. Only authorised administrators for the system hosting the TOE shall have physical access to that system. Such administrators include the Operating System Administrators, Database Administrators and OID Directory Administrators.

[DI.A-2] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorised users.

[DI.A-3] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorised physical access.

[DI.A-4] A reliable time source such as an NTP server, radio clock or GPS unit shall be used to ensure clock coherence between all servers within the environment.

2.4 Electronic Delivery of the TOE

To receive electronic delivery of the TOE installation software, complete the following steps:

1. Access the Oracle Technology Network Website at http://www.oracle.com/technology/index.html.

2. Click on the ‘Downloads’ link.

3. Scroll down to the Middleware section and click ‘Business Intelligence Suite EE’.

4. Click the checkbox if you agree to the Licence Terms and export restrictions.

5. Click the ‘I Accept’ button to agree to the OTN licence terms.

6. You should now be looking at the ‘Oracle Business Intelligence (10.1.3.x) Downloads’ page: http://www.oracle.com/technology/software/products/ias/htdocs/101320bi.html.

7. The following product needs to be downloaded for the Microsoft Windows and Linux operating systems:

Oracle Business Intelligence Suite Enterprise Edition, v. 10.1.3.3.2

8. Hovering the mouse pointer over the link to the download will display the download's cksum number. This number should be recorded for later verification.

9. When the first download is requested, the OTN Sign-in page is presented.

10. Complete the form with your OTN login details, or create an account by clicking 'sign up now'.

11. The download will start. Ensure that you download all disks for the Microsoft Windows and Linux operating system.

12. Once the download is complete and the file has been transferred to the target environment, check the file with the cksum filename command to ensure that the download has not become corrupted. If the CKSUM numbers do not match, the file should be downloaded again.

For the Evaluated Configuration, the 64-bit Oracle Enterprise Linux 4 Update 5 operating system software was obtained via download from the Oracle E-Delivery Web site and made available to the host servers via an NFS mount.

Use the steps in section 2.6 to obtain Quick Fix 090406.

2.5 Physical Delivery of the TOE

To request the media pack:

1. Go to www.oracle.com and select Shop Online.

2. Choose the appropriate store and select Application Server.

3. Select Oracle Business Intelligence Suite Enterprise Edition Plus and choose your licensing terms.

4. Select 'Purchase Media Packs'.

5. Select Linux x86.

6. Select Oracle Business Intelligence (10.1.3) Media Pack for Linux x86 (32 bit).

When the media pack arrives the relevant CDs / DVDs are:

B45769-01 – Oracle® Business Intelligence Suite Enterprise Edition 10.1.3.3.2 for Linux x86.

B45770-01 – Oracle® Business Intelligence Suite Enterprise Edition 10.1.3.3.2 for Microsoft Windows.

Use the steps in section 2.6 to obtain Quick Fix 090406.

2.6 Delivery of Quick Fix 090406

Use the following procedure to obtain Quick Fix 090406:

1. Logon into metalink 3 Portal at:
   https://metalink3.oracle.com

2. Navigate to the Patches and Downloads tab

3. From the Patches and Downloads window, select the "Oracle, Siebel and Hyperion Products" hyperlink.

4. Click the "Simple Search" link

5. In the simple search window, populate the Patch Number field with the “Quick Fix 090406”. Select “Oracle Enterprise Linux” from the Platform/Language field. and hit the Go bottom. Please note patches are platform specific, so ensure proper platform is selected.

6. From the returned record set, hover the mouse pointer over the link under the patch column to display the download’s cksum number. This number should be recorded for later verification.

7. Click the hyperlink under the Patch column

8. In the resulting window, provide the password provided to you for the patch. Please note that passwords expire a week after they are generated.

9. A download button is displayed. Hover the mouse pointer over the download button to display the download’s cksum number. This number should be recorded for later verification.

10. Click the download button.

11. All patch downloads are provided in zip format.

12. Once the download is complete and the file has been transferred to the target environment, check the file with the cksum filename command to ensure that the download has not become corrupted. If the CKSUM numbers do not match, the file should be downloaded again.

13. Repeat this process for the Windows platform by repeating this procedure and substituting “Windows XP” for “Oracle Enterprise Linux” at step 5.

14. Unzip the Quick Fix into a known directory on machines 1, 2 and 5 ready for install in accordance with instructions in Annex I.

2.7 Additional Software for the TOE

The following supplementary software is required for the installation of the TOE:

- Oracle Enterprise Linux 4 Update 5 x86_64
- Oracle SOA Suite 10*g* (10.1.3.1.0) for Linux x86 (32-bit), part number B34625-01
- Oracle Database 10*g* Release 2 (10.2.0.1.0) for Linux x86_64, part number B24792-01
- Oracle Database 10*g* Release 2 (10.2.0.3.0) for Linux x86_64, MetaLink patch 5337014
- OPatch 10.2.0.0.0 for Linux x86_64, MetaLink patch 6880880
- MetaLink patch 5240469 for Linux x86_64
- Critical Patch Update April 2007 for Linux x86_64, MetaLink patch 5901891
- Oracle Identity Management Infrastructure and Oracle Identity Federation (10.1.4.0.1) for Linux x86 (32-bit), part numbers B30971-01 and B30972-01
- Oracle Application Server Companion CD 10*g* (10.1.2.0.2) for Linux x86 (32-bit), part numbers B24492-01 and B24493-01
- J2SE Development Kit 5 Update 16
- Oracle Database 10*g* Client Release 2 (10.2.0.1.0) for Microsoft Windows (32-bit), part number B24559-01
- Oracle Database 10*g* Client Release 2 (10.2.0.3.0) for Microsoft Windows (32-bit), MetaLink patch 5337014
- OPatch 10.2.0.0.0 for Microsoft Windows (32-bit), MetaLink patch 6880880
- Critical Patch Update April 2007 for Microsoft Windows (32-bit), MetaLink patch 5948242

3 Installation

This chapter describes the installation of the software for the evaluated configuration.

3.1 Operating System Installation / Configuration

Oracle Enterprise Linux Version 4 Update 5 shall be installed as described in Annex C and [ECGOEL4].

3.2 Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) Installation

Annex D describes the steps needed to install Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) on Oracle Enterprise Linux 4 Update 5. This annex should be followed to install Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) on machines 1, 2 and 5.

3.3 Oracle Database 10*g* Client Release 2 (10.2.0.3.0) Installation

Annex E describes the steps needed to install Oracle Database 10*g* Client Release 2 (10.2.0.3.0). This annex should be followed to install Oracle Database 10*g* Client Release 2 (10.2.0.3.0) on machines 1 and 2.

3.4 Oracle Database 10*g* Release 2 (10.2.0.3.0) Installation

Annex F describes the steps needed to install Oracle Database 10*g* Release 2 (10.2.0.3.0). This annex should be followed to install Oracle Database 10*g* Release 2 (10.2.0.3.0) on machine 3.

3.5 Oracle Internet Directory 10*g* (10.1.4.0.1) Installation

Annex G describes the steps needed to install Oracle Internet Directory 10*g* (10.1.4.0.1). This annex should be followed to install Oracle Internet Directory 10*g* (10.1.4.0.1) on machine 4.

3.6 Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2) Installation

Annex H describes the steps needed to install the Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2). This annex should be followed to install Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2) on machine 5.

3.7 Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Installation

Annex I describes the steps needed to install Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406. This annex should be followed to install Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 on machines 1 and 2.

3.8 Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Presentation Services Plug-In Installation

Annex J describes the steps needed to install Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Presentation Services Plug-In. This annex should be followed to install Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Presentation Services Plug-In on machine 5.

3.9 J2SE Development Kit 5.0 Update 16 Installation

Annex K describes the steps needed to install J2SE Development Kit 5.0 Update 16. This annex should be followed to install J2SE Development Kit 5.0 Update 16 on machine 6.

3.10 Oracle Database 10g Client Release 2 (10.2.0.3.0) Installation

Annex L describes the steps needed to install Oracle Database 10g Client Release 2 (10.2.0.3.0). This annex should be followed to install Oracle Database 10g Client Release 2 (10.2.0.3.0) on machine 6.

3.11 Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) Client Tools Installation

Annex M describes the steps needed to install Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) Client Tools. This annex should be followed to install Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Client Tools on machine 6.

3.12 IBM GSKit 7 Installation

Annex N describes the steps needed to install IBM GSKit 7. This annex should be followed to install IBM GSKit 7 on machines 1, 2 and 6.

4 Configuration

This part of the ECG describes the post-installation actions to complete the evaluated configuration.

4.1 Repository Configuration

The repository configuration will be performed using the client tools installed on the Windows XP Client machine (machine 6). The paint repository configuration below is provided as an example of how the repository setup should be done. The configuration is not intended to be used in a customer's environment.

4.1.1 Database Configuration for Paint Repository

To setup the paint repository create a schema, on the database server (machine 3), to hold the paint data:

```
sqlplus / as sysdba
create user paint identified by oracle10 quota unlimited on
users;
grant create session, create table to paint;
```

Connect as the `PAINT` user and run the following scripts:

```
@create_paint_tables.sql
@fact.sql
@forecast.sql
@market.sql
@period.sql
@product.sql
commit;
```

4.1.2 Database Configuration for Usage Tracking Repository

To setup the usage tracking repository create a schema, on the database server (machine 3), to hold the usage tracking data:

```
sqlplus / as sysdba
create user ut identified by oracle10 quota unlimited on users;
grant create session, create table, create view to ut;
```

Connect as the `UT` user and run the following scripts:

```
@SAACCT.Oracle.sql
@Oracle_create_nQ_Calendar.sql
@Oracle_create_nQ_Clock.sql
@Oracle_nQ_Calendar.sql
@Oracle_nQ_Clock.sql
commit;
```

Issue the following SQL:

```
create view NQ_LOGIN_GROUP as
select distinct USER_NAME as LOGIN, USER_NAME as RESP
from S_NQ_ACCT;
```

4.1.3 Database Configuration for Database Authorization

If database authorization is required a schema on the database server (machine 3) must be created:

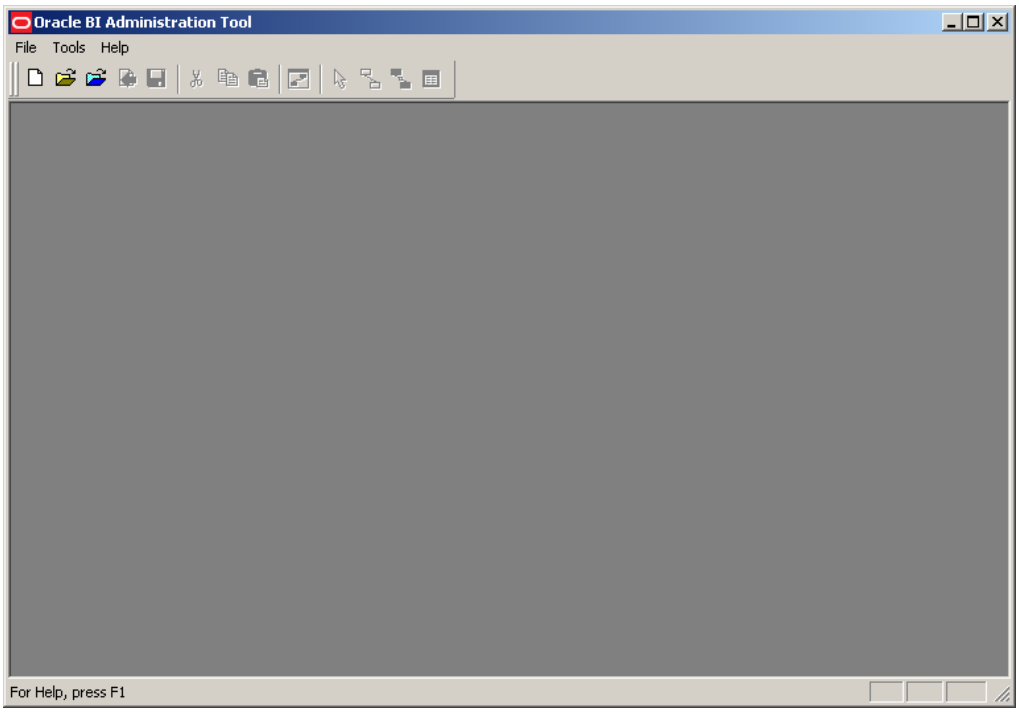
```
sqlplus / as sysdba
create user sa identified by oracle10 quota unlimited on users;
grant create session, create table to sa;
```

Connect as the SA user and issue the following SQL:

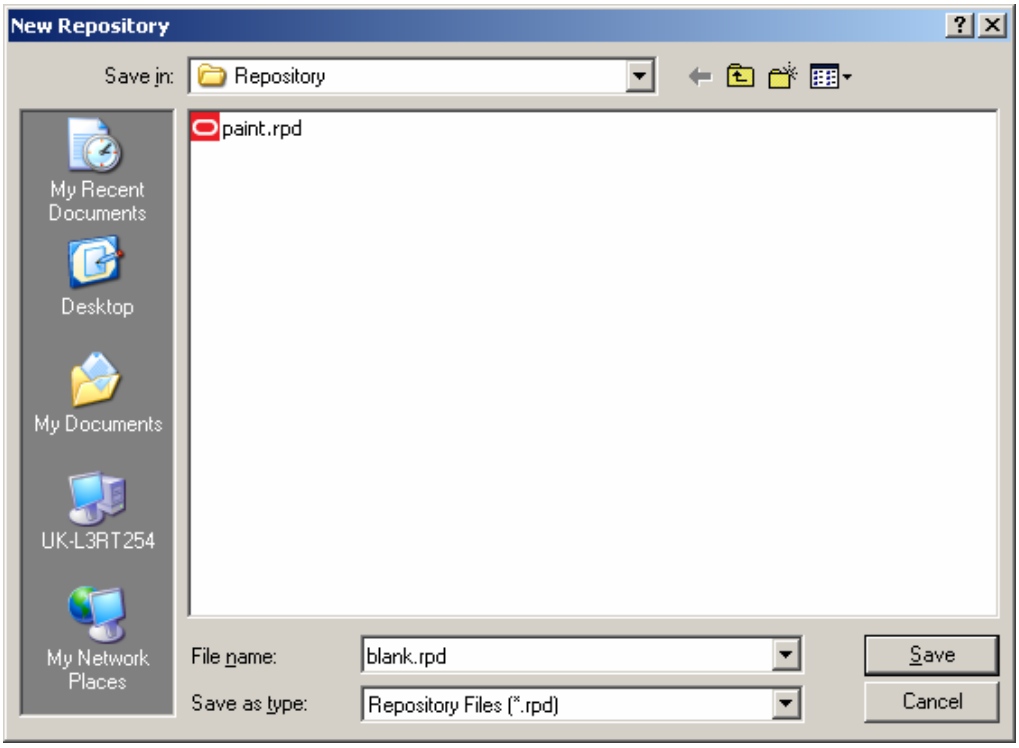
```
CREATE TABLE SA_USER_GROUP (
   GROUP_NAME     varchar2(40) NOT NULL,
   LOGON          varchar2(40) NOT NULL)
;
```

4.1.4 Create Blank Repository

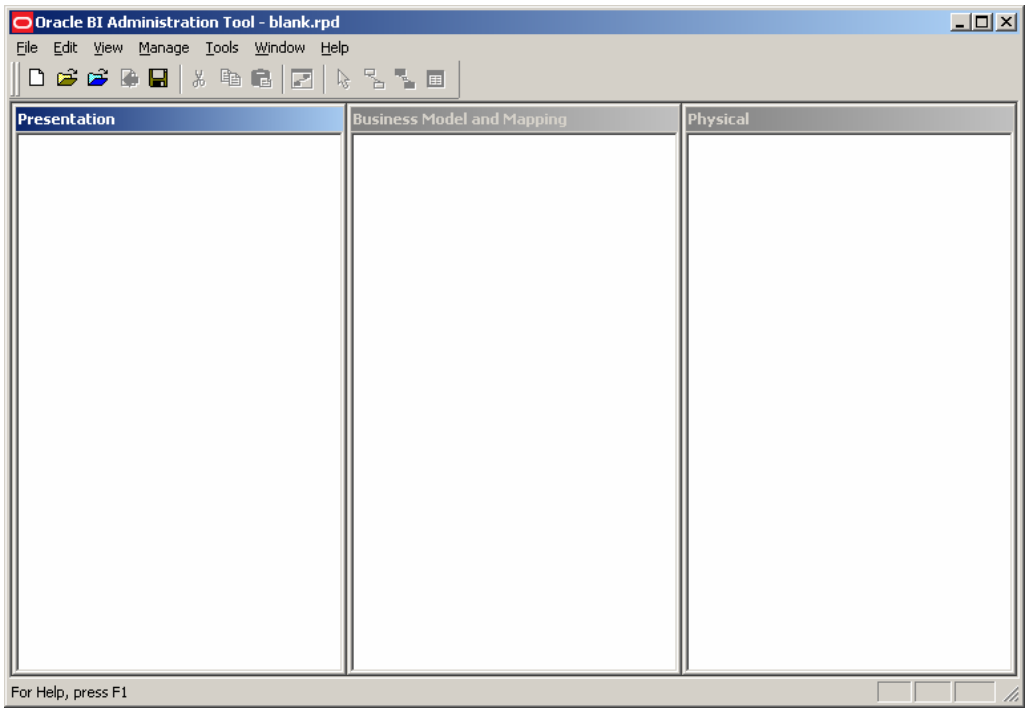
Open the BI Administration Tool (machine 6) by navigating to Start > Programs > Oracle Business Intelligence > Administration



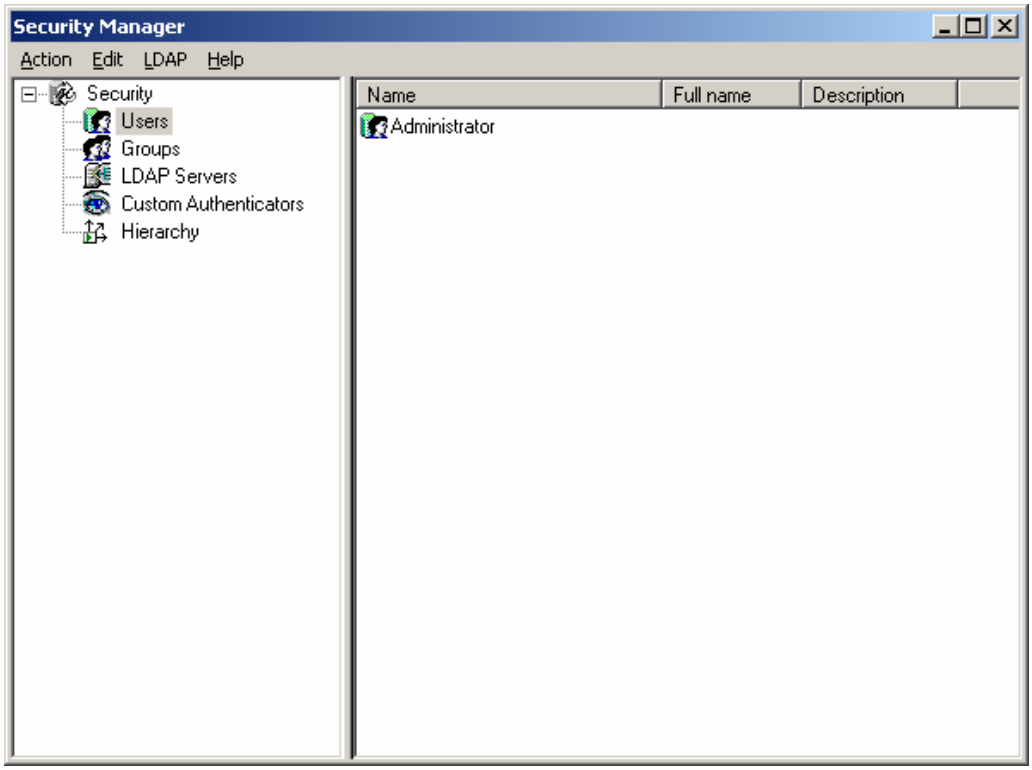
Click File > New



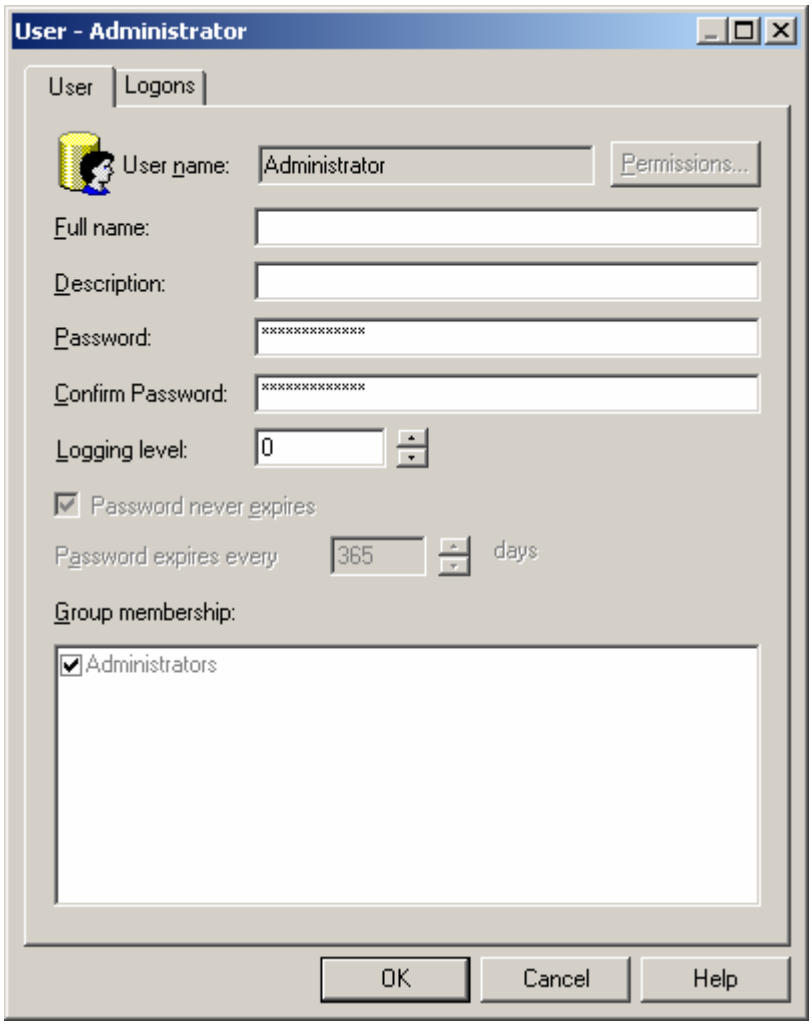
Enter **'blank.rpd'** in the **'File name'** field and click Save.



Click **'Manage'** > **'Security'**

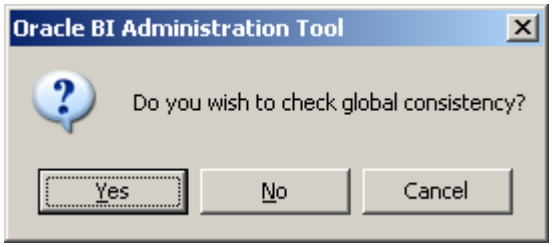


Select **'Users'** from the left-hand pane and double-click the **'Administrator'** user.

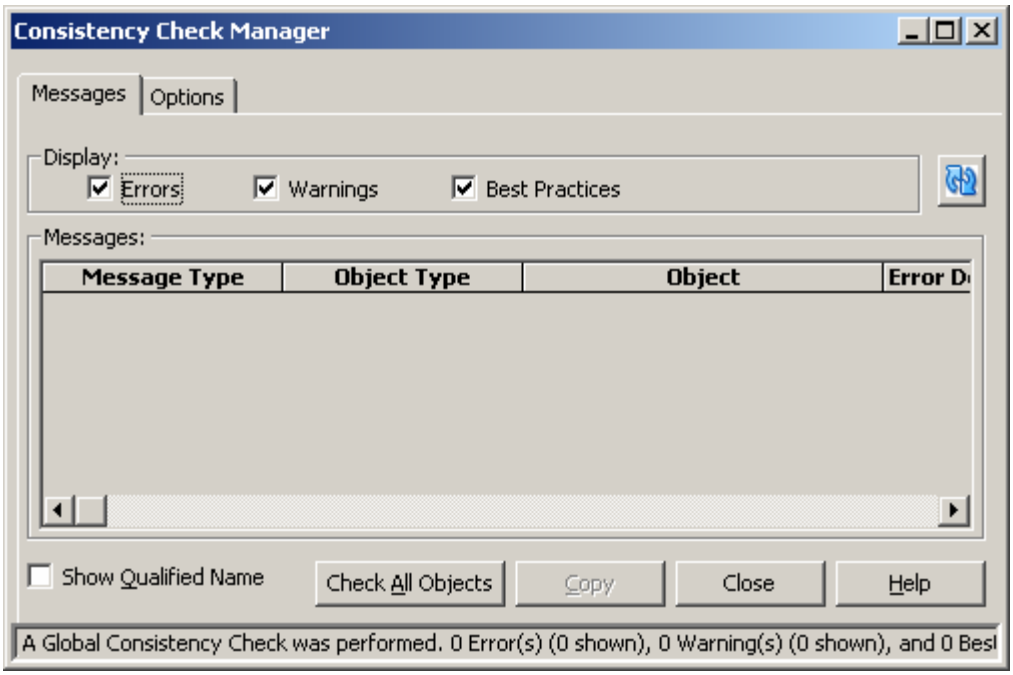


Enter a password into the **'Password'** and **'Confirm Password'** fields and click OK.

Close the Security Manager and save the blank repository.



Click **'Yes'** to check global consistency.

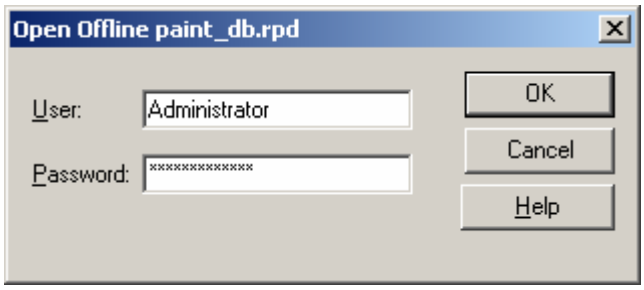


No errors should be shown. Click Close. Close the blank repository.

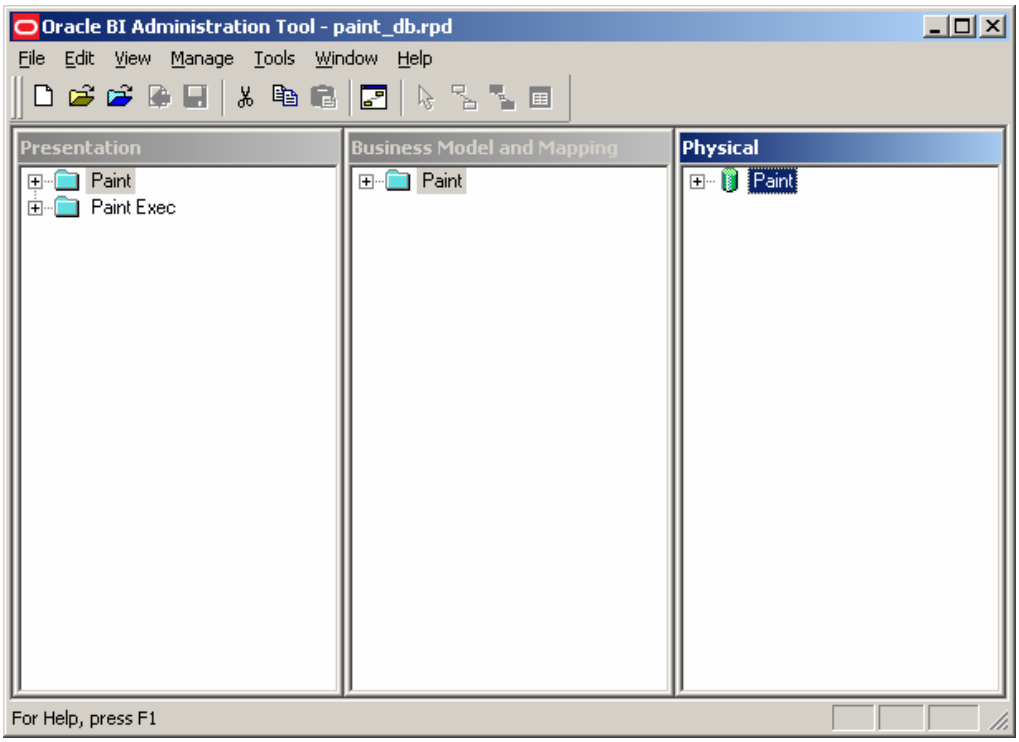
4.1.5 Merge Repositories

The paint and usage tracking repositories will be merged. Copy the repositories to the `C:\oracle\product\OBIEE\server\Repository` directory.

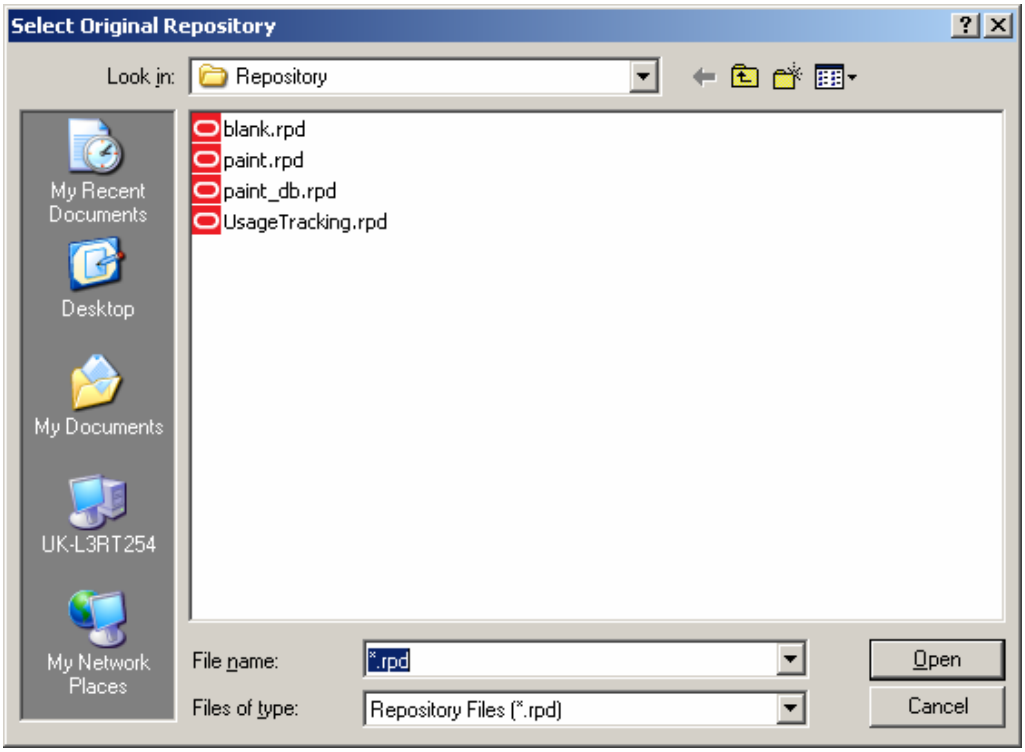
Use the BI Administration tool to open the **'paint_db'** repository.



The default password for the **'paint_db'** repository is **'Administrator'**.

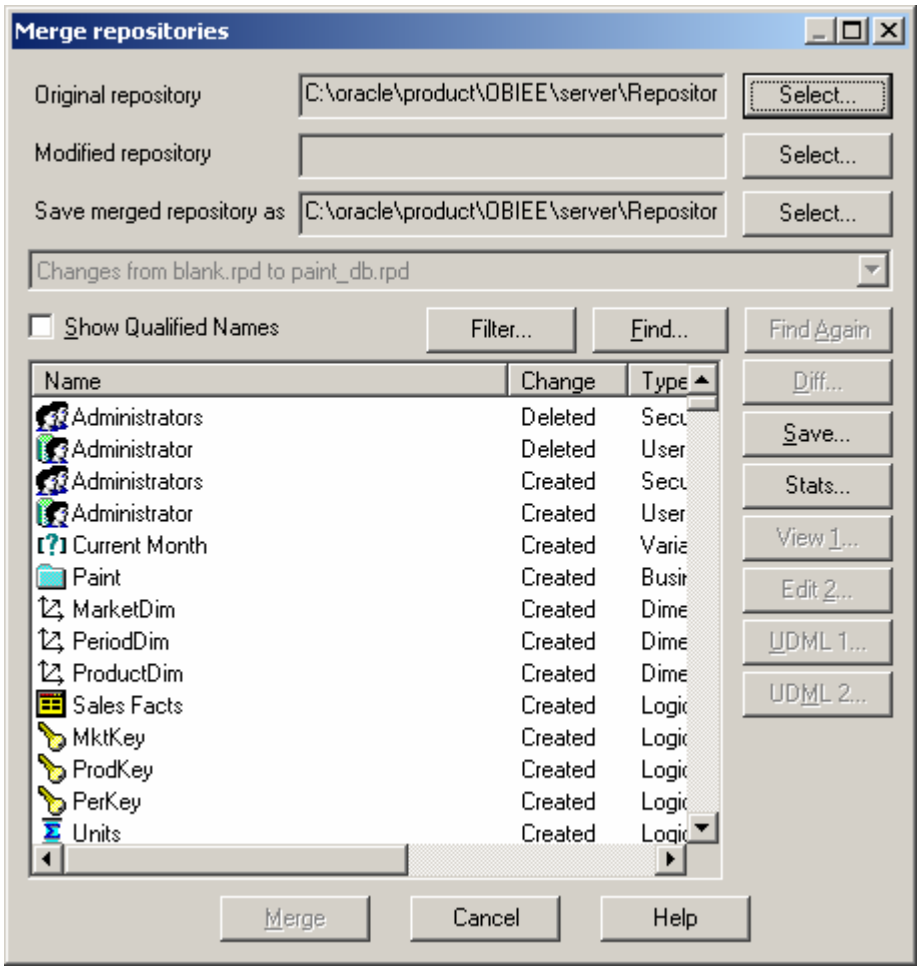


Click File > Merge

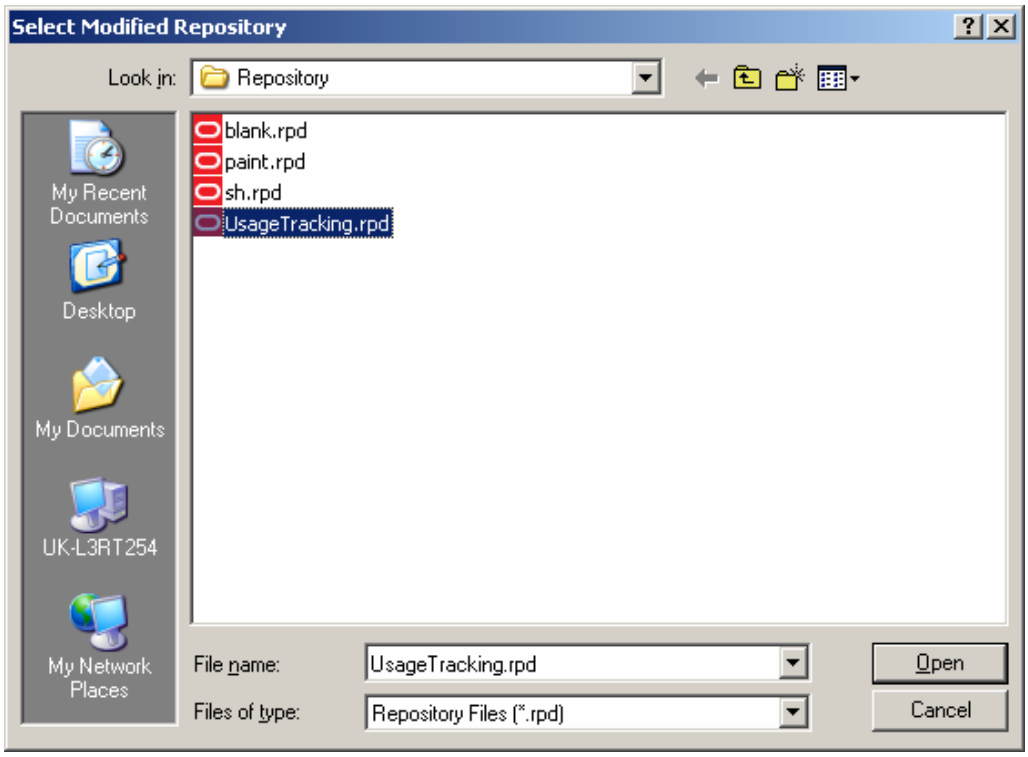


Select the **'blank.rpd'** file and click Open.

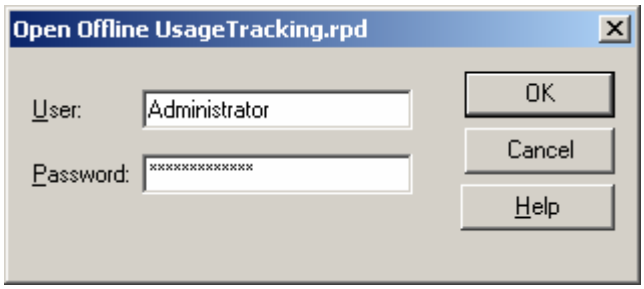
Enter the **'Administrator'** password for the **'blank'** repository.



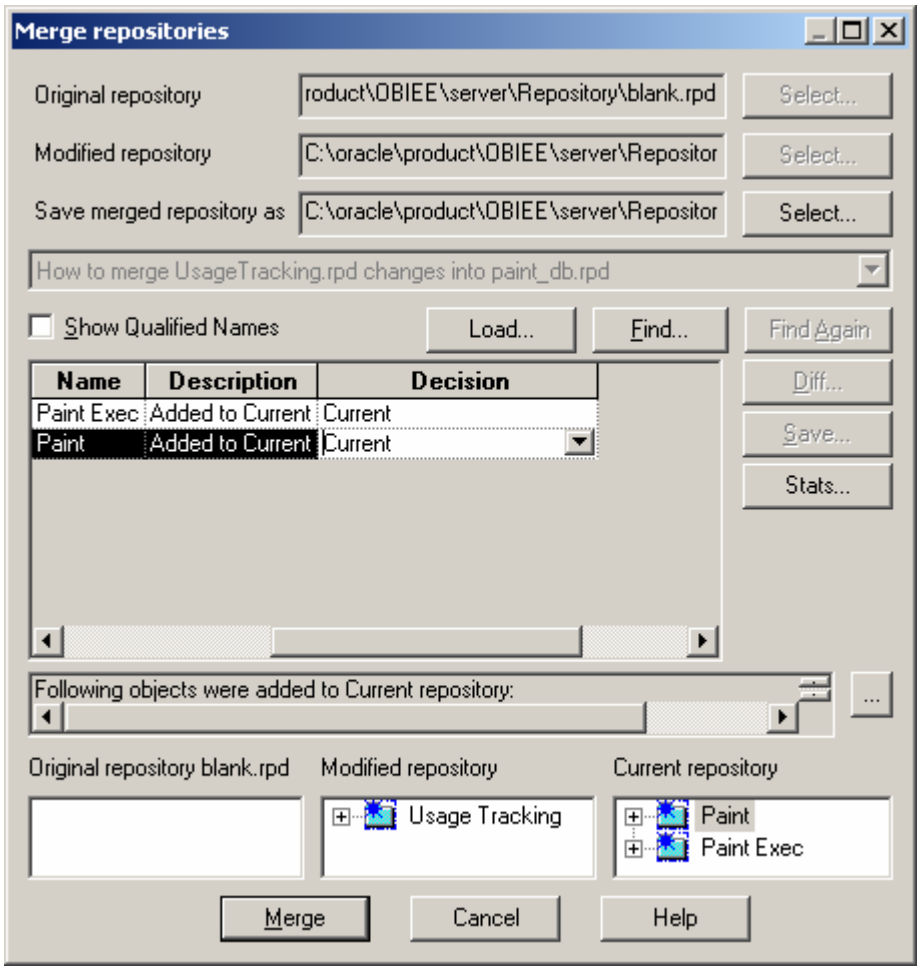
Click the **'Select…'** button for the Modified repository.



Select the **'UsageTracking.rpd'** repository and click Open.

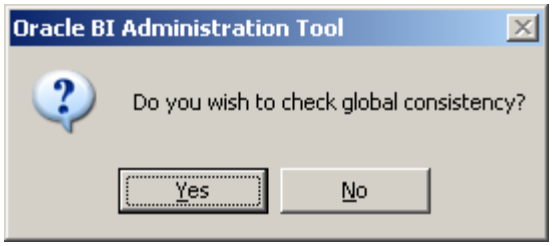


Enter the password for the **'Usage Tracking'** repository and click OK.

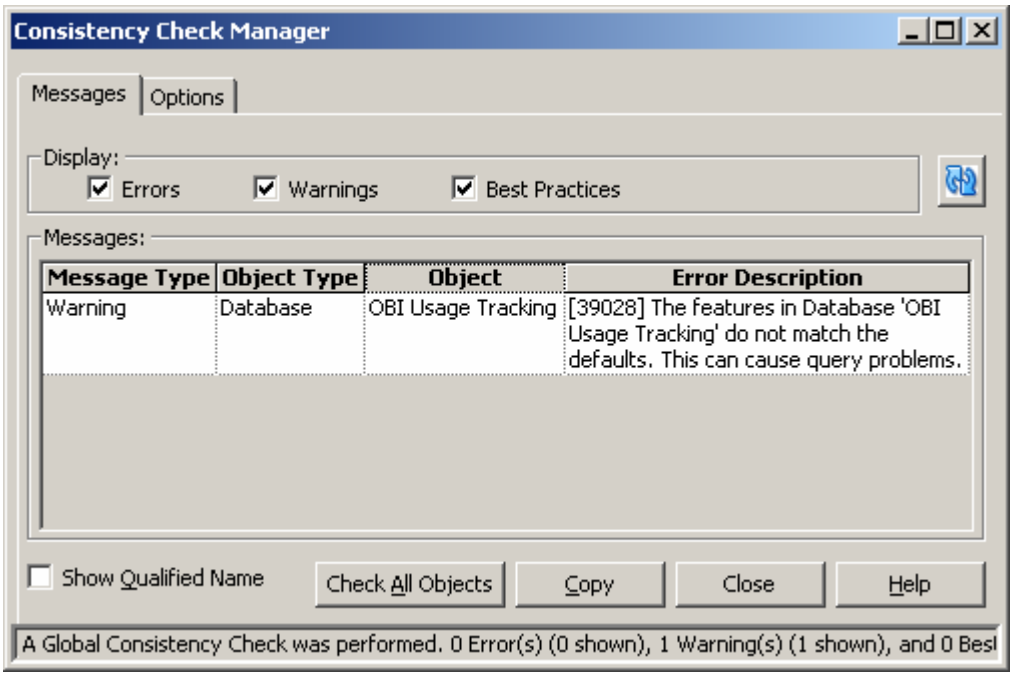


Scroll across to the 'Decision' column and select **'Current'** from the drop-down list from both rows.

Click Merge.

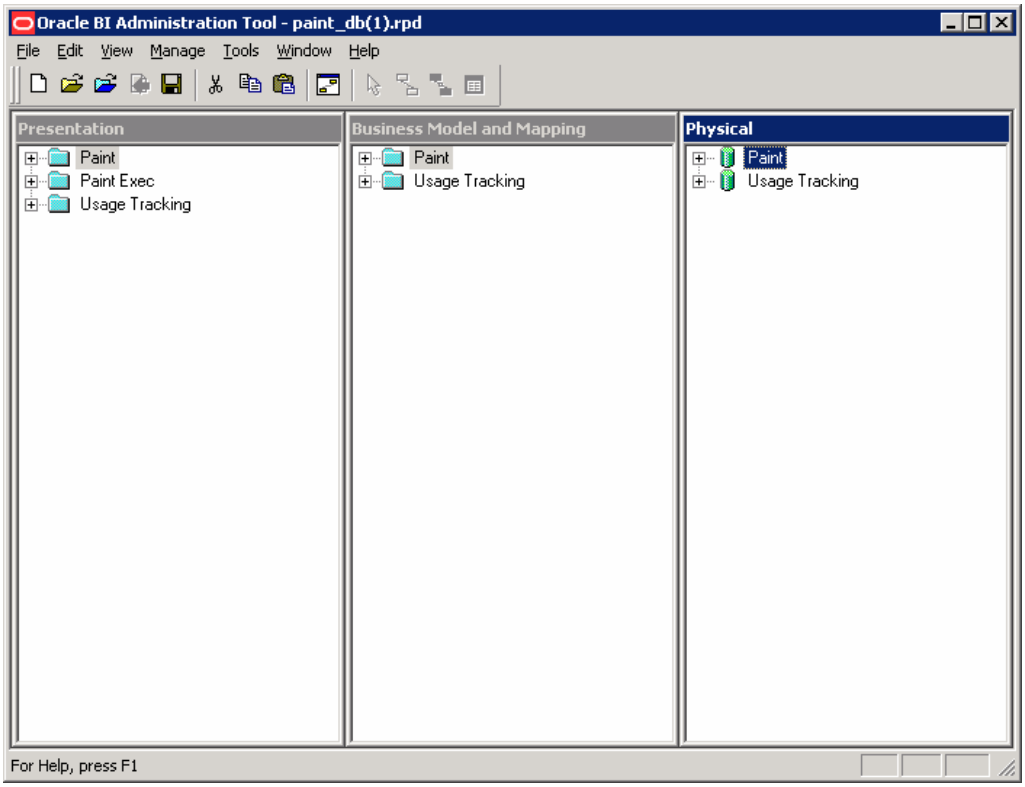


Click Yes

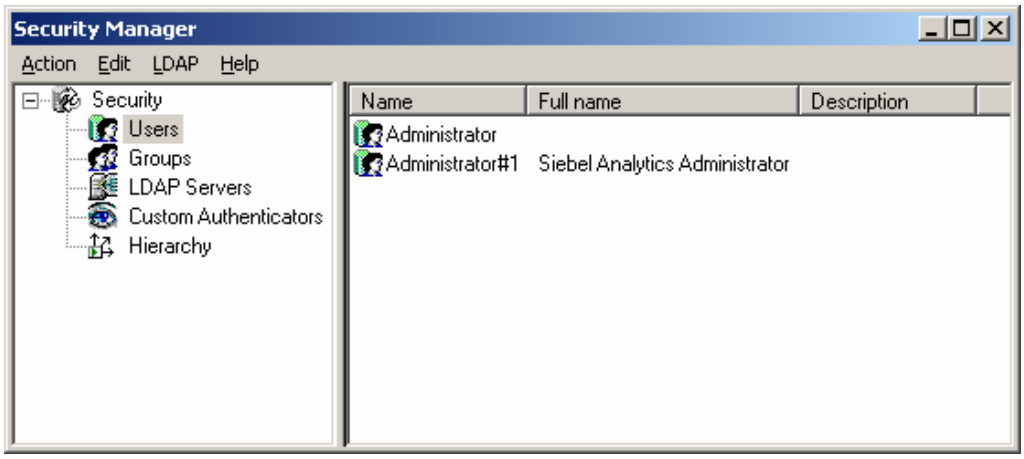


Ignore the error shown and click Close.

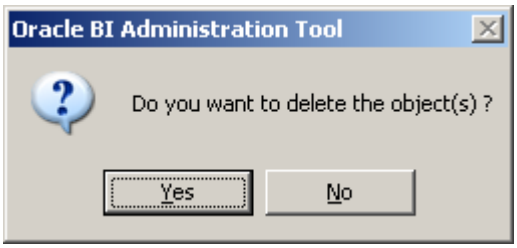
The merged repository is now available in the Oracle BI Administration Tool and is saved as `paint_db(1).rpd`.



Click Manage > Security

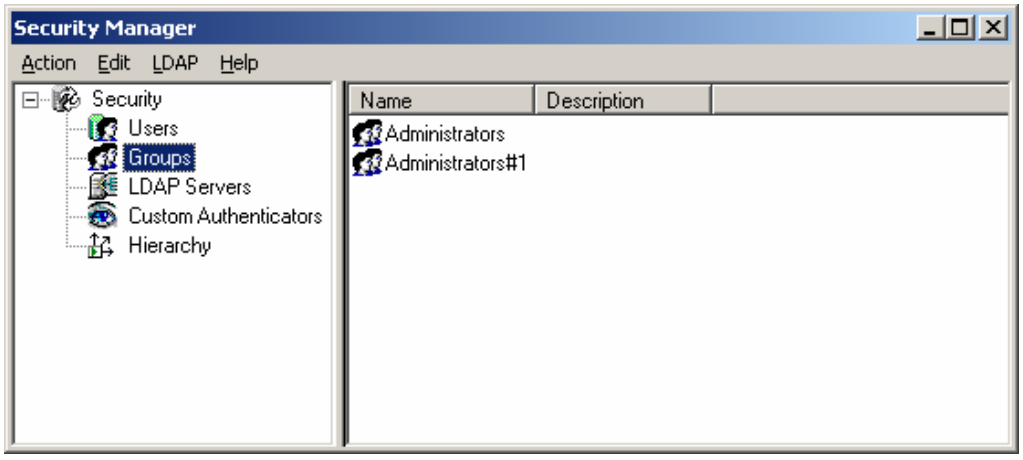


Delete the **'Administrator#1'** user by right-clicking the user and selecting **'Delete'**.

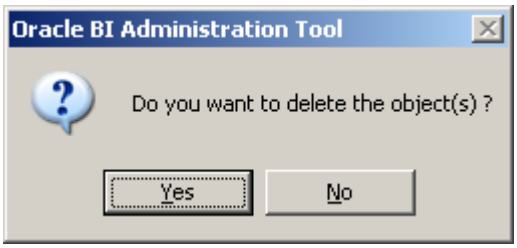


Click Yes.

Select **'Groups'** from the left-hand pane.



Delete the **'Administrators#1'** group by right-clicking the group and selecting **'Delete'**.



Click Yes.

Close Security Manager.

Click Manage > Variables

Click Repository > Variables > Static

Modify the value of the **'OLTP_USER'** variable to the name of the Usage Tracking schema (UT).

Modify the value of the **'OLTP_DSN'** variable to **'ORCL'**.

Modify the value of the **'DSN'** variable to **'ORCL'**.

Note: The values of the **'OLTP_DSN'** and **'DSN'** should be a valid TNS Names entry in the relevant `tnsnames.ora` file.

Click Action > Close.

In the Physical layer pane:

Expand the **'Paint'** folder and rename the connection pool named **'Connection Pool'** to **'Paint Connection Pool'**.

Rename the **'OBI Usage Tracking'** folder to **'Usage Tracking'**.

Expand the **Usage Tracking** > **Catalog** > **dbo** tree.

Rename the **'dbo'** folder to **'UT'**.

Drag and drop the **'UT'** folder so that the **'Usage Tracking'** folder is its parent.

Delete the **'Catalog'** folder and the connection pool named **'Usage Tracking Writer Connection Pool'**.

Rename the connection pool named **'Connection Pool'** to **'Usage Tracking Connection Pool'**.

Double-click the **'Usage Tracking'** folder.

Select **'Oracle 10g R2/11g'** from the Database select list.

Click the **'Set…'** button.

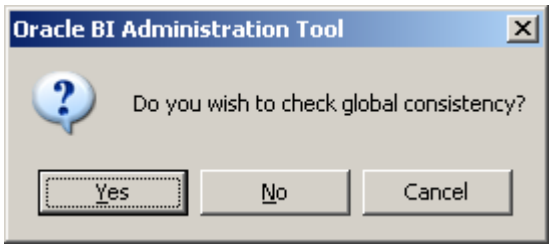
Click OK.

Double-click the **'Usage Tracking Connection Pool'** entry for **'Usage Tracking'**

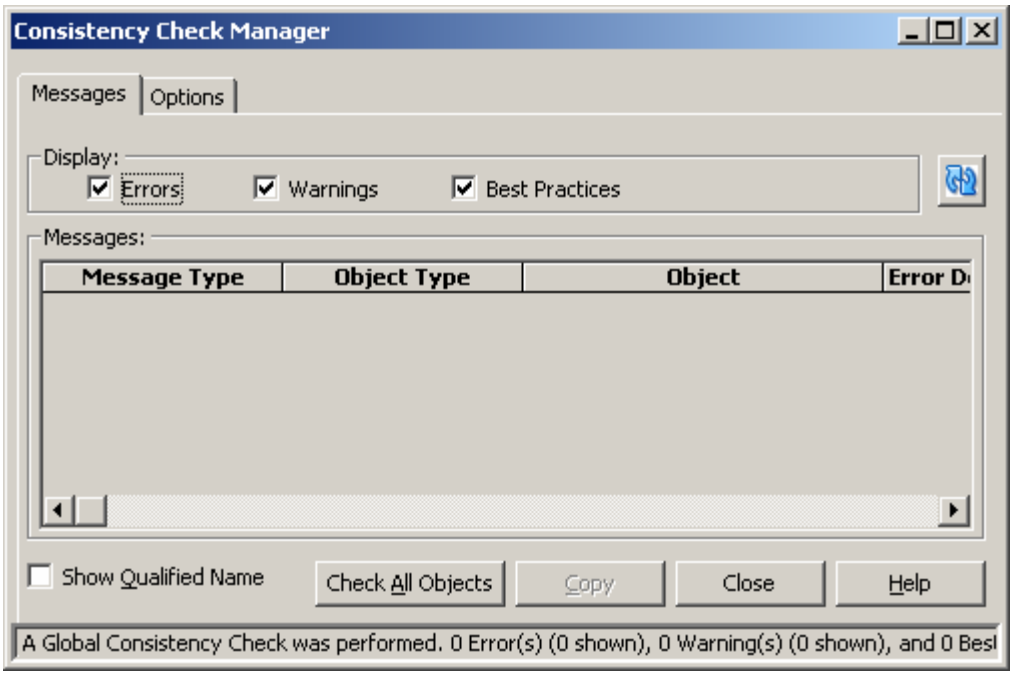
Update the password field with the password for the UT schema.

Click OK.

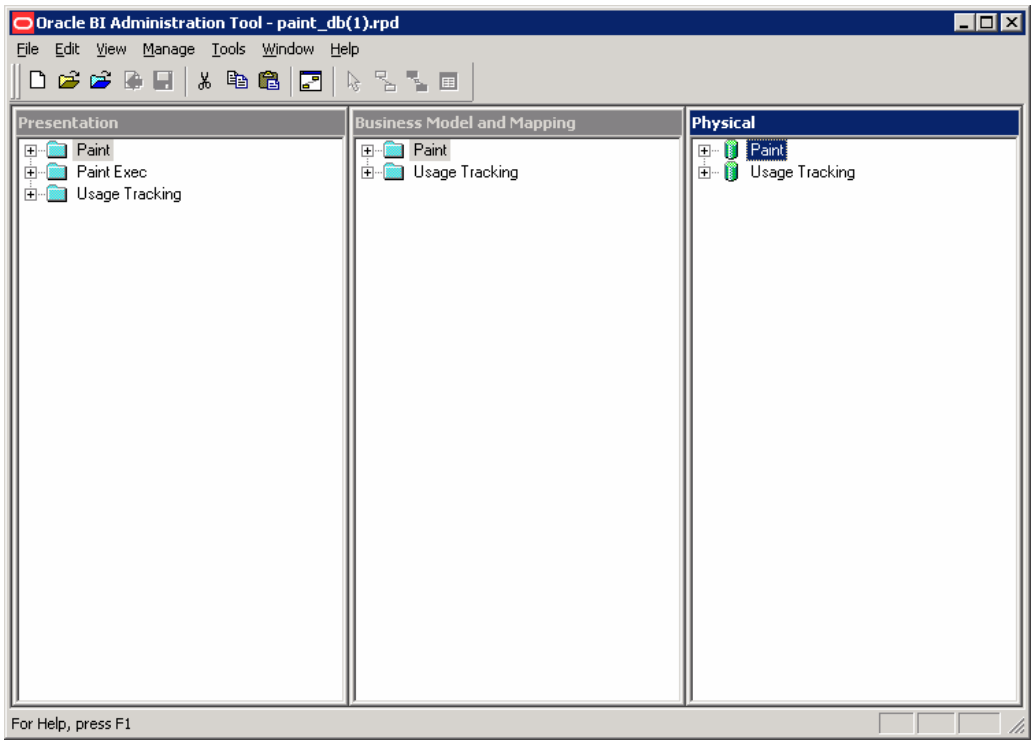
Click File > Save.



Click Yes.



Click Close.

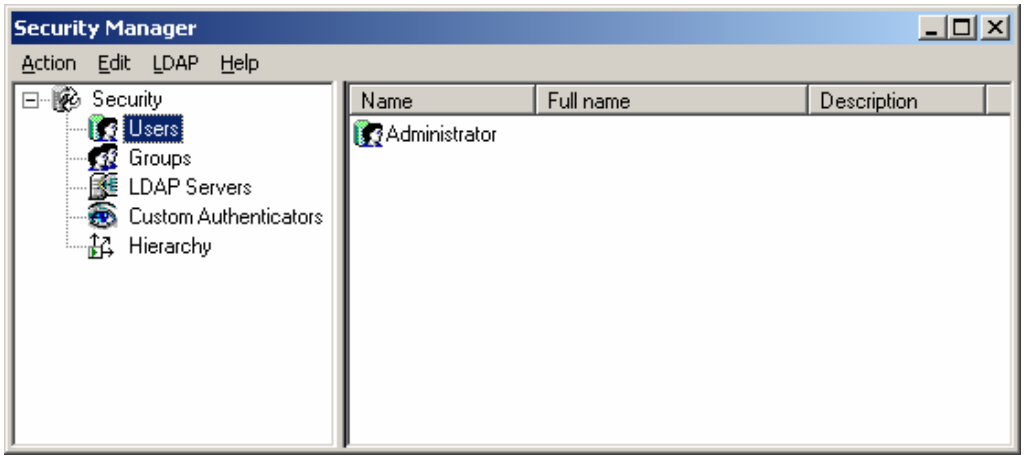


Save the repository twice, once as `oid_obiee.rpd` and once as `db_obiee.rpd`.

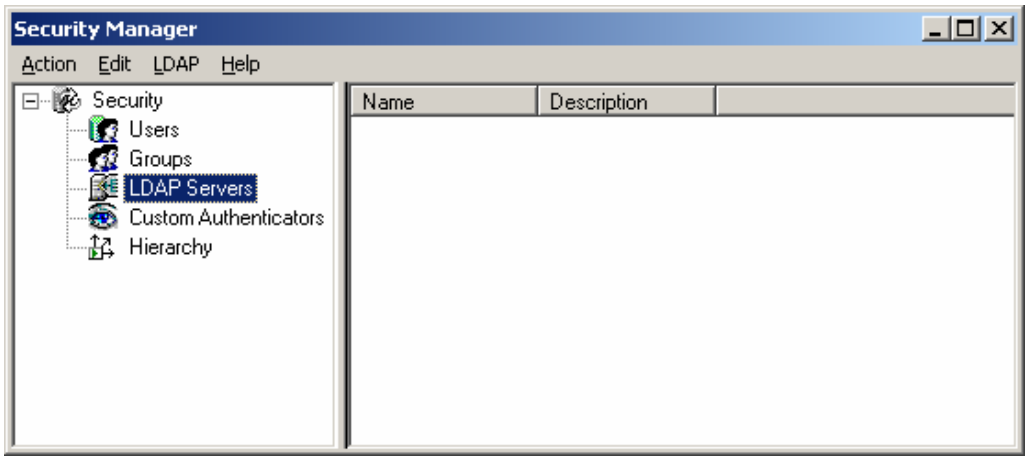
4.1.6 Configure LDAP Authentication and Authorization

Open the `oid_obiee.rpd` repository file.

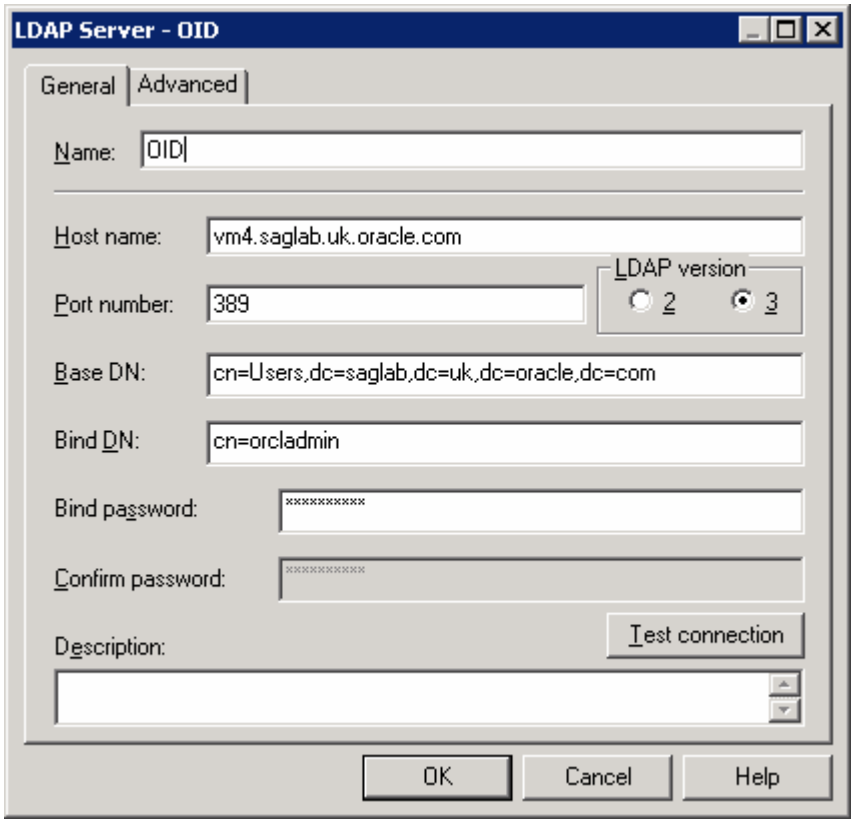
Click Manage > Security.



Select **'LDAP Servers'** from the left hand pane.



Right-click in the right-hand pane and select **'New LDAP Server…'**



Enter **'OID'** in the Name field.

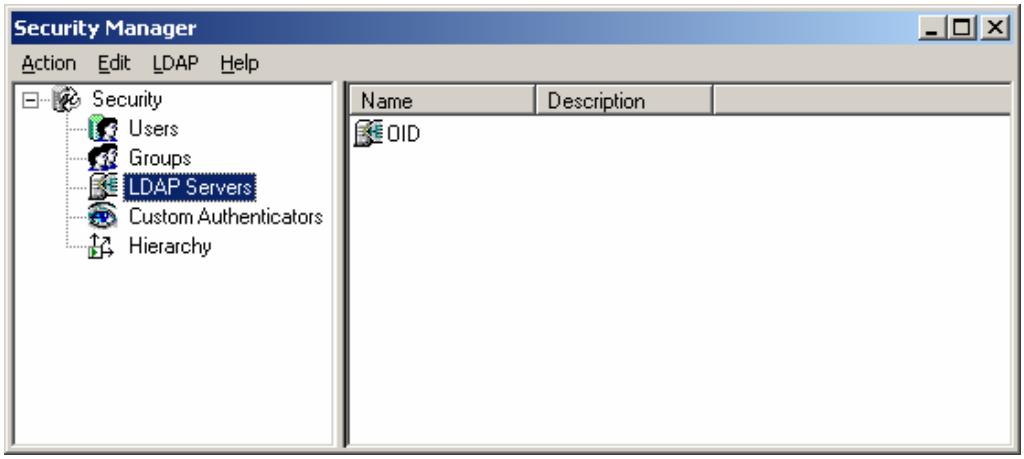
Enter the correct parameters for the **'Host name'**, **'Port number'**, **'Base DN'**, **'Bind DN'**, **'Bind password'** and **'Confirm password'** fields for the LDAP Server.

Click the **'Test connection'** button.

You should see the **'LDAP Server connected successfully'**.

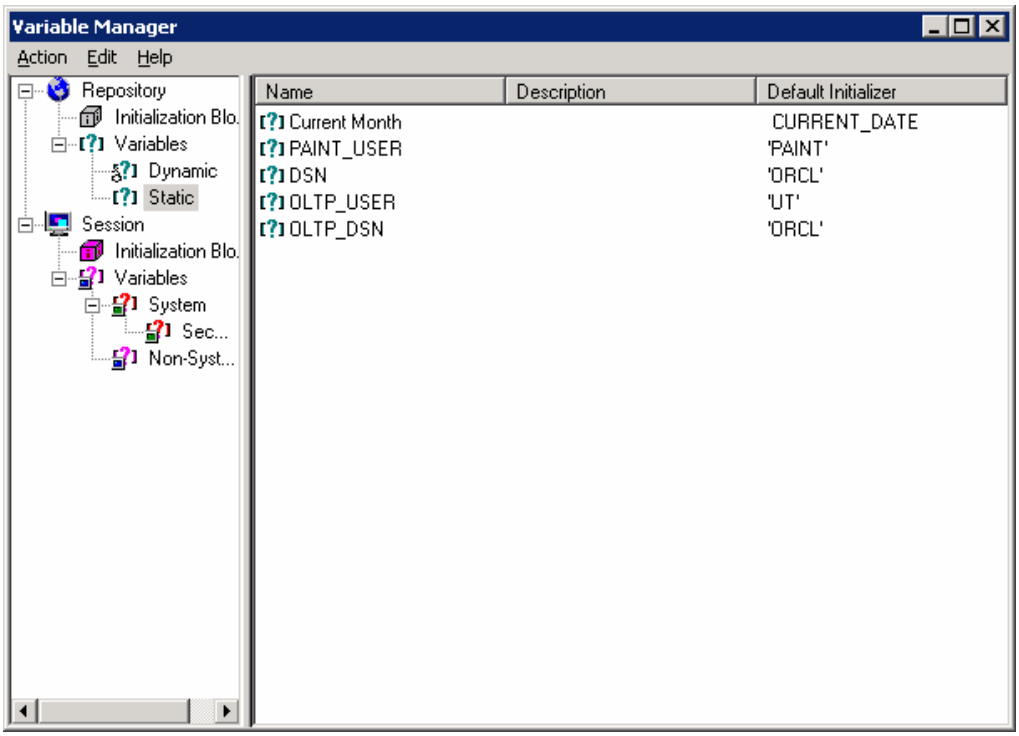
Click OK on the Oracle BI Administration Tool dialog box.

Click OK on the LDAP Server – OID dialog box.



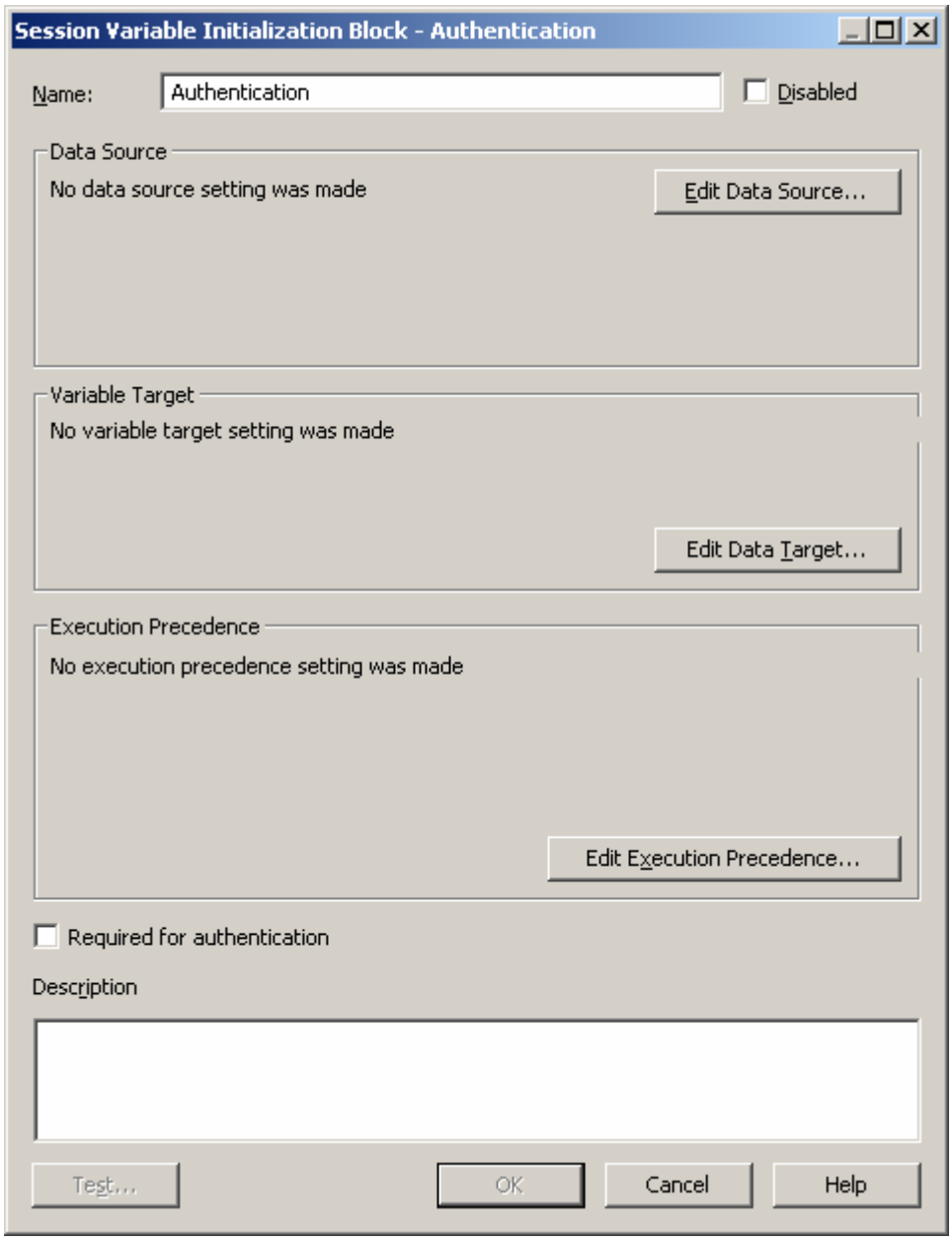
Click Action > Close in the Security Manager window.

From the Administration Tool main menu select Manage > Variables.



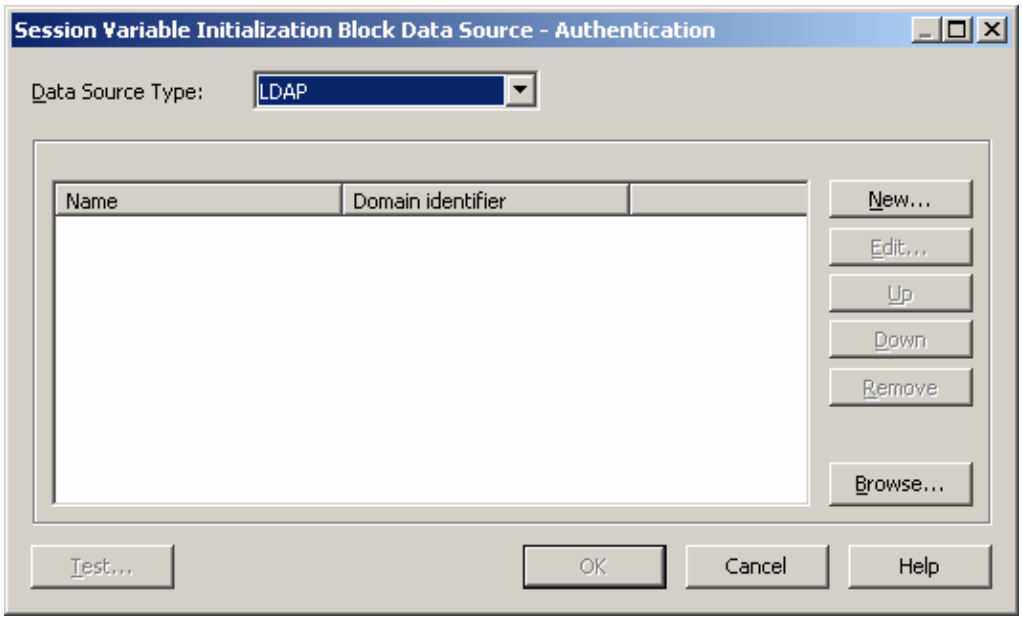
Click the Session > Initialization Blocks link.

Right-click in the right hand pane and select **'New Initialization Block'**.



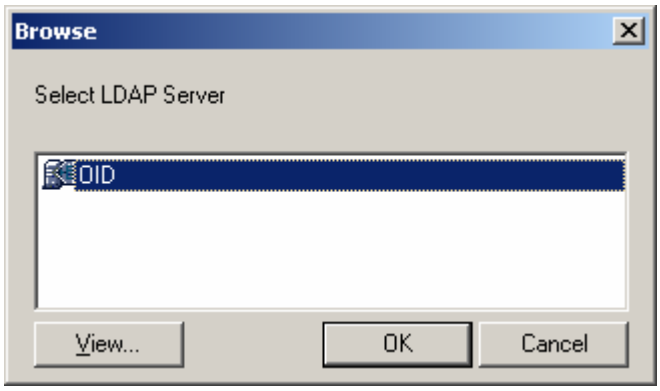
Enter **'Authentication'** in the Name field.

In the **'Data Source'** region press the **'Edit Data Source'** button.

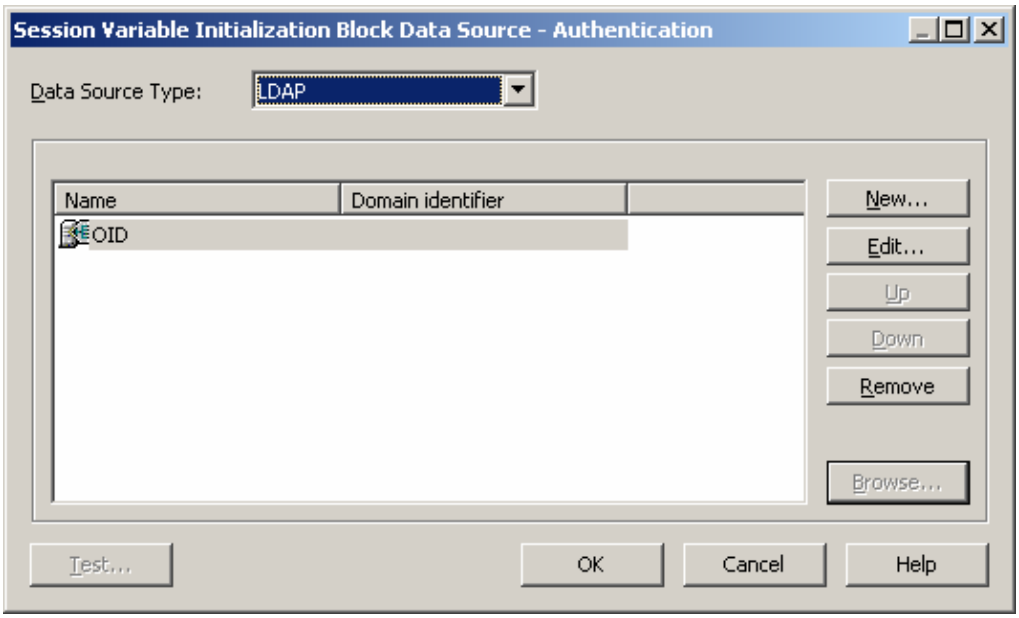


Select **'LDAP'** from the **'Data Source Type'** drop down list.

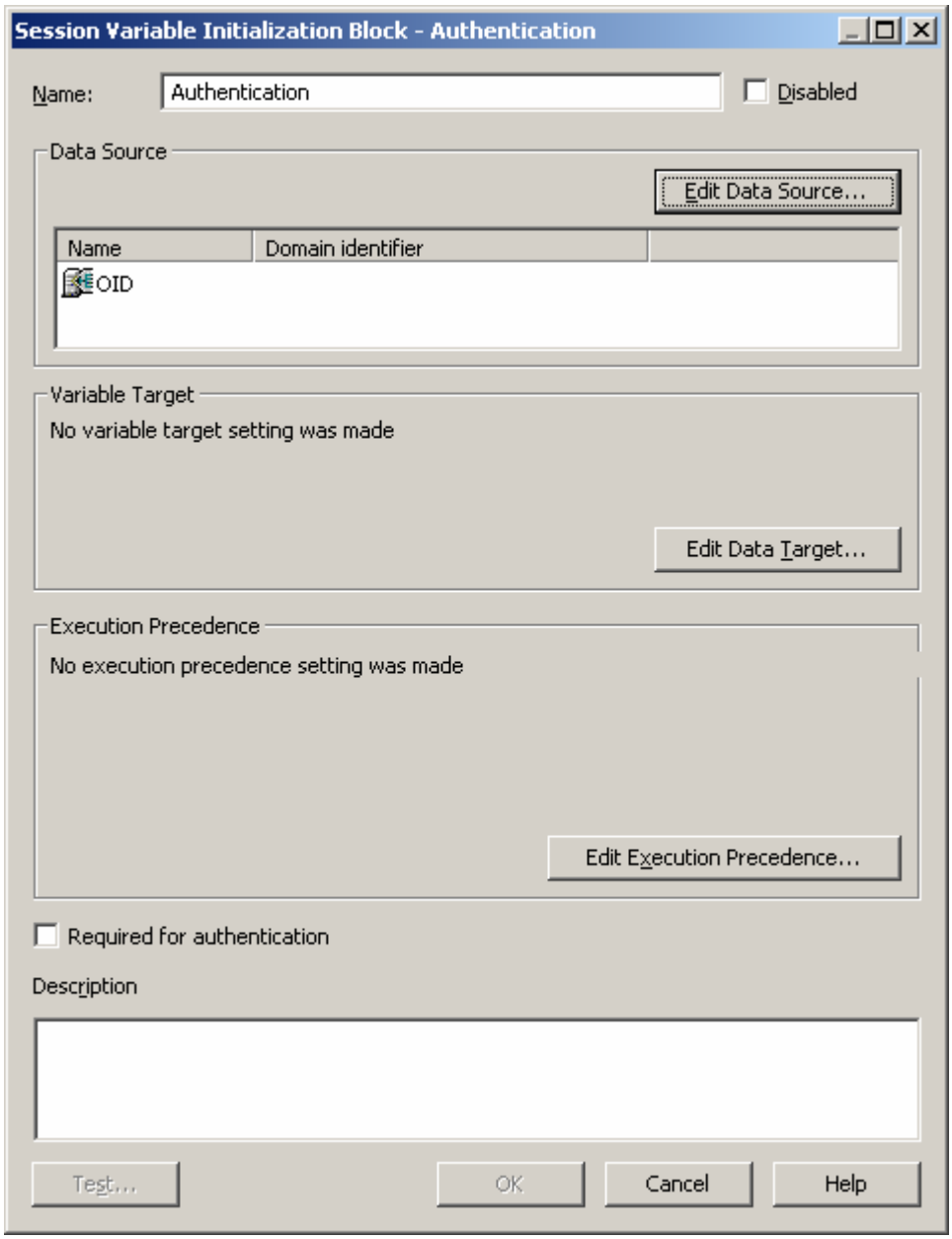
Click the Browse button



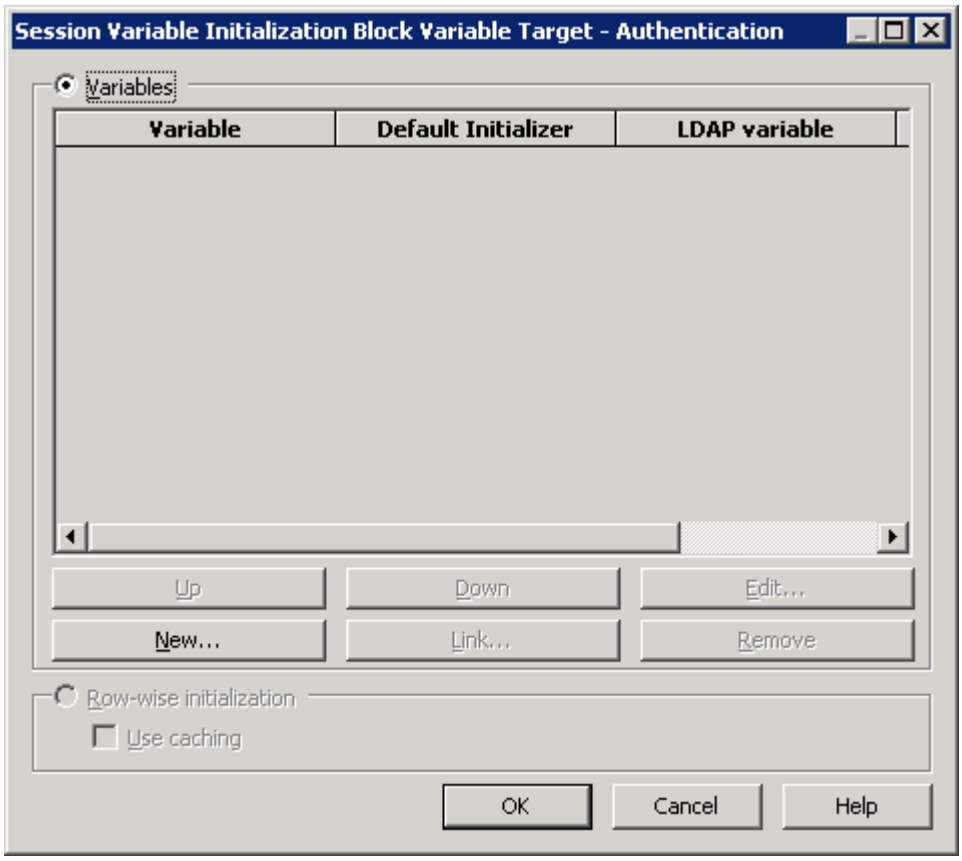
Select the LDAP Server that was setup previously. Click OK on the Browse dialog box.



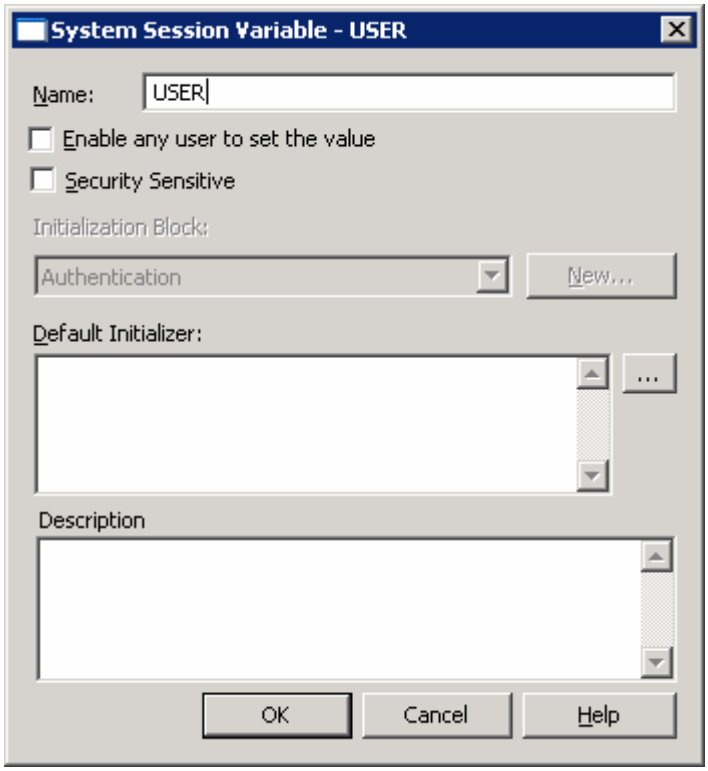
Click OK.



In the **'Variable Target'** region press the **'Edit Data Target'** button.

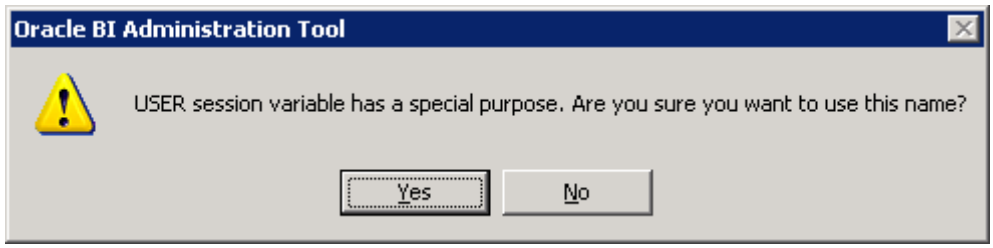


Click **'New…'**

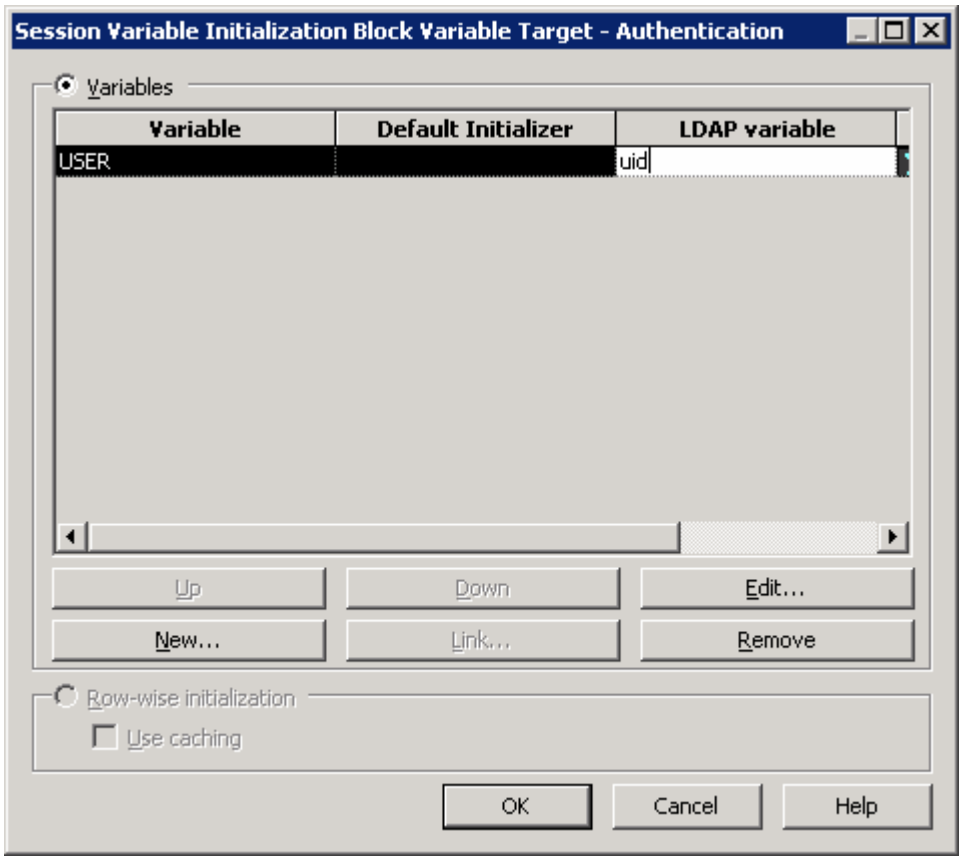


Enter **'USER'** in the Name field.

Click OK on the **'System Session Variable'** dialog box.



Click **'Yes'**.

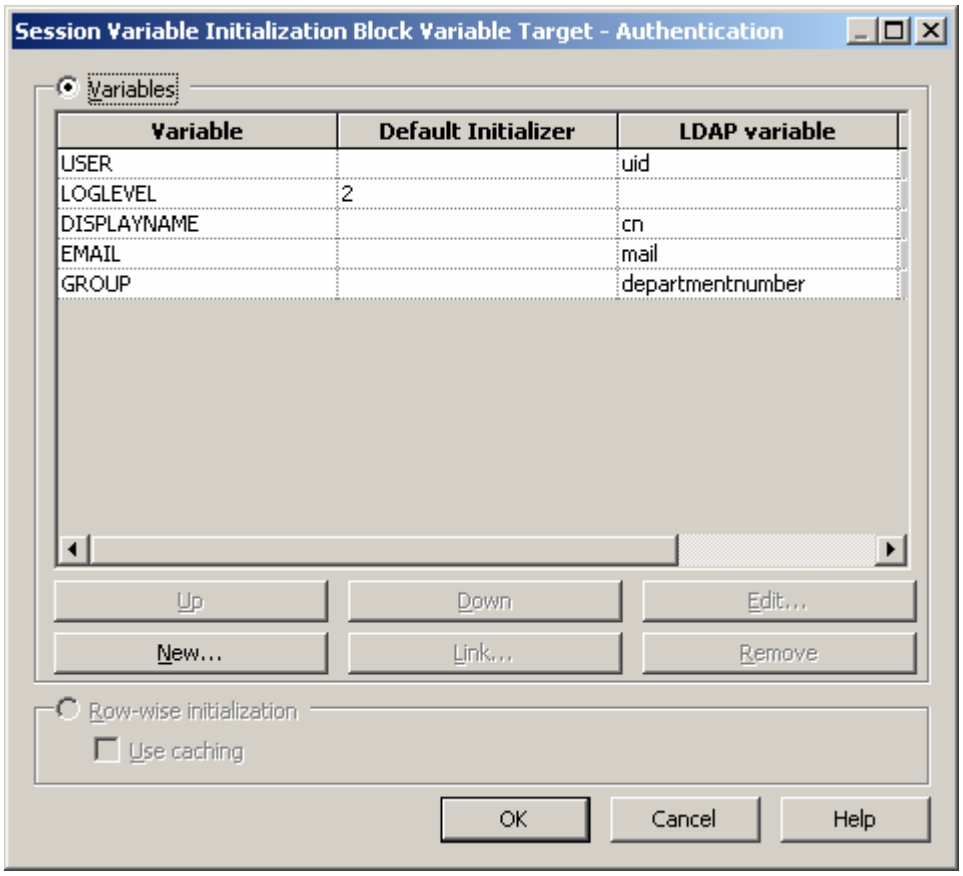


Enter **'uid'** in the LDAP variable field for the **'USER'** variable.

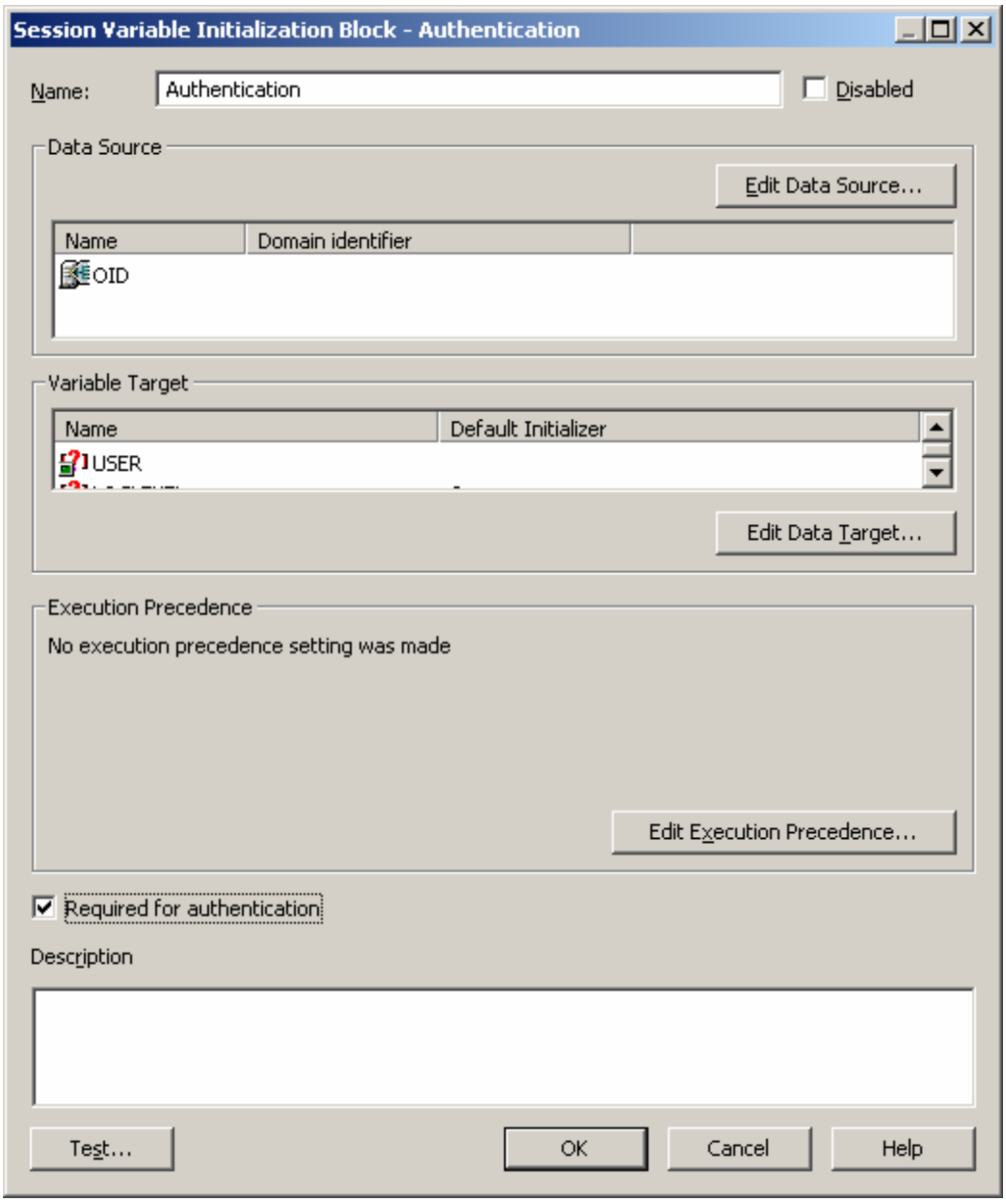
Repeat the process for the following variables:

Variable	Default Initializer	LDAP variable
LOGLEVEL	2	
DISPLAYNAME		cn
EMAIL		mail
GROUP		departmentnumber

Once all the variables have been created you should see the dialog below:

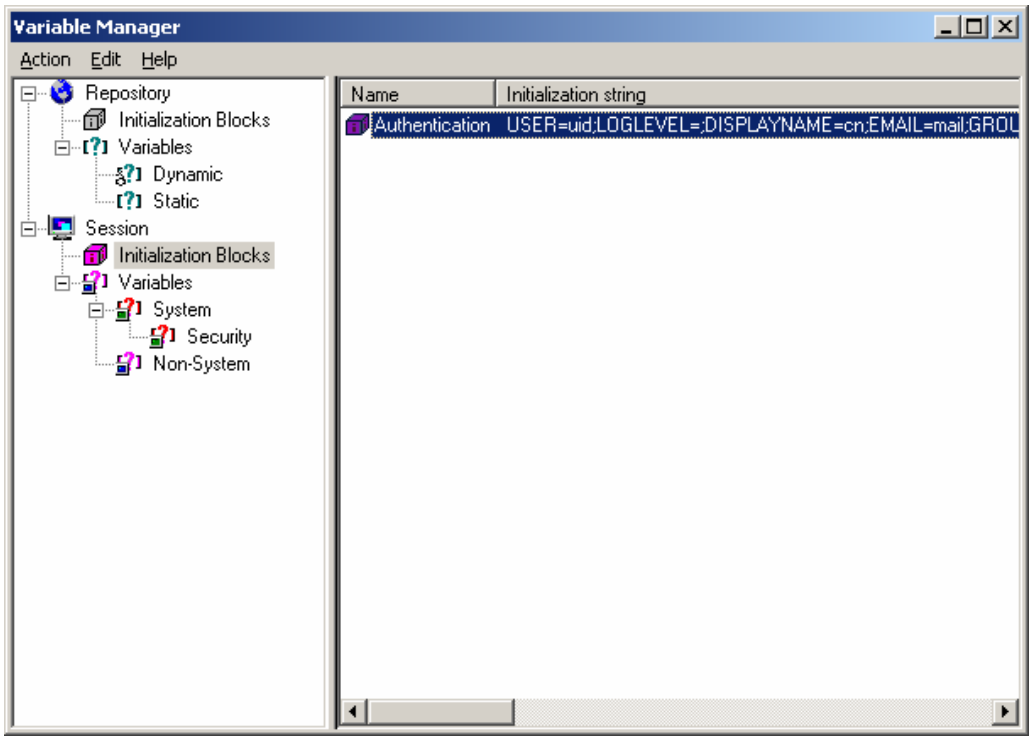


Click OK on the **'Session Variable Initialization Block Variable Target'** dialog box.



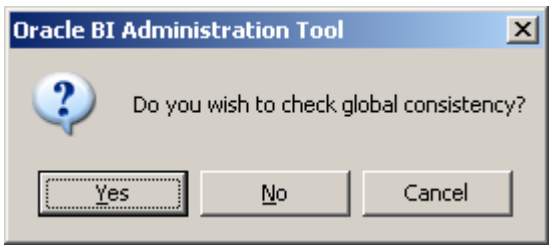
Click the **'Required for Authentication'** tick box. This directly affects the behaviour of authentication and the check box ***must*** be ticked.

Click OK on the **'Session Variable Initialization Block'** dialog box.

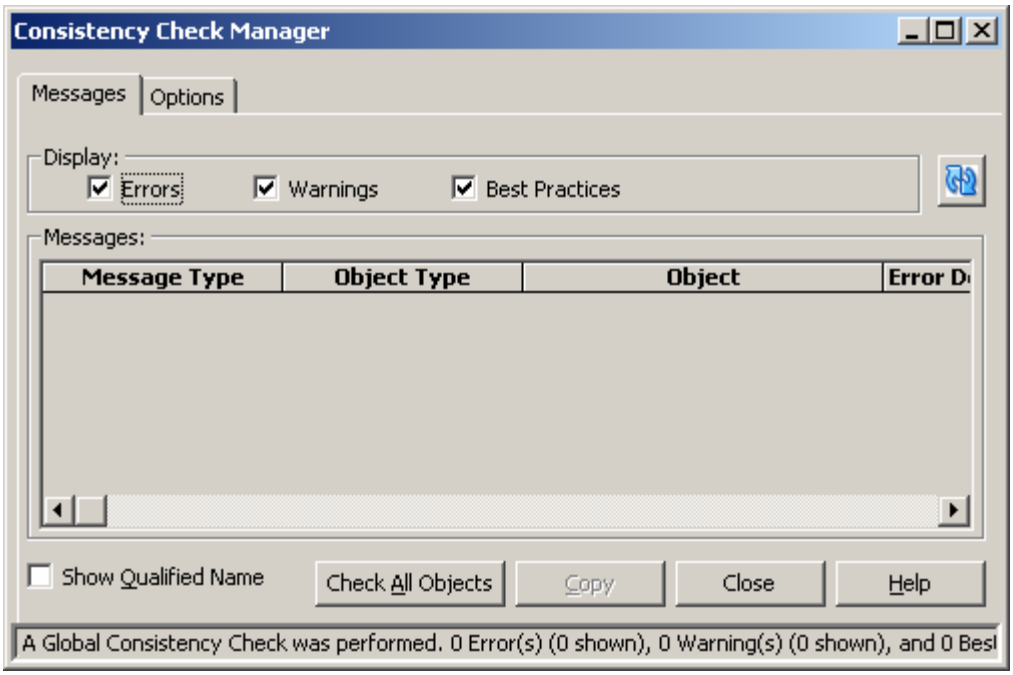


Click Action > Close in the **'Variable Manager'** window.

Click File > Save.



Click 'Yes'.



Click Close.

Click File > Close.

4.1.7 Configure Database Authentication and Authorization

Open the `db_obiee.rpd` file.

Create a new static variable **'SA_USER'** with its value set as the name of the SA System schema.

Add the SA System table `SA_USER_GROUP` to the repository by clicking File > Import > from Database…

Select **'OCI 10g/11g'** from the **'Connection Type'** select list.

Enter **'ORCL'** in the **'TNS Name'** field.

Enter **'SA'** in the **'User Name'** field and the password for the **'SA'** schema in the **'Password'** field.

Click OK.

Click the **'SA'** folder and click Import.

Make the following changes in the **'Connection Pool'** dialog box:

Change the value of the Name field to **'SA System Connection Pool'**.

Change the value of the Data source name field to **'VALUEOF(OLTP_DSN)'**.

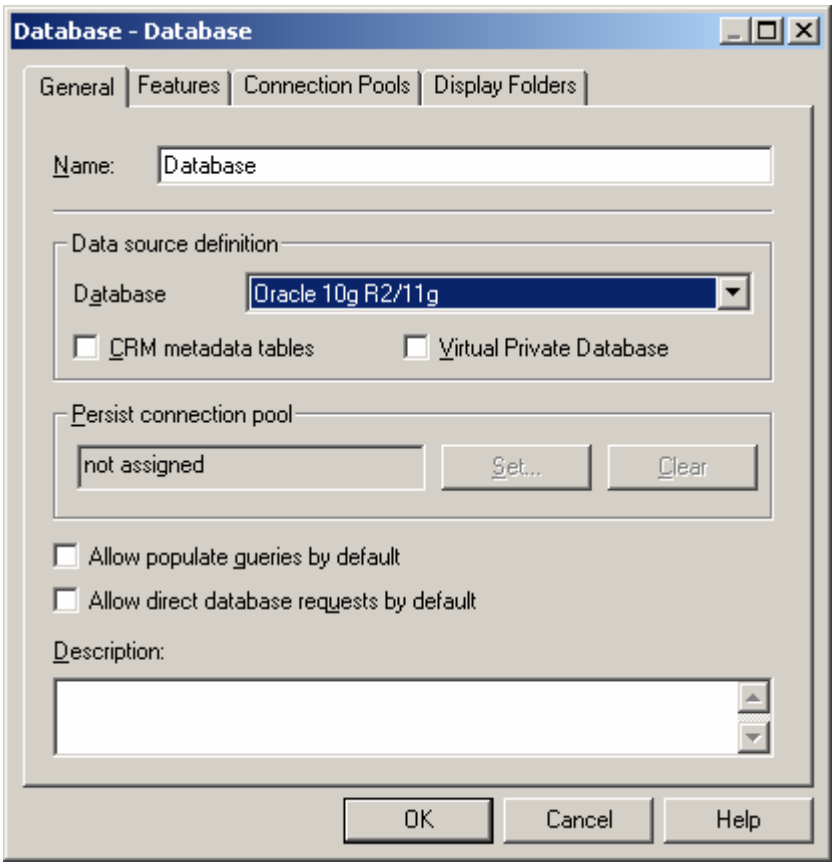
Change the value of the User name field to **'VALUEOF(SA_USER)'**.

Click OK.

Click Close on the Import window once the import process has completed.

In the Physical layer rename **'ORCL'** to **'SA System Database'**.

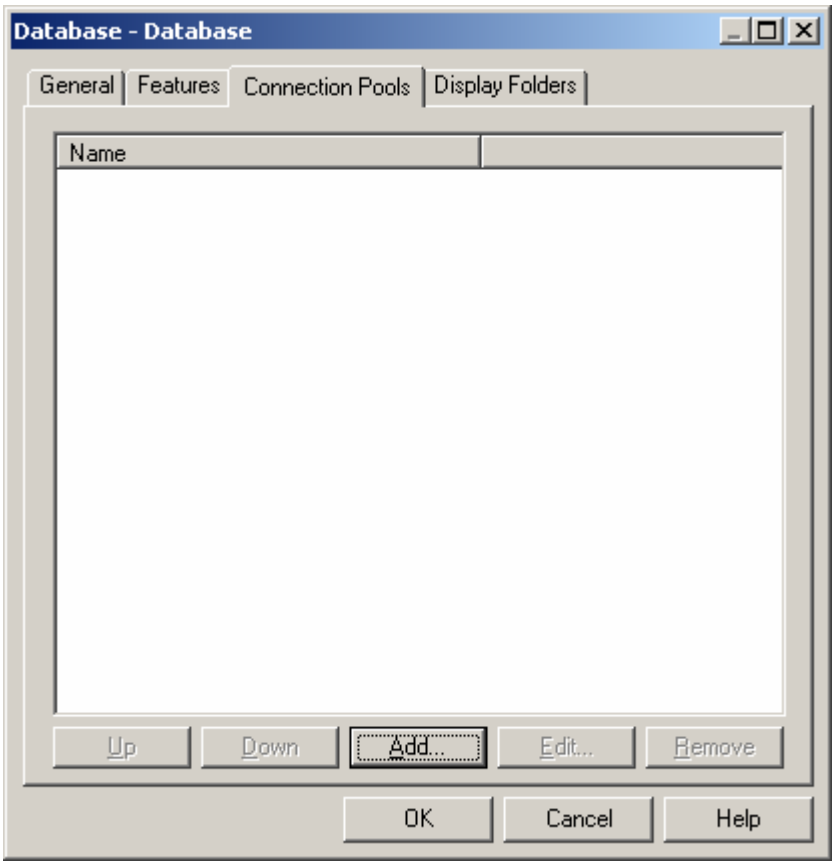
In the Administration Tool right-click in the Physical layer and click **'New Database…'**



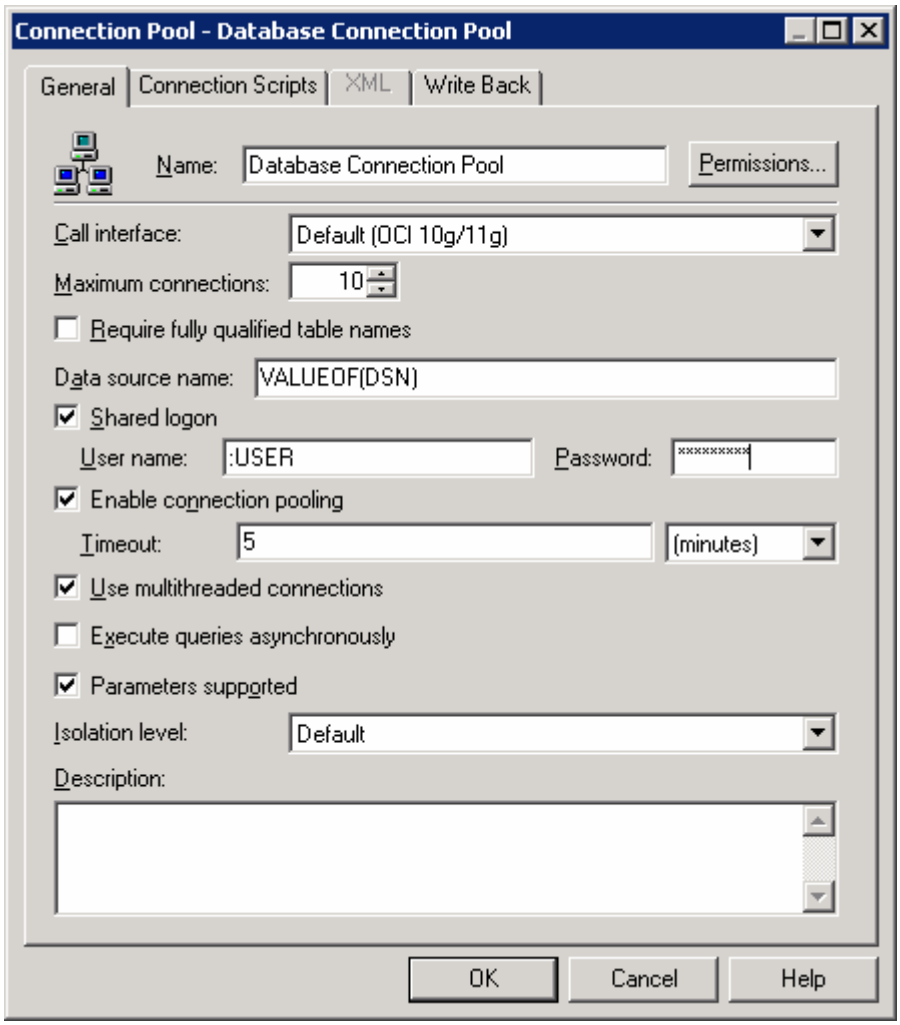
In the Name field enter **'Database'**

Select **'Oracle 10g R2/11g'** from the Database select list.

Click the **'Connection Pools'** tab.



Click the **'Add'** button.



Enter **'Database Connection Pool'** in the **'Name'** field.

Enter **'VALUEOF(DSN)'** in the **'Data source name'** field.

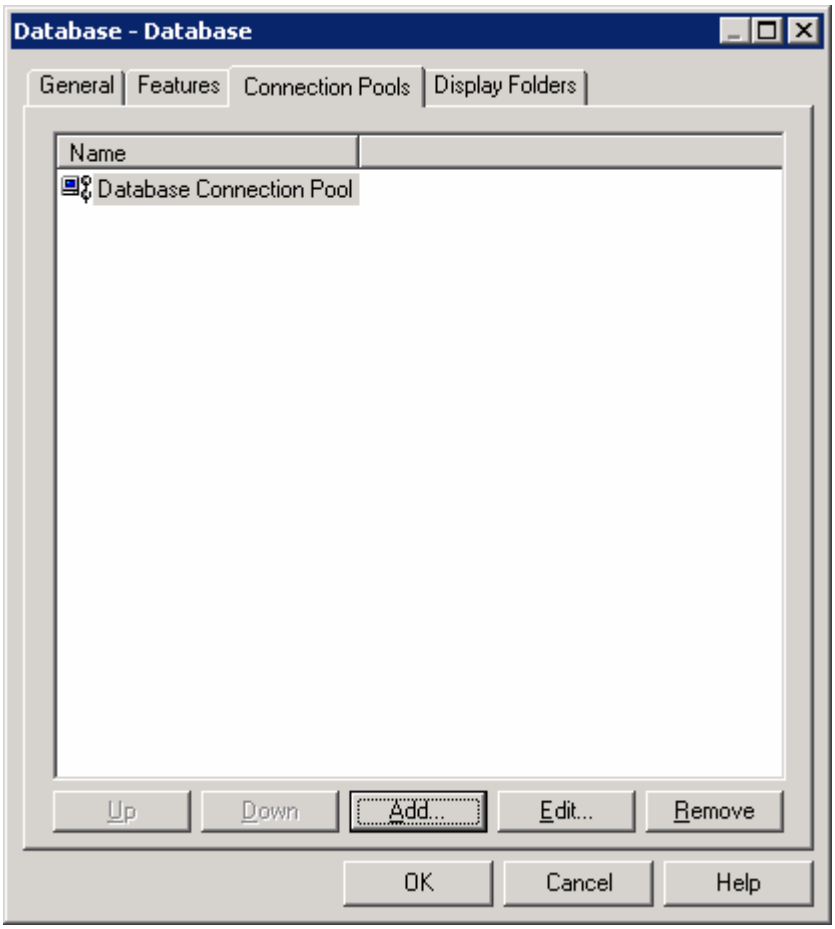
Enter **':USER'** in the **'User name'** field.

Enter **':PASSWORD'** in the **'Password'** field.

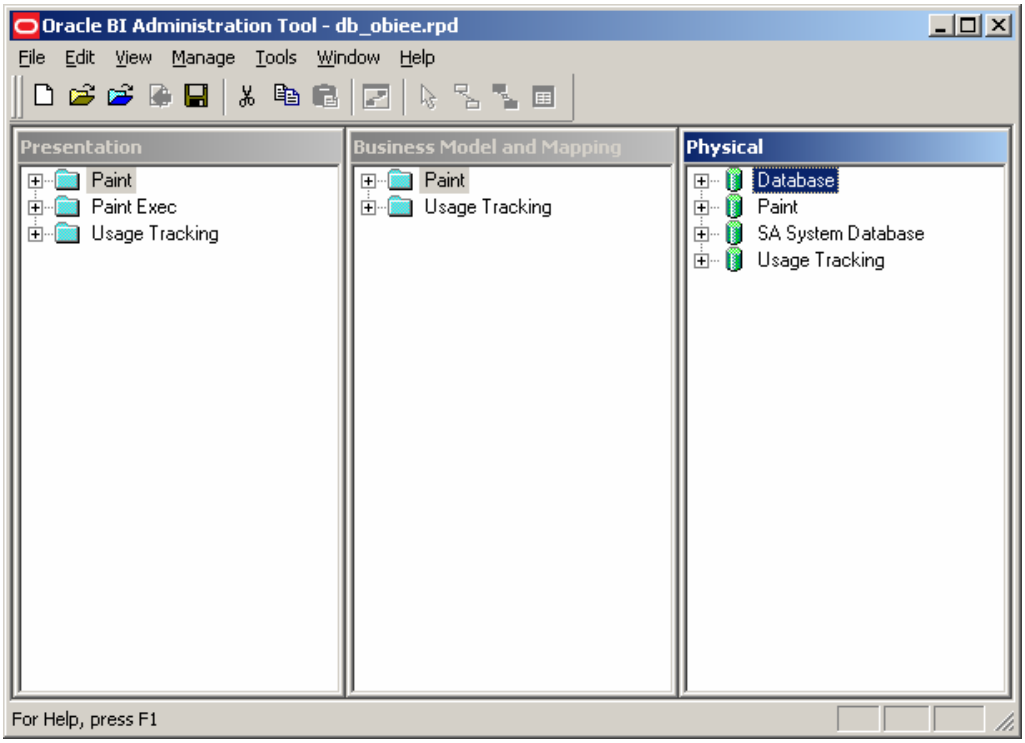
Click OK.

Re-enter **':PASSWORD'** in the **'Password'** field.

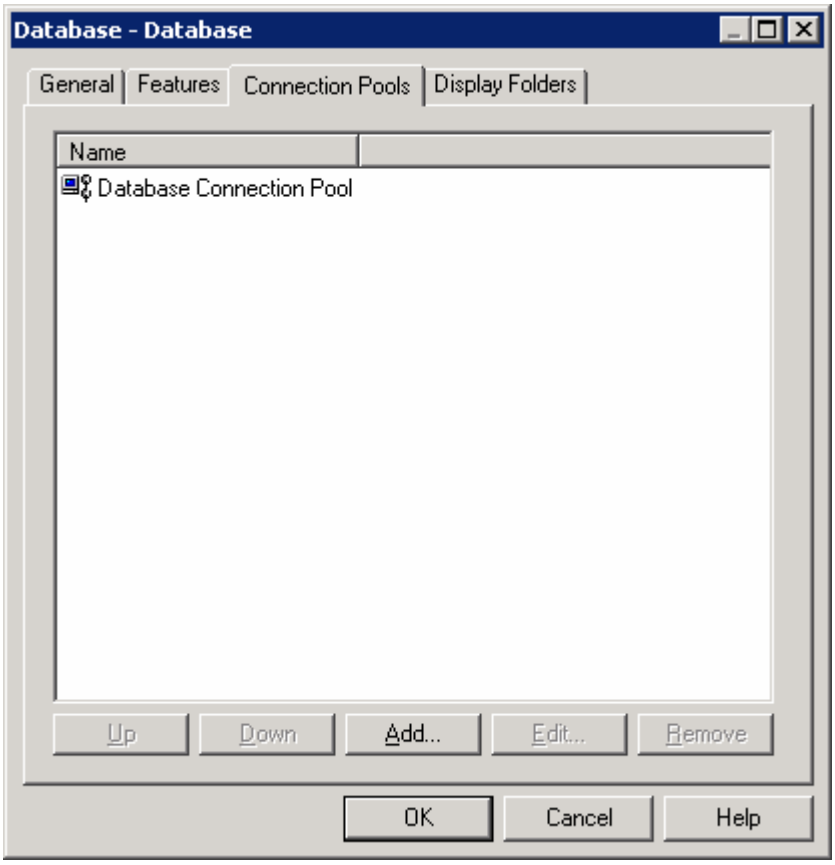
Click OK.


Database - Database
General
Features
Connection Pools
Display Folders
Name
Database Connection Pool
Up
Down
Add...
Edit...
Remove
OK
Cancel
Help

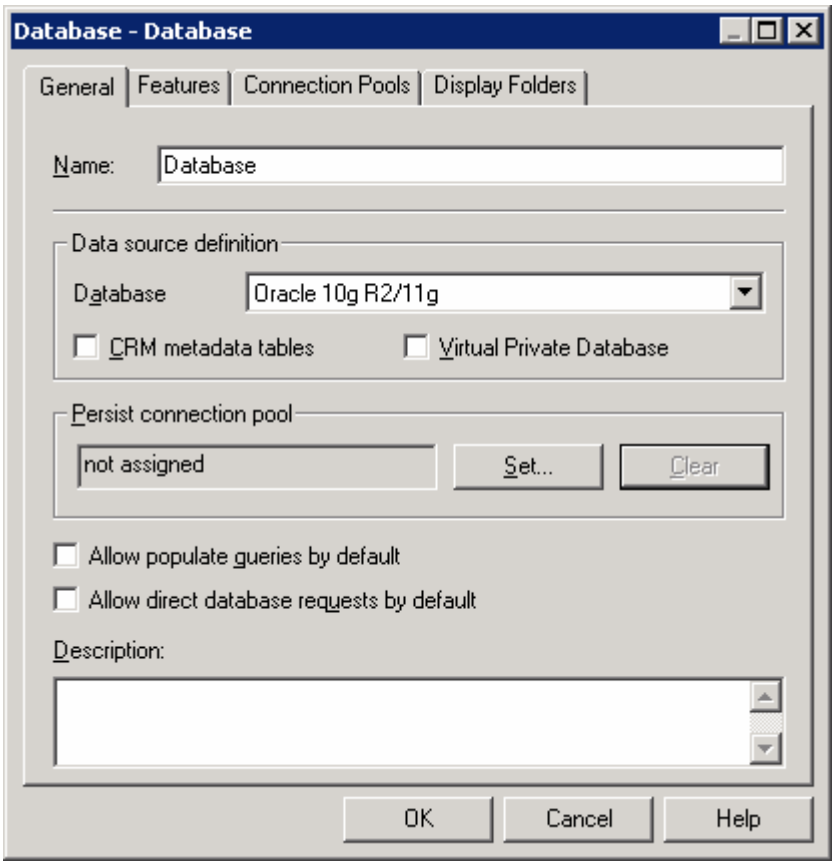
Click OK.


Oracle BI Administration Tool - db_obiee.rpd
File Edit View Manage Tools Window Help
Presentation
Paint
Paint Exec
Usage Tracking
Business Model and Mapping
Paint
Usage Tracking
Physical
Database
Paint
SA System Database
Usage Tracking
For Help, press F1

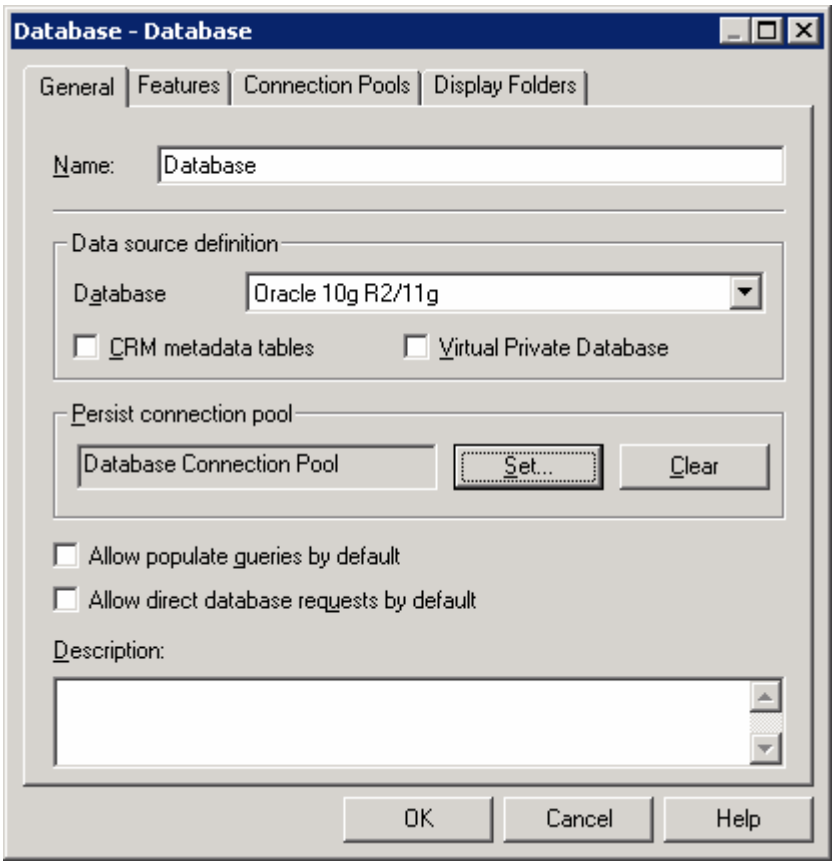
Double-click the **'Database'** entry in the Physical layer.



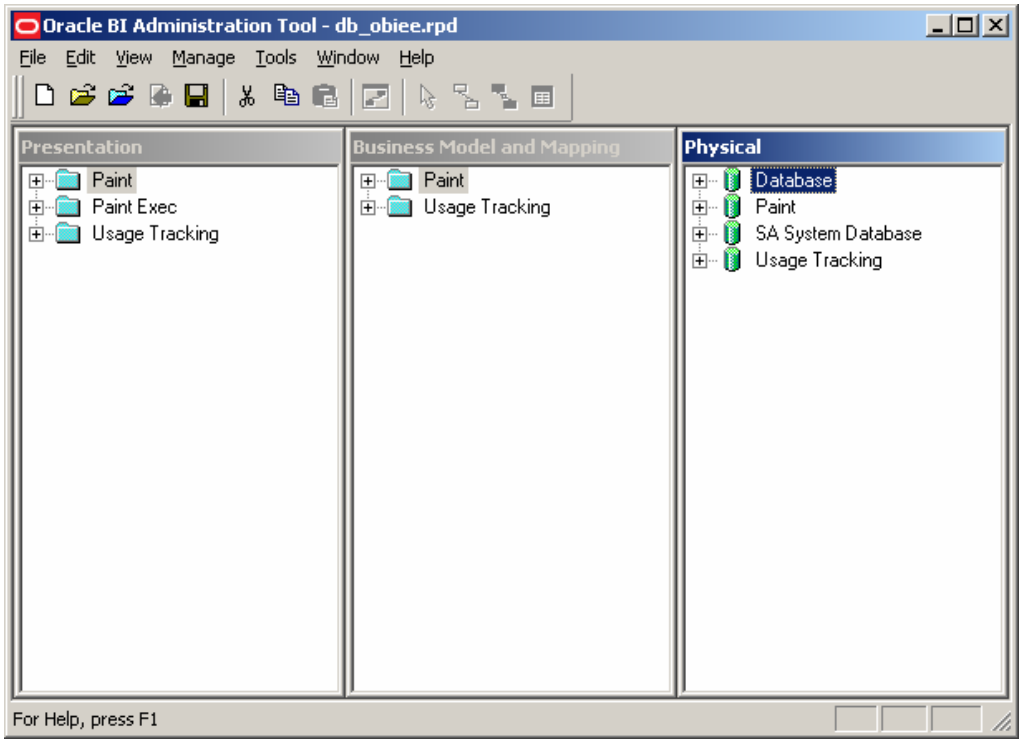
Click the **'General'** tab.



Click the **'Set…'** button.

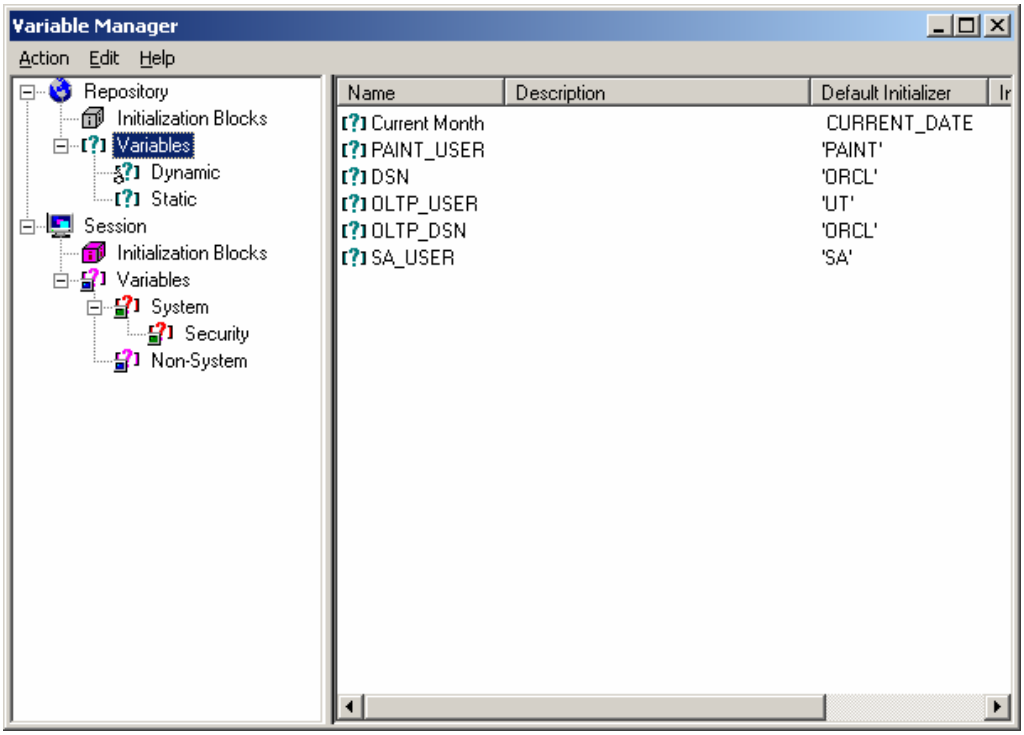


Click OK.

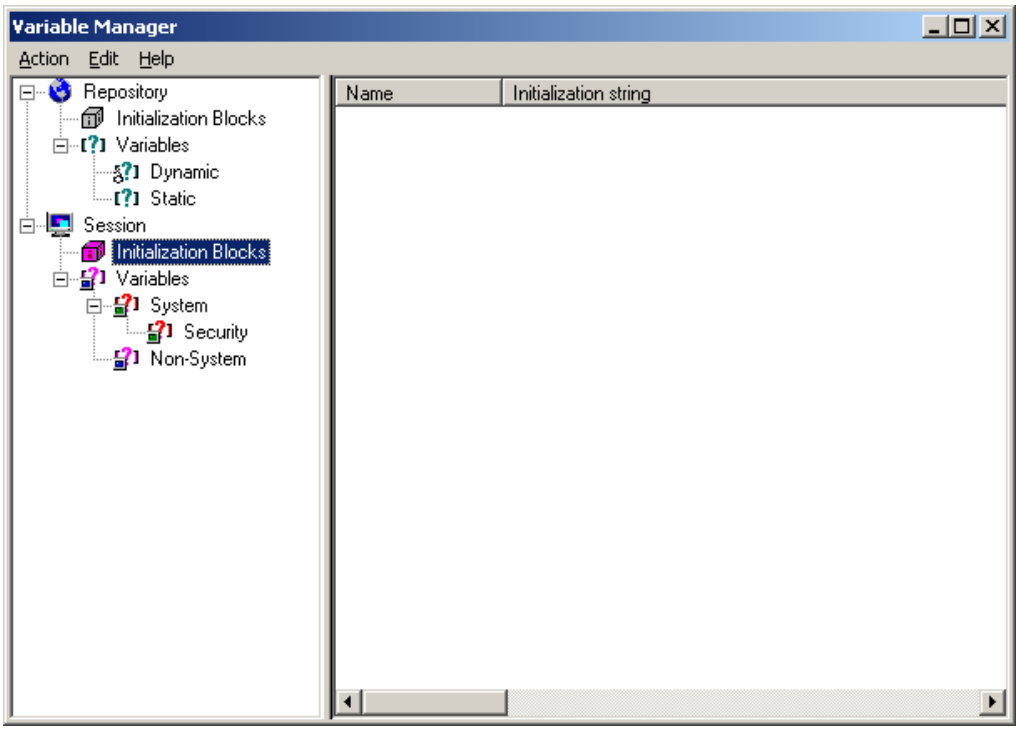


Setup Database Authentication

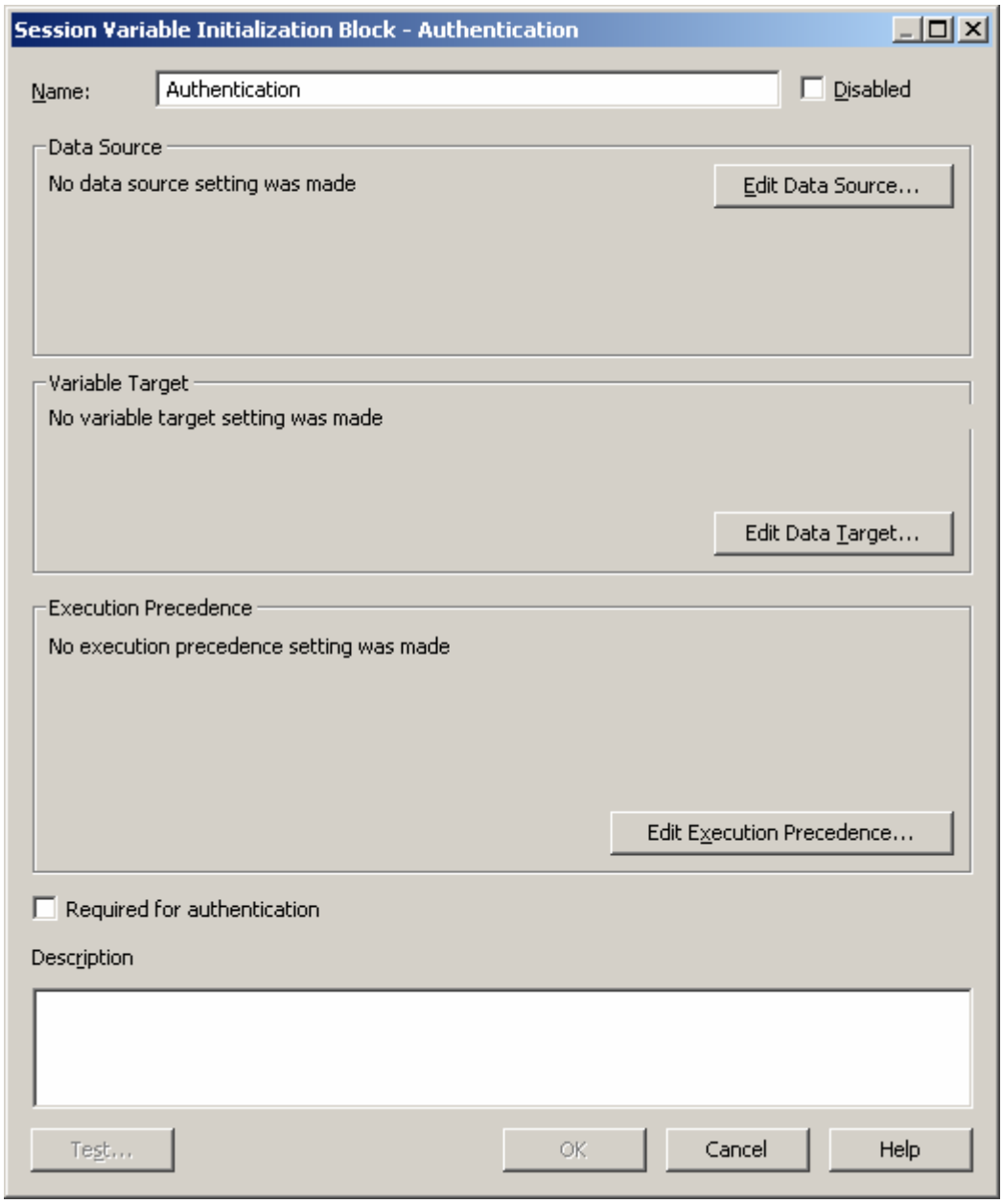
Click Manage > Variables



Click Session > Initialization Blocks

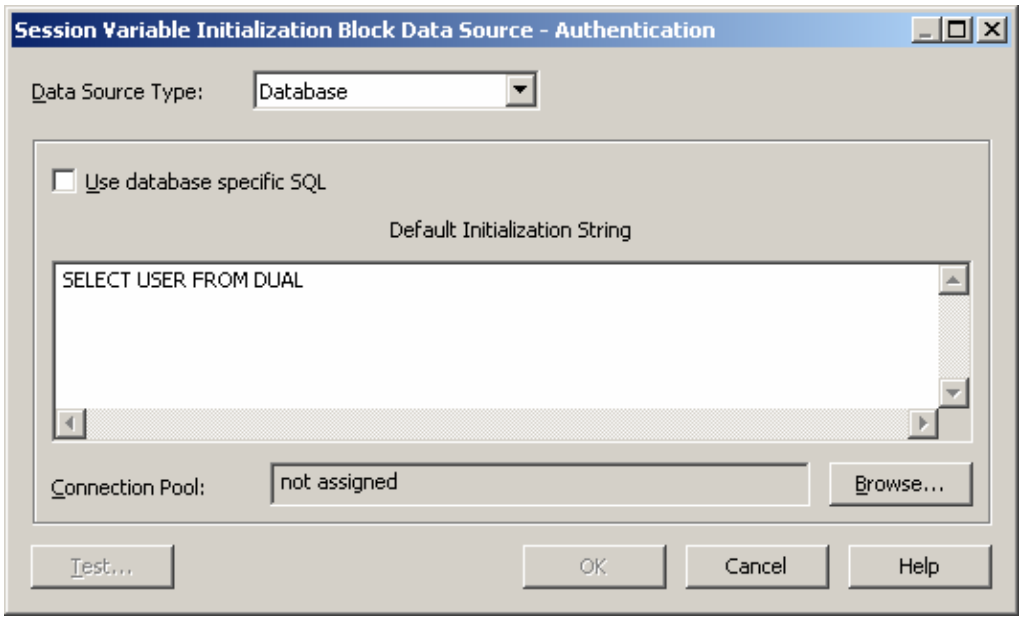


Right-click in the right-hand pane and select **'New Initialization Block…'**



Enter **'Authentication'** in the **'Name'** field.

Click the **'Edit Data Source'** button.

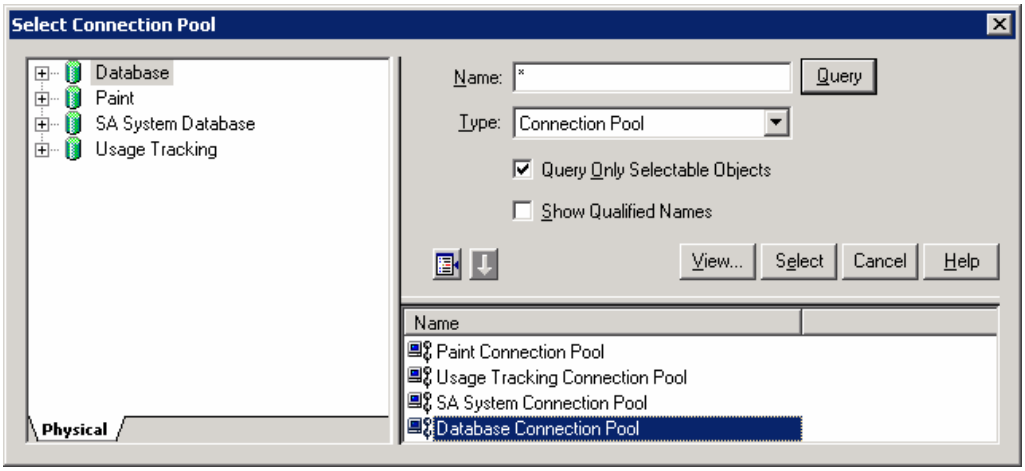


Select **'Database'** from the **'Data Source Type'** select list.

Enter the following SQL into the **'Default Initialization String'** field:

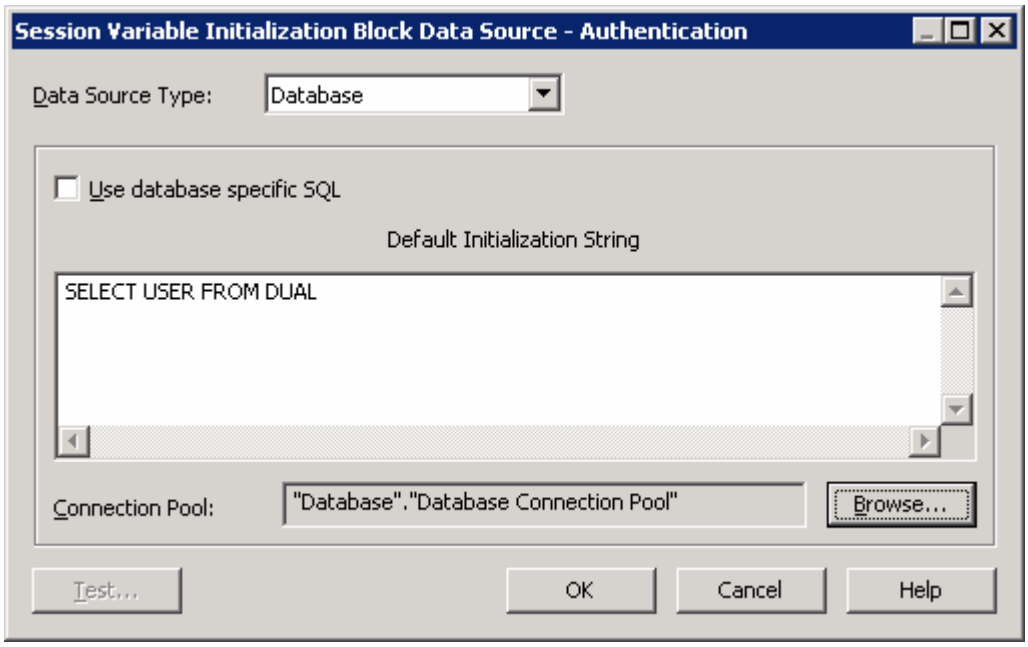
```
SELECT USER FROM DUAL
```

Click the **'Browse…'** button.

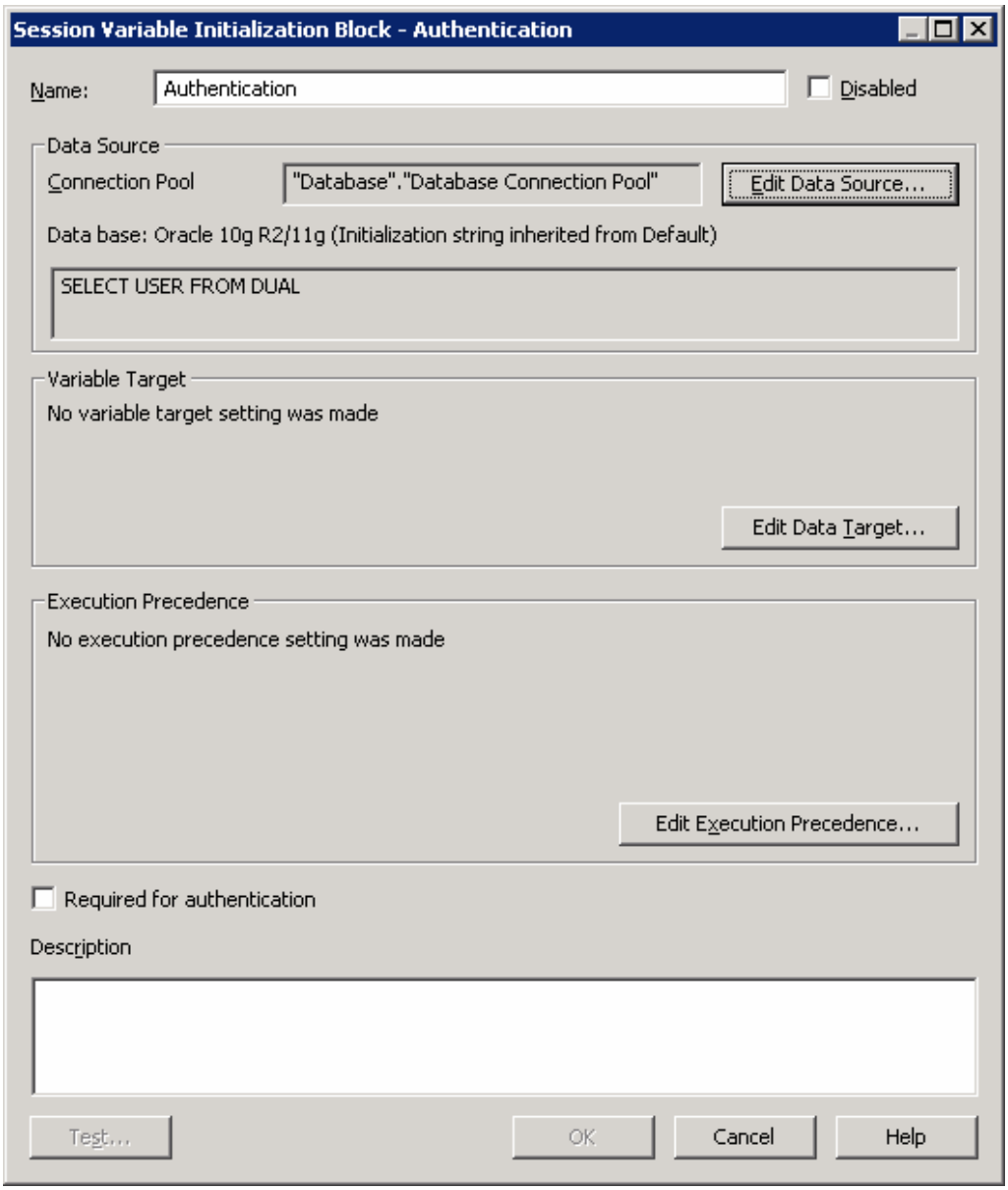


Click the **'Database Connection Pool'** name.

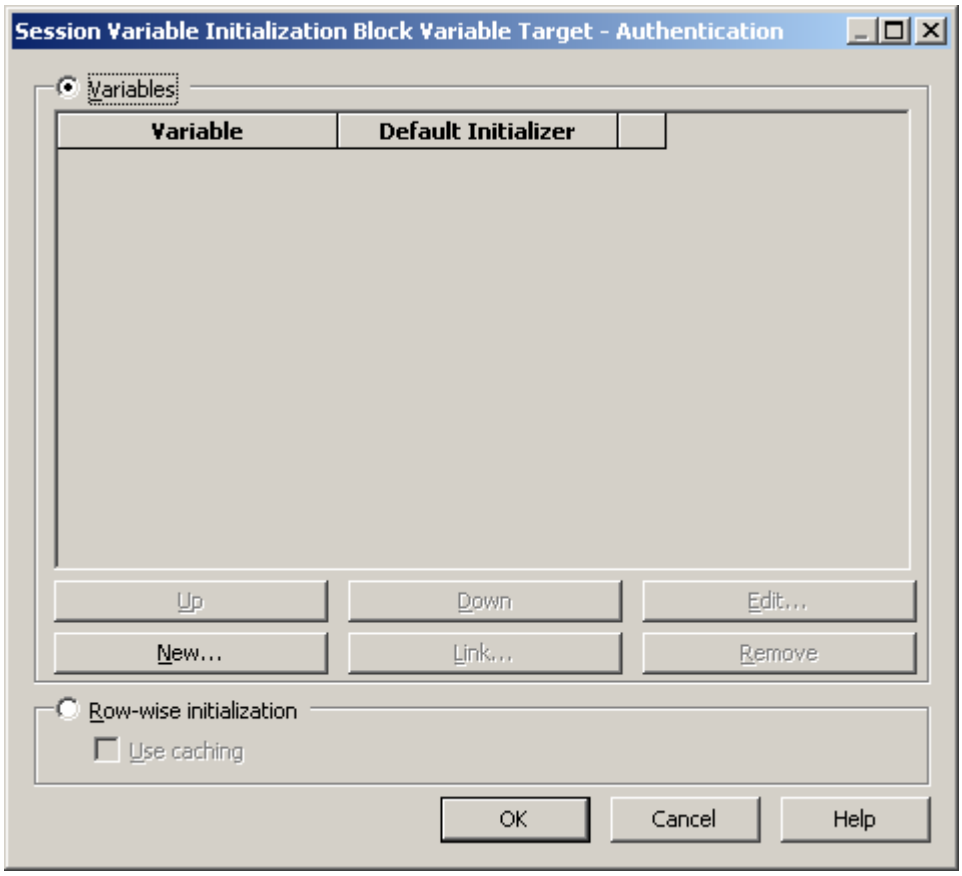
Click the **'Select'** button.



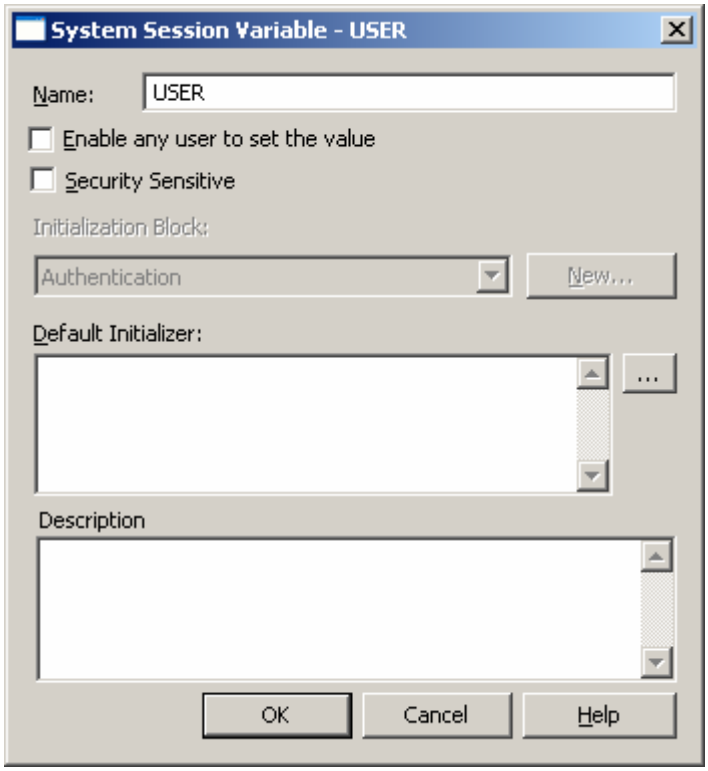
Click OK.



Click the **'Edit Data Target'** button.

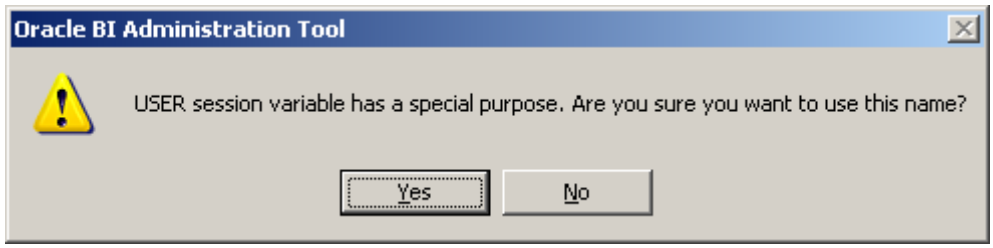


Click the **'New…'** button.

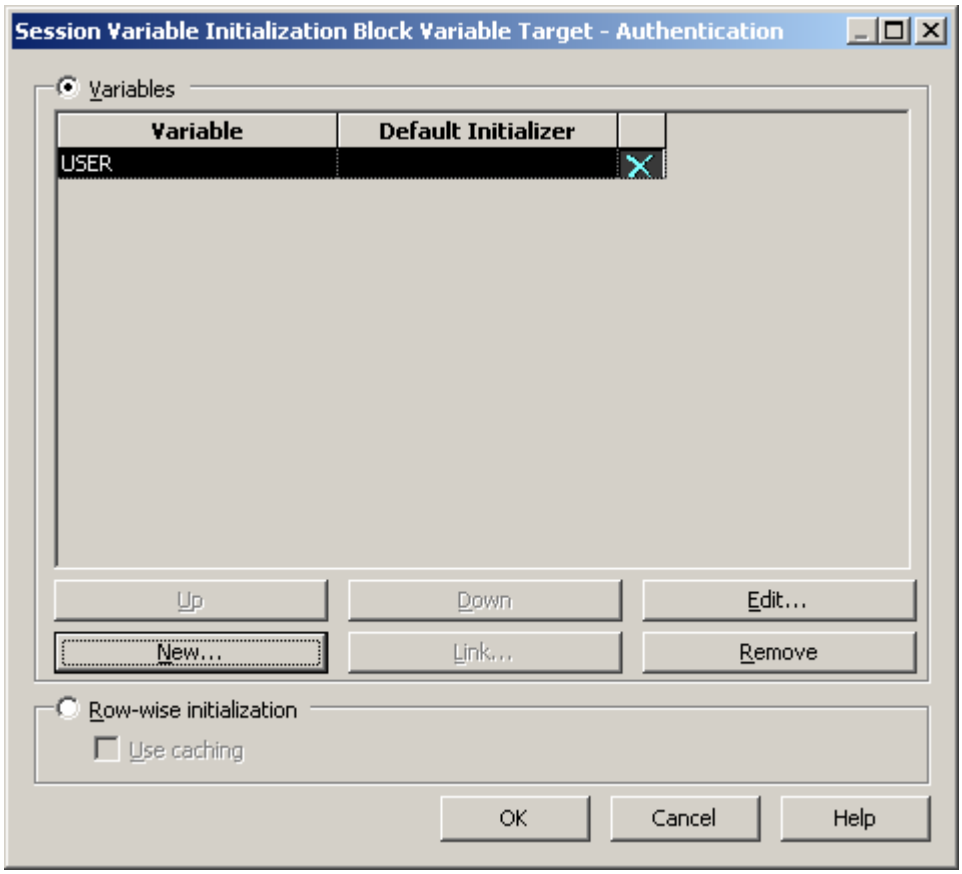


Enter **'USER'** in the **'Name'** field.

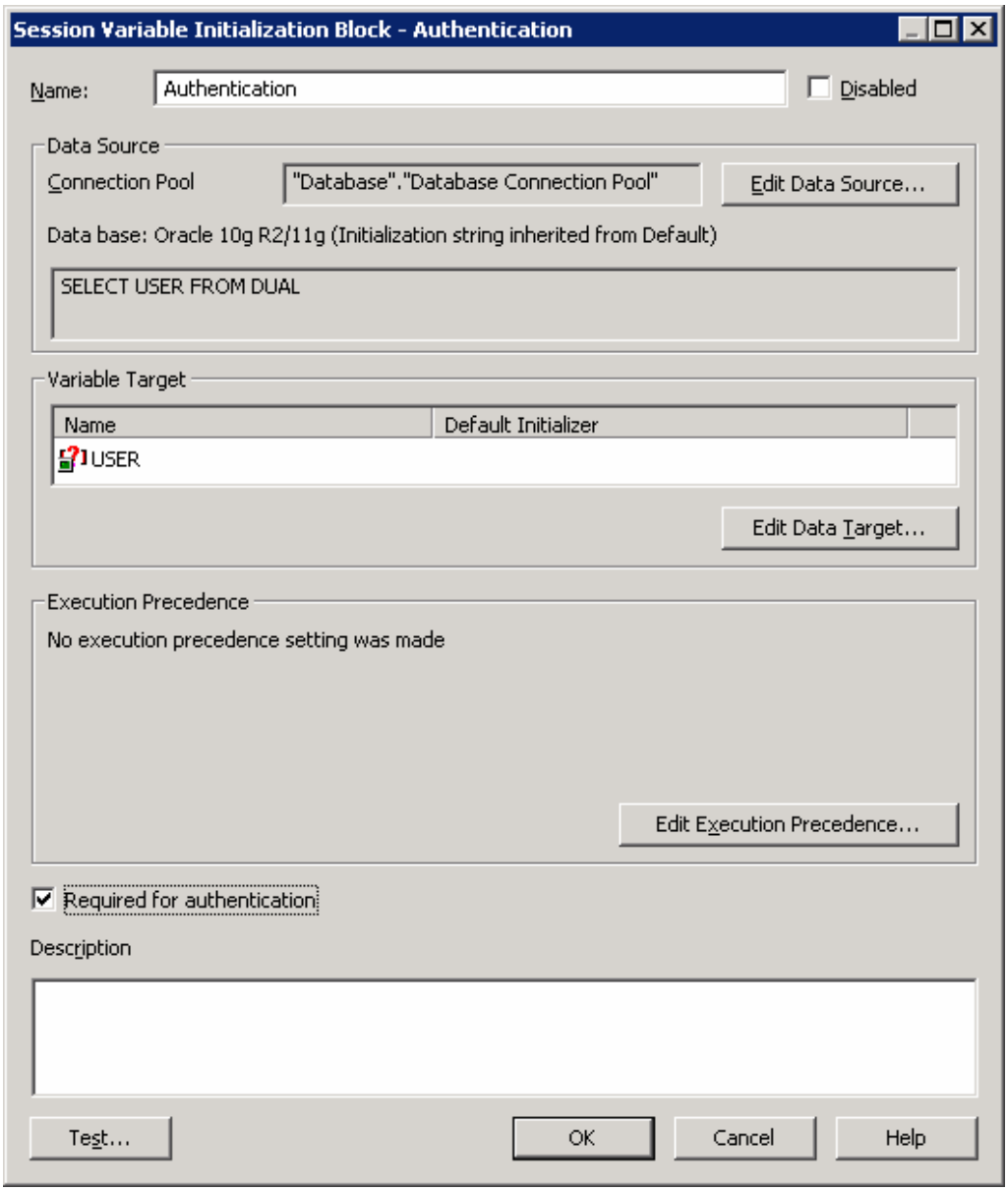
Click OK.



Click Yes.

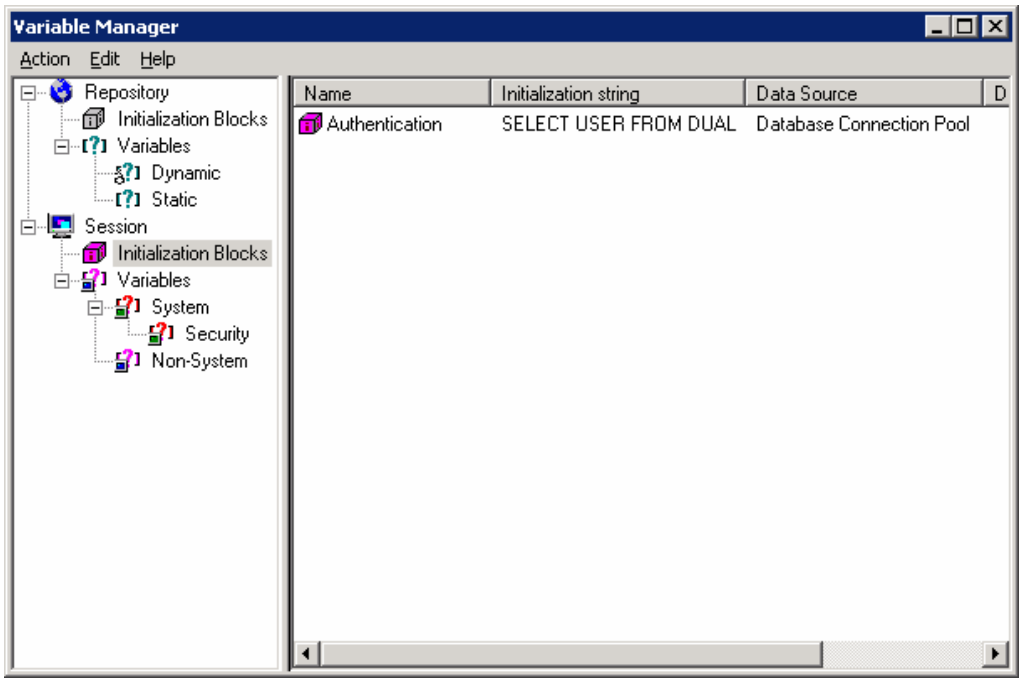


Click OK.



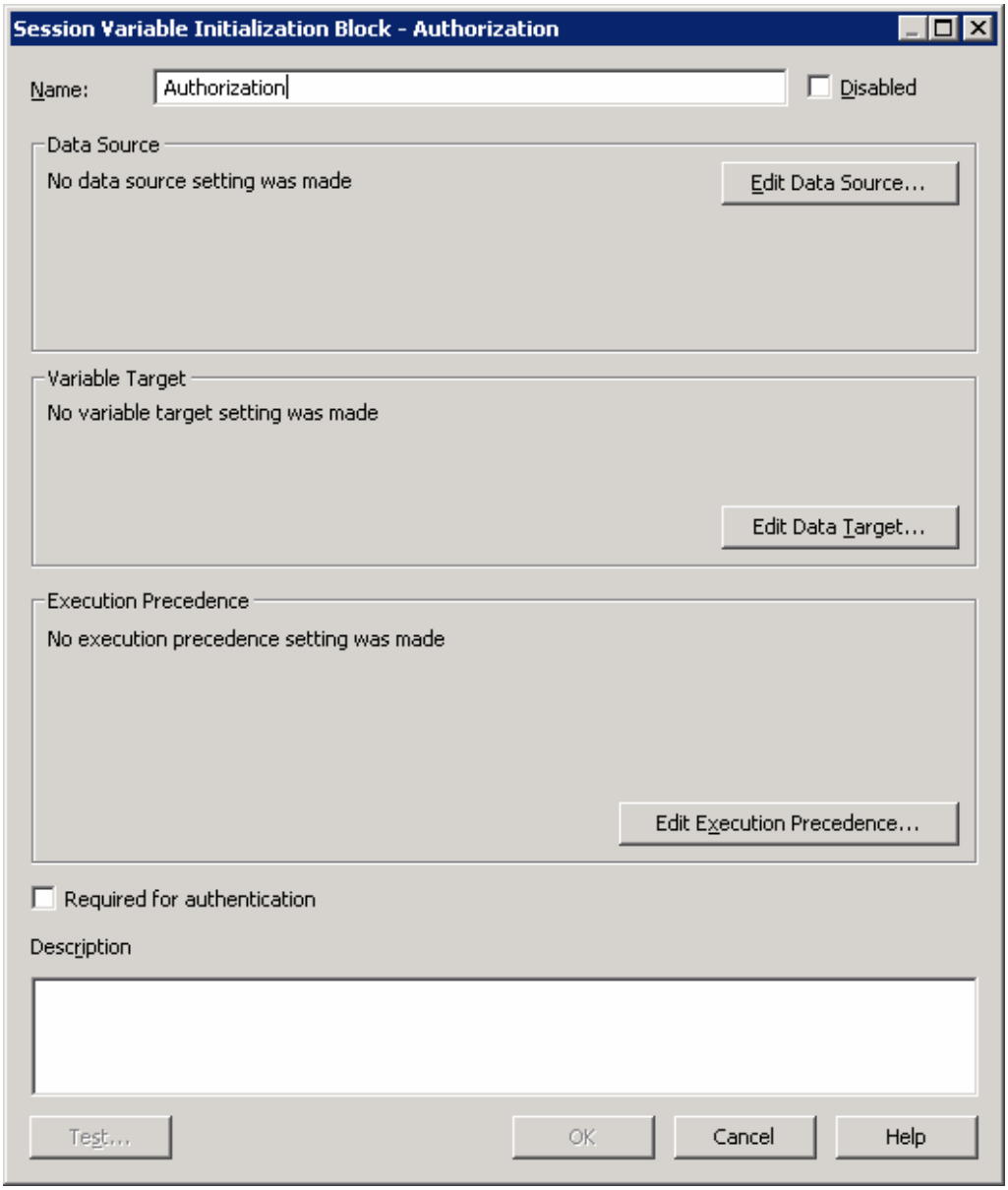
Tick the **'Required for authentication'** check box.

Click OK.


Variable Manager
Action
Edit
Help
Repository
Initialization Blocks
Variables
Dynamic
Static
Session
Initialization Blocks
Variables
System
Security
Non-System
Name
Initialization string
Data Source
Authentication
SELECT USER FROM DUAL
Database Connection Pool

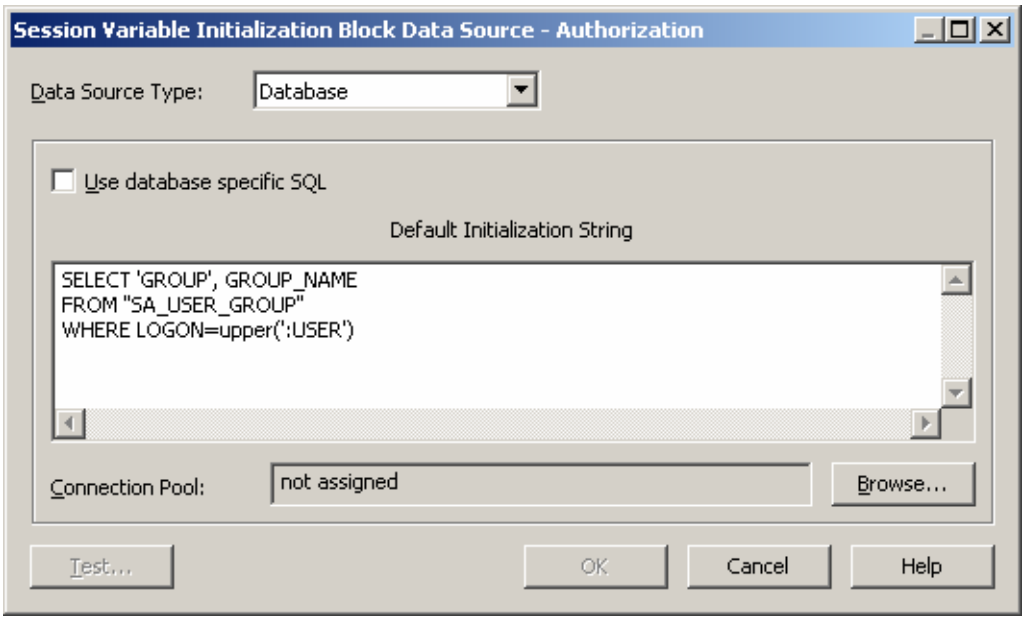
Setup Authorization

Right-click in the right-hand pane and select **'New Initialization Block…'**



Enter **'Authorization'** in the 'Name' field.

Click the **'Edit Data Source'** button in the **'Data Source'** region.

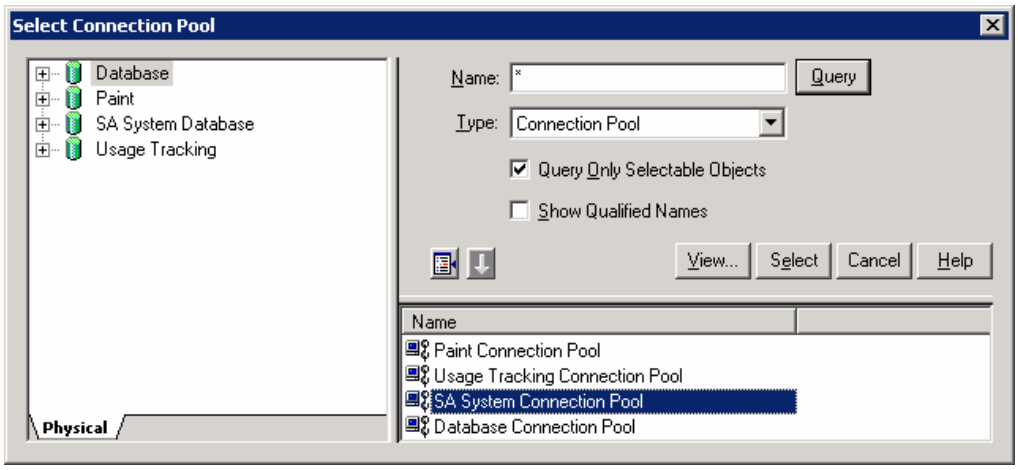


Select **'Database'** from the **'Data Source Type'** select list.

Enter the following SQL into the **'Default Initialization String'** field:

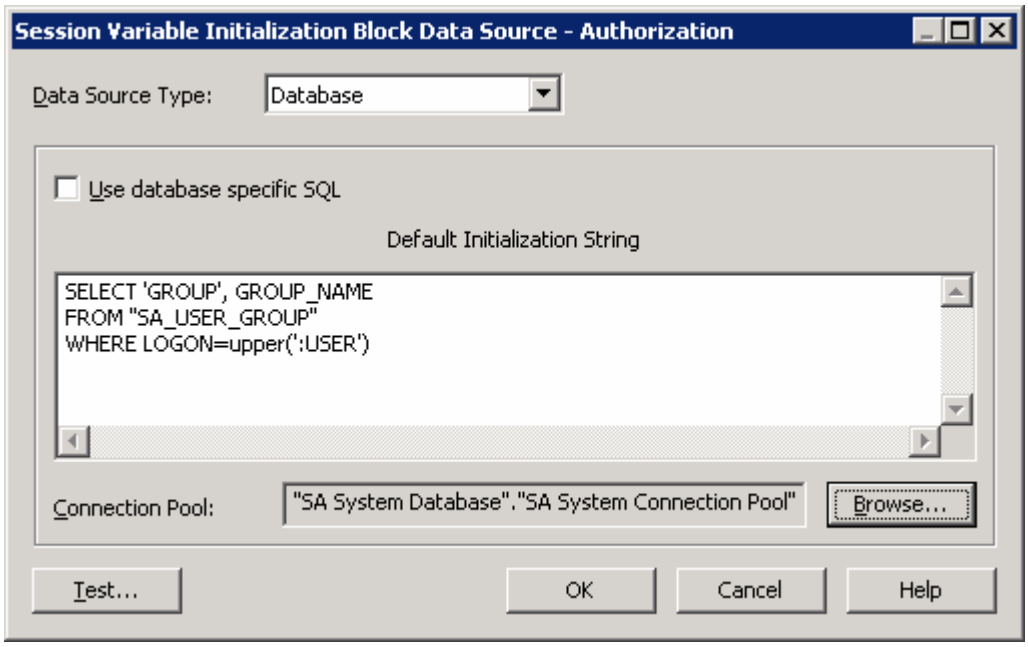
```
SELECT 'GROUP', GROUP_NAME
FROM "SA_USER_GROUP"
WHERE LOGON=upper(':USER')
```

Click the **'Browse…'** button.

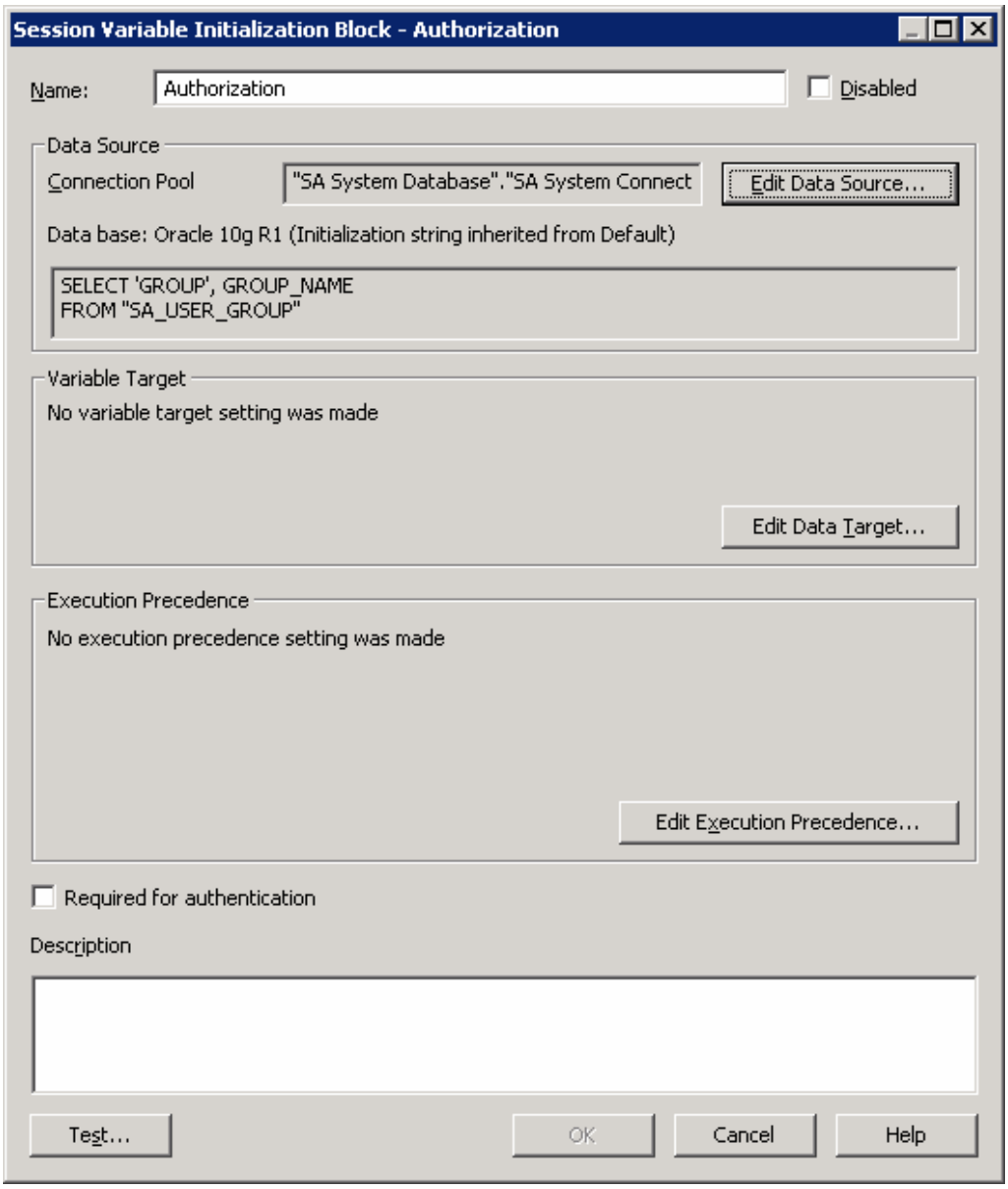


Click the **'SA System Connection Pool'** name.

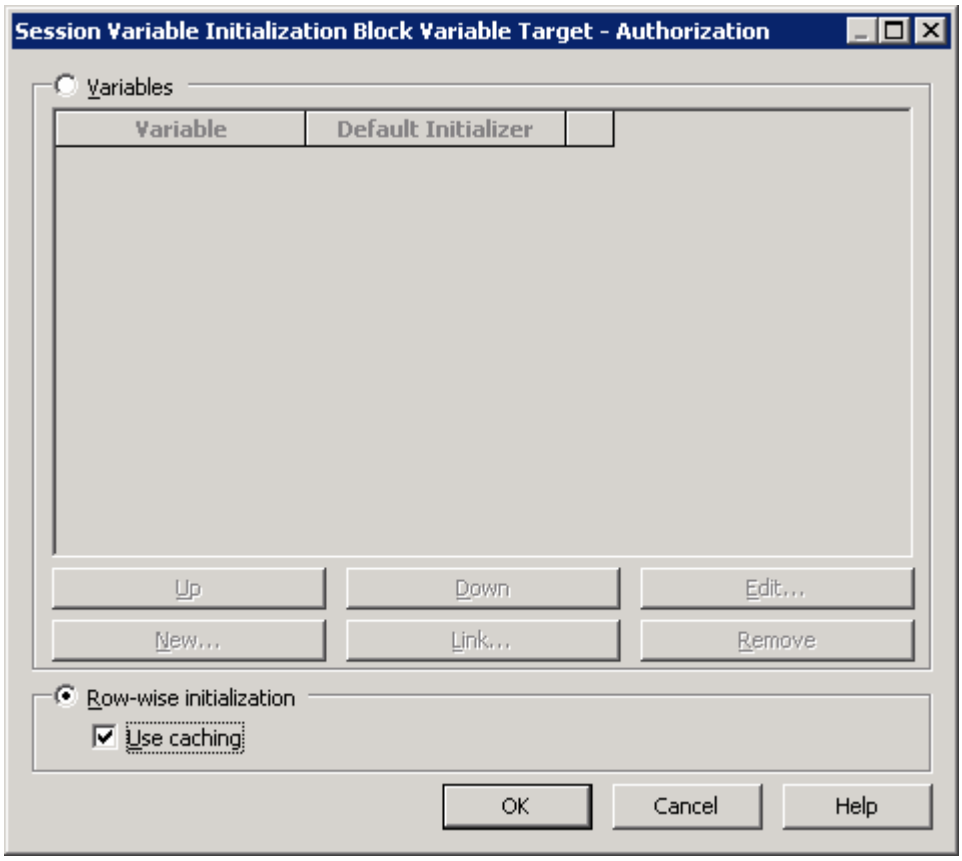
Click Select.



Click OK.

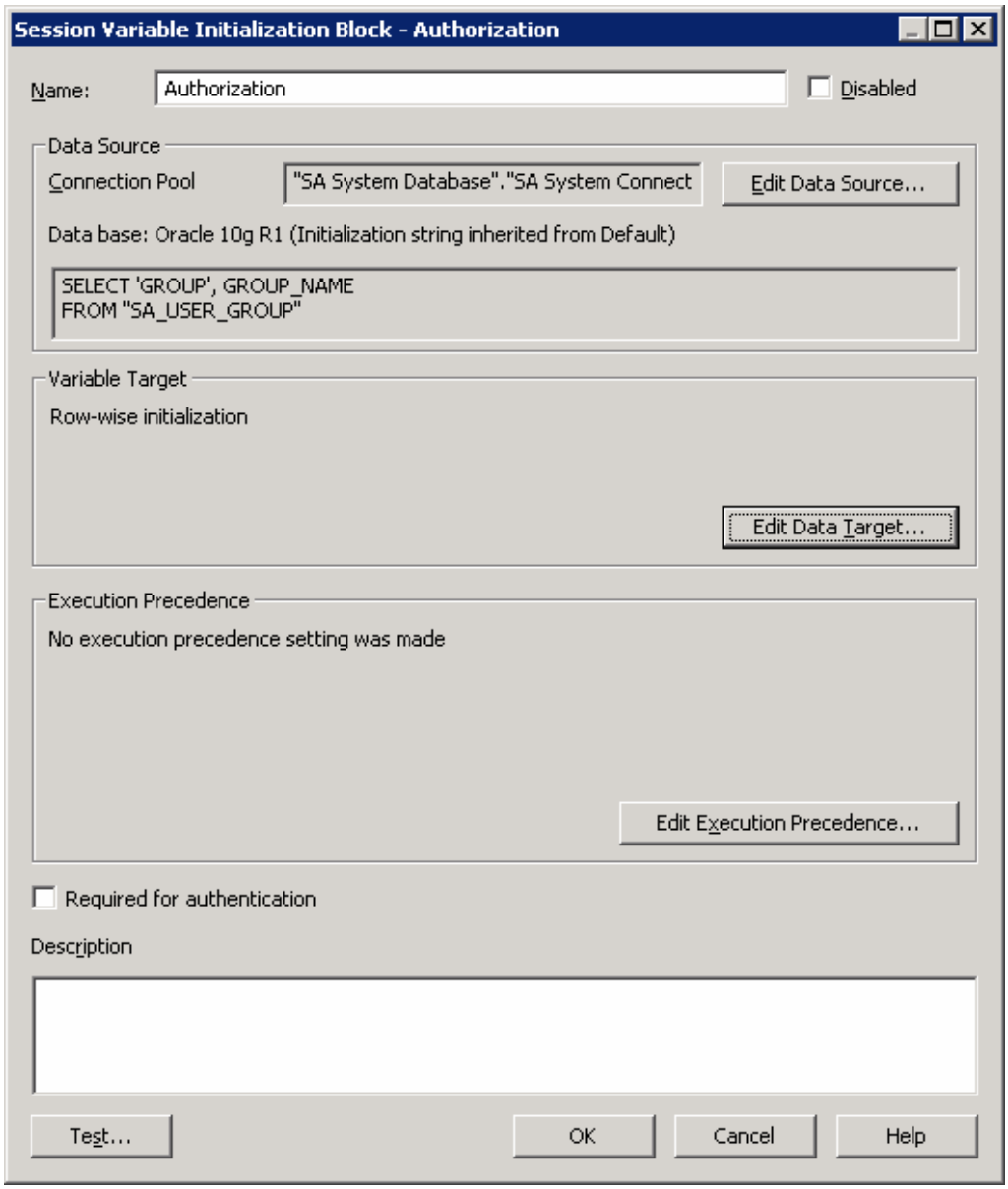


Click the **'Edit Data Target'** button in the **'Variable Target'** region.

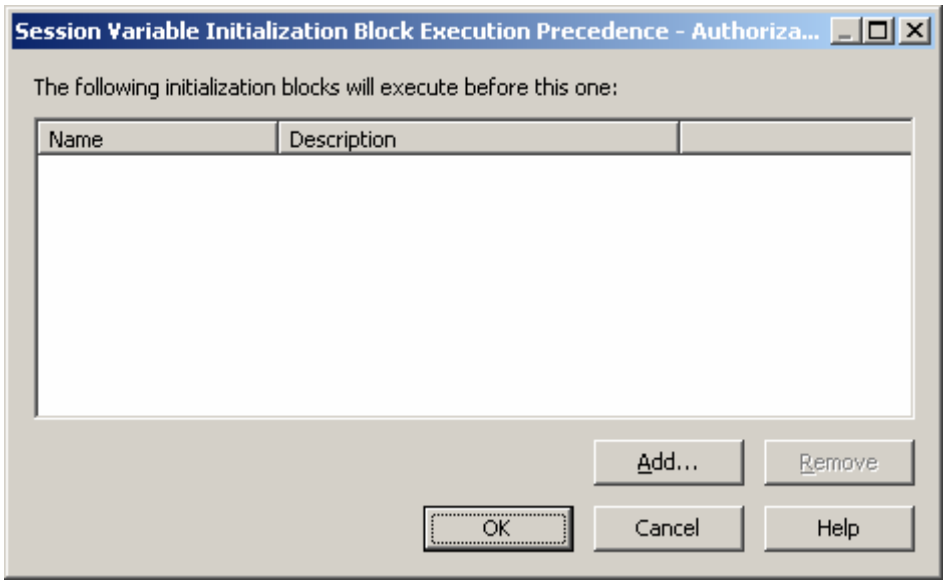


Select the **'Row-wise Initialization'** radio button and tick the **'Use caching'** check box.

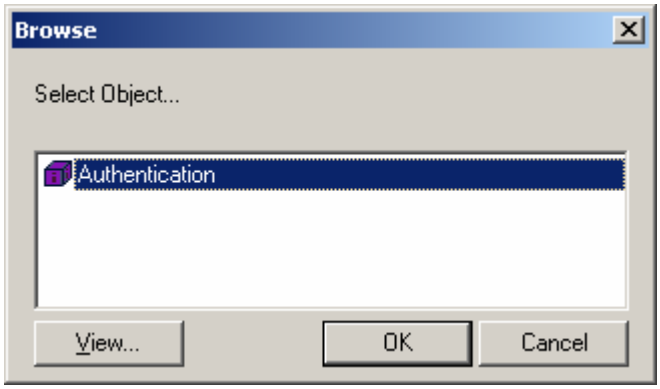
Click OK.



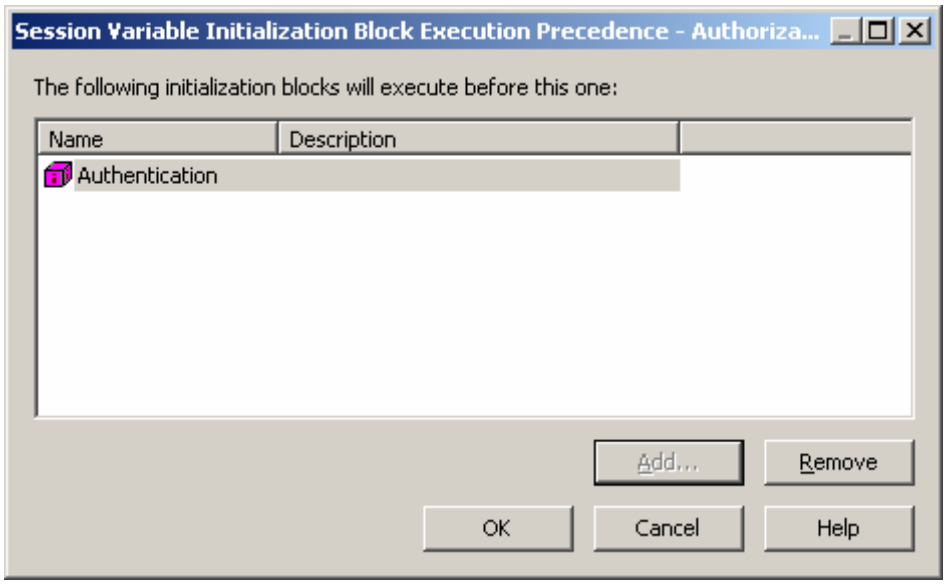
Click the **'Edit Execution Precedence...'** button in the **'Execution Precedence'** region.



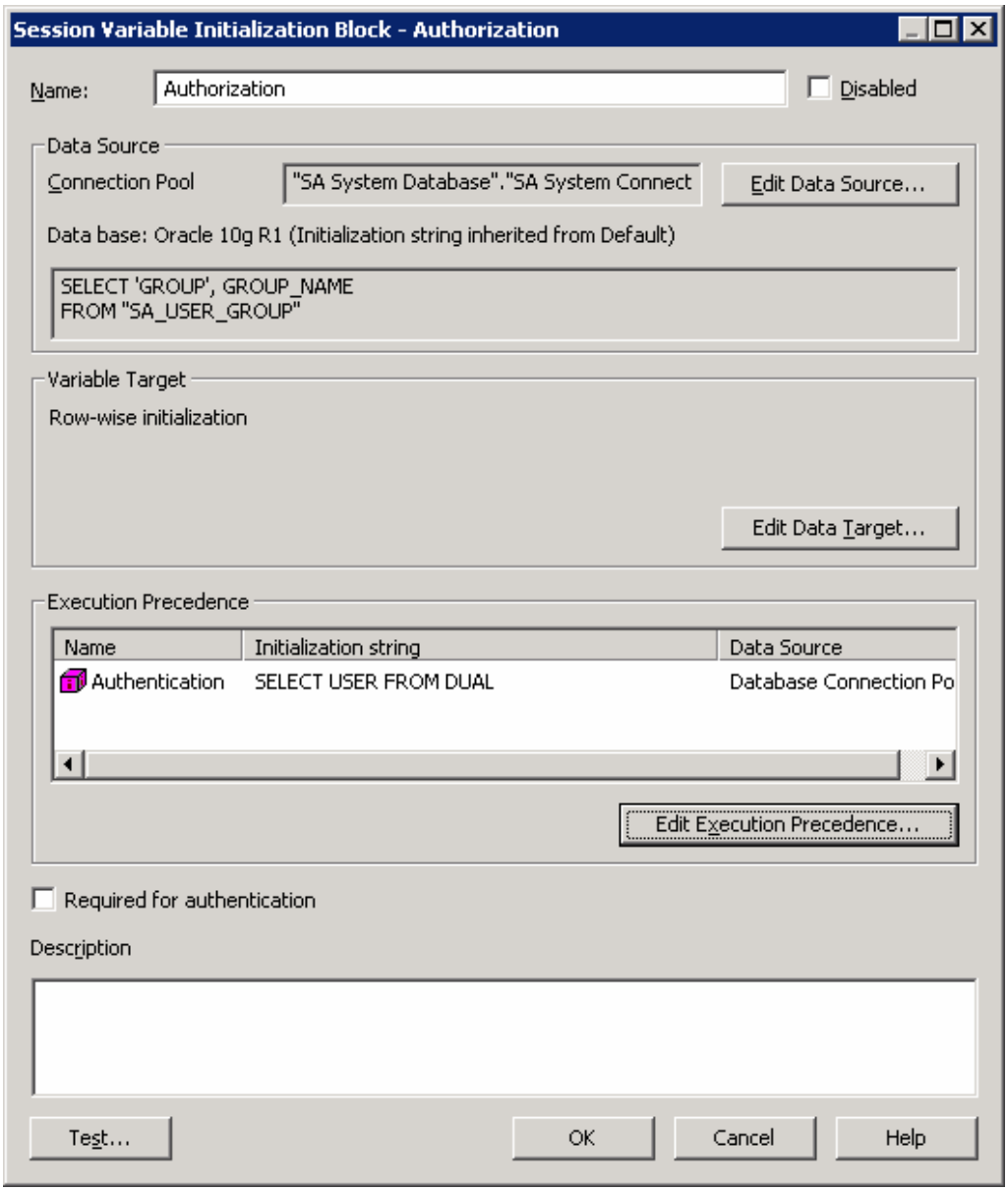
Select the **'Add…'** button.



Select **'Authentication'** and click OK.

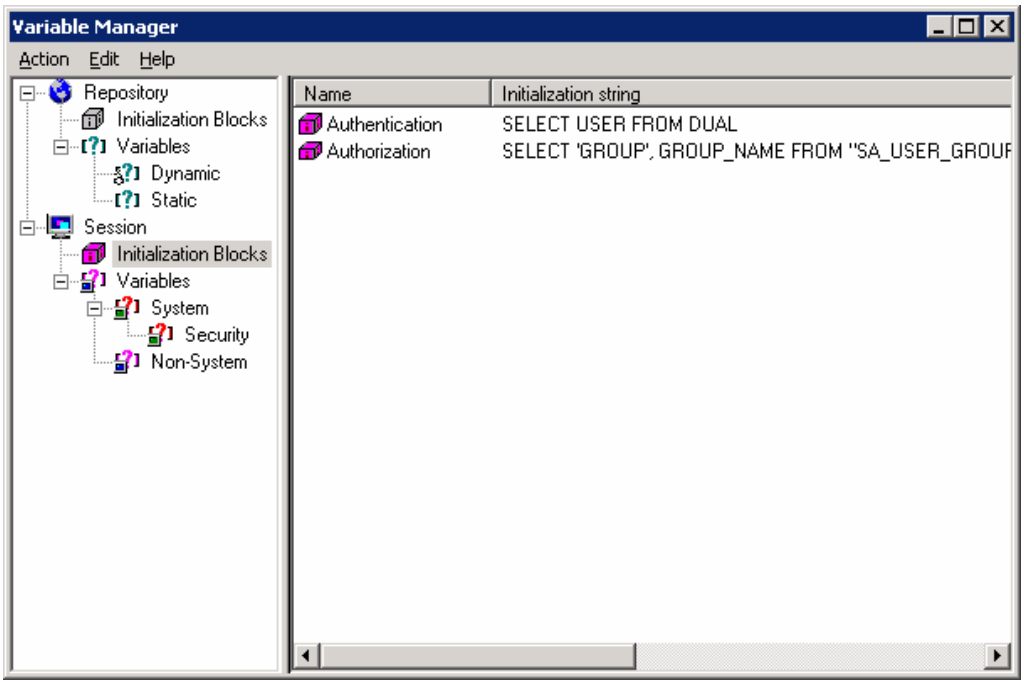

Session Variable Initialization Block Execution Precedence - Authoriza...
The following initialization blocks will execute before this one:
Name
Description
Authentication
Add...
Remove
OK
Cancel
Help

Click OK.



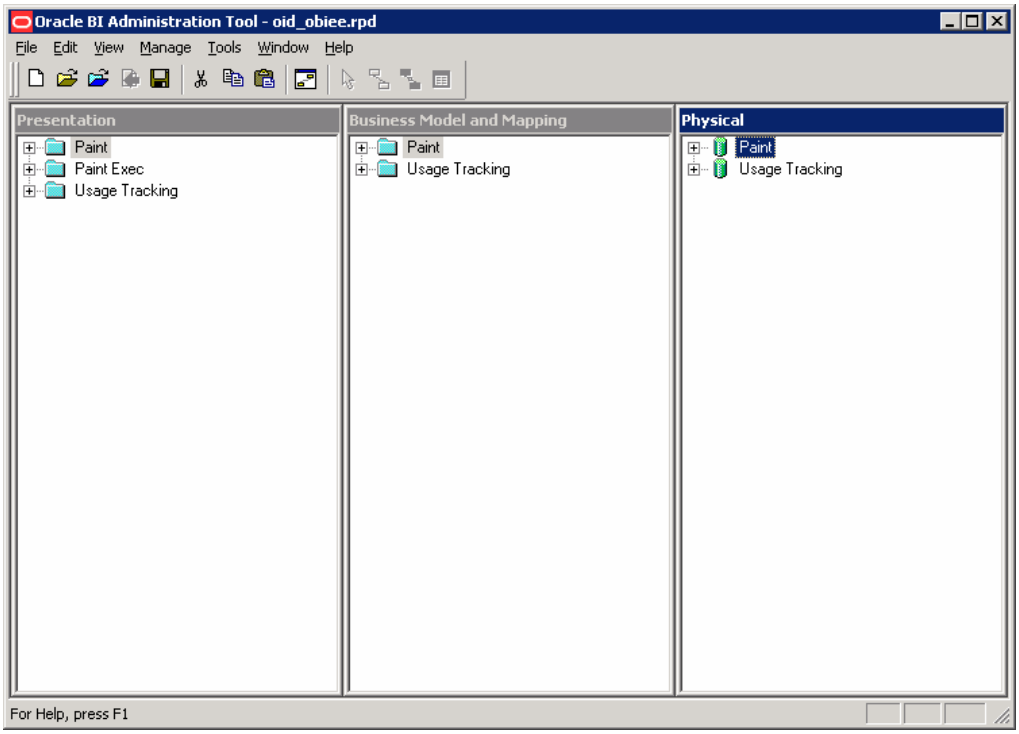
Do **NOT** check the **'Required for authentication'** check box.

Click OK.

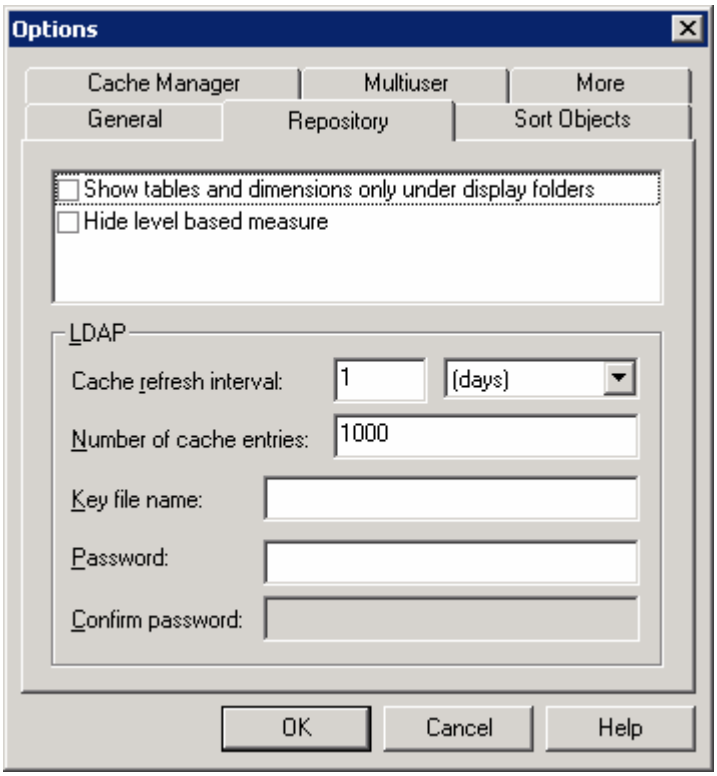


Close the Variable Manager and save the repository.

4.1.8 Disable LDAP Caching



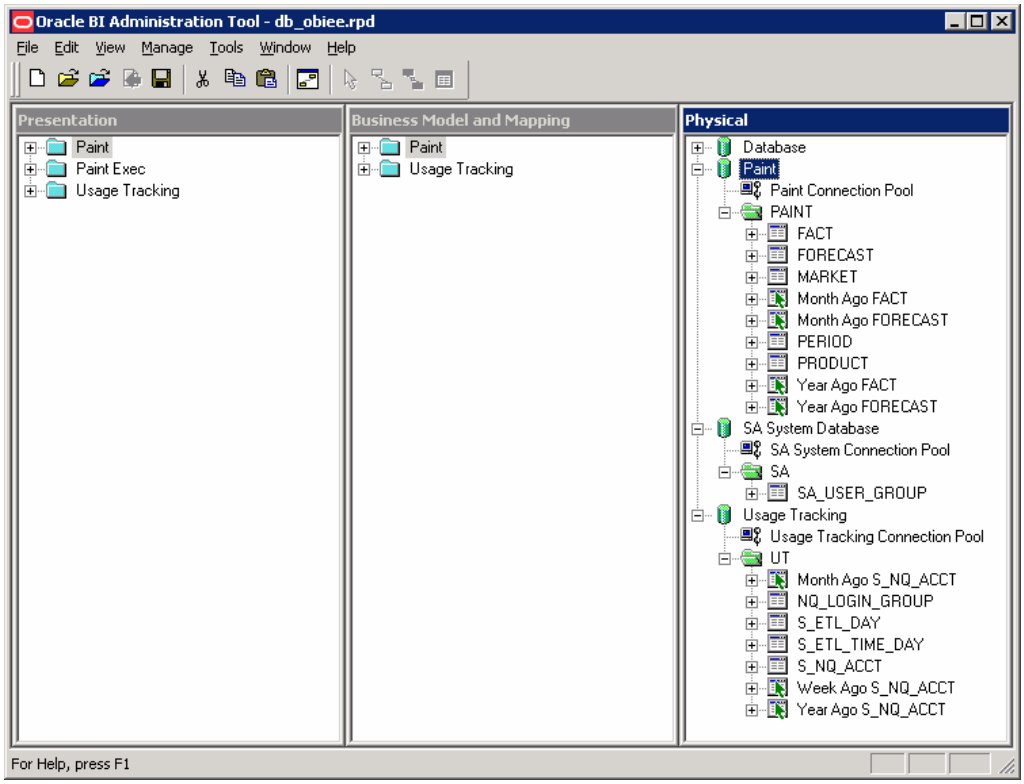
Click Tools > Options and click on the **'Repository'** tab.



Change the value in the **'Number of cache entries'** field to **'0'**.

Click OK.

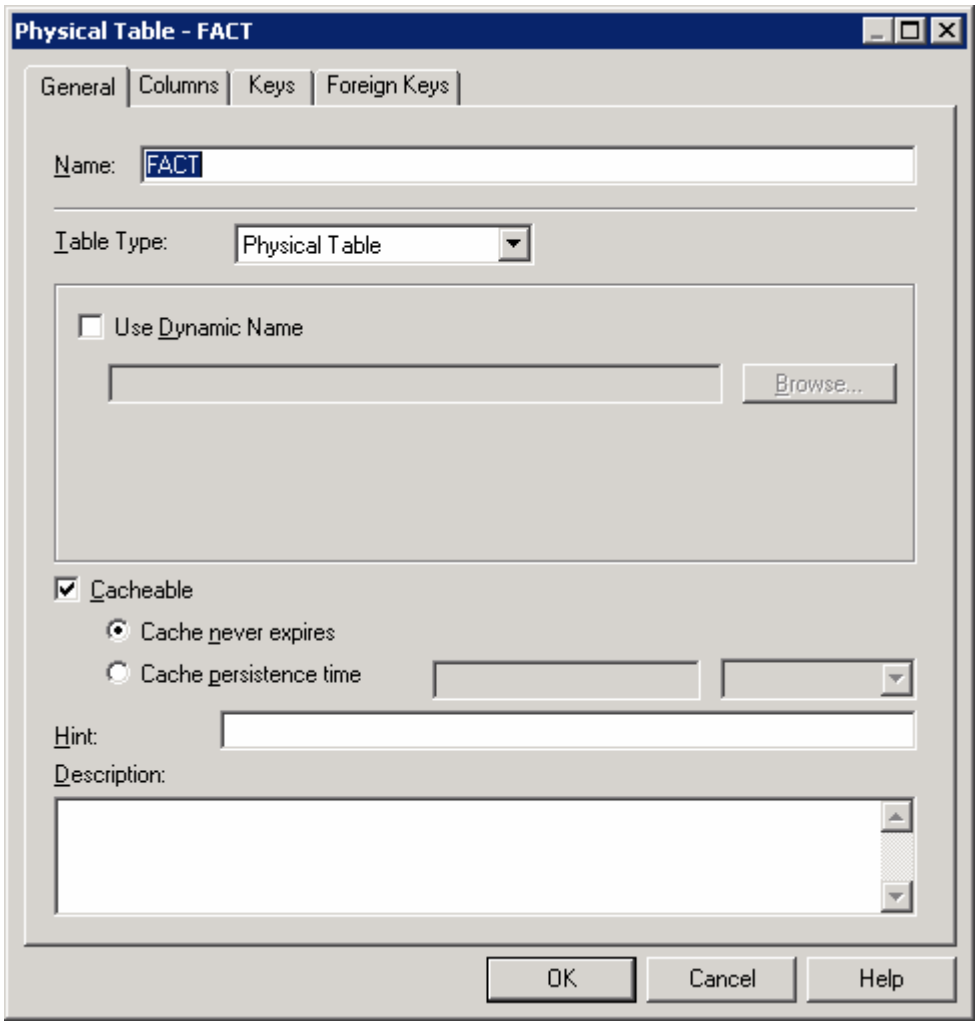
4.1.9 Disable Table Caching



In the Physical layer pane expand the **'Paint'**, **'SA System Database'** and **'Usage Tracking'** databases so that they appear as shown above.

NOTE: 'SA System Database' will only appear in the `db_obiee.rpd` file.

Right-click the **'FACT'** table and click **'Properties'**.



Uncheck the 'Cacheable' tick box.

Click OK.

Repeat the process for the following tables:

- FORECAST
- MARKET
- PERIOD
- PRODUCT
- SA_USER_GROUP
- NQ_LOGIN_GROUP
- S_ETL_DAY
- S_ETL_TIME_DAY
- S_NQ_ACCT

Save the repository and close it.

4.1.10 Repository Specification

The `db_obiee.rpd` and `oid_obiee.rpd` repository files should be copied from the `C:\oracle\product\OBIEE\server\Repository` directory on the Windows XP machine (machine 6) to the `/space/oracle/product/OBIEE/server/Repository` directory on machines 1 and 2.

The repository to be used is specified in the `NQSConfig.INI` file located in the `/space/oracle/product/OBIEE/server/Config` directory

Open the `NQSConfig.INI` file where the BI Server has been deployed (machines 1 and 2) and add the following entries to the `[ REPOSITORY ]` section:

```
#Star  =    oid_obiee.rpd, DEFAULT;
#Star  =    db_obiee.rpd, DEFAULT;
```

If OID authentication and authorization is to be used uncomment the first line.

If DB authentication and authorization is to be used uncomment the second line.

4.2 Usage Tracking Configuration

Usage Tracking is enabled by modifying parameters in the `NQSConfig.INI` file located in the following directory:

```
/space/oracle/product/OBIEE/server/Config
```

Open the `NQSConfig.INI` file and make the following changes on all machines in the cluster (machines 1 and 2):

In the `[ USAGE_TRACKING ]` section:

```
ENABLE = YES;
DIRECT_INSERT = YES;
PHYSICAL_TABLE_NAME = "Usage Tracking"."UT"."S_NQ_ACCT";
CONNECTION_POOL  =  "Usage  Tracking"."Usage  Tracking  Connection
Pool";
```

4.3 Cluster Configuration

This section describes the actions required to setup Oracle Business Intelligence Enterprise Edition in a cluster configuration.

4.3.1 Network Share Configuration

In the evaluated configuration of the TOE, BI components deployed in a clustered environment must have access to shared resources for the Presentation Catalog and Repository. NFS will be used to provide this functionality. On the NFS server (machine 7), as the `oracle` user, create directories for the repository and presentation catalog:

```
cd /space/oracle/oradata/OBIEE
mkdir –p share/catalog
mkdir –p share/repository
mkdir –p share/logs
```

As the `root` user, add the following entries to the `/etc/exports` file:

```
/space/oracle/oradata/OBIEE/share/repository
vm1(rw,no_root_squash) vm2(ro,no_root_squash)
/space/oracle/oradata/OBIEE/share/catalog
vm1(rw,no_root_squash) vm2(rw,no_root_squash)
/space/oracle/oradata/OBIEE/share/logs
vm1(rw,no_root_squash) vm2(rw,no_root_squash)
```

As the `root` user, add the following entries to the `/etc/sysconfig/nfs` file:

```
MOUNTD_PORT=2050
RQUOTAD_PORT=2051
LOCKD_UDPPORT=2052
LOCKD_TCPPORT=2052
```

Start the `portmap` and `nfs` services and enable them to start after a reboot:

```
/etc/init.d/portmap start
/etc/init.d/nfs start
/sbin/chkconfig --level 3 portmap on
/sbin/chkconfig --level 3 nfs on
```

As the `root` user, add the following lines to the `/etc/fstab` file on machines 1 and 2:

```
vm7:/space/oracle/oradata/OBIEE/share/catalog
/space/oracle/oradata/OBIEE/share/catalog nfs
proto=udp,hard,intr,nfsvers=3,actimeo=1 0 0
vm7:/space/oracle/oradata/OBIEE/share/repository
/space/oracle/oradata/OBIEE/share/repository nfs
proto=udp,hard,intr,nfsvers=3,actimeo=1 0 0
vm7:/space/oracle/oradata/OBIEE/share/logs
/space/oracle/oradata/OBIEE/share/logs nfs
proto=udp,hard,intr,nfsvers=3,actimeo=1 0 0
```

As the `oracle` user, create the corresponding directories on machines 1 and 2:

```
cd /space/oracle/oradata/OBIEE
mkdir –p share/catalog
mkdir –p share/repository
mkdir –p share/logs
```

As the `root` user, start the `portmap` and `netfs` services and enable them to start after a reboot:

```
/etc/init.d/portmap start
/etc/init.d/netfs start
/sbin/chkconfig --level 3 portmap on
/sbin/chkconfig --level 3 netfs on
```

4.3.2 Cluster Controller Configuration

Configuring the Oracle BI Cluster Controller to communicate in a clustered environment consists of modifying parameters in the `NQClusterConfig.INI` file located in the following directory:

```
/space/oracle/product/OBIEE/server/Config
```

Open the `NQClusterConfig.INI` file where the BI Cluster Controller has been deployed (machines 1 and 2) and make the following changes:

```
ENABLE_CONTROLLER = YES;
PRIMARY_CONTROLLER = vm1.saglab.uk.oracle.com;
SECONDARY_CONTROLLER = vm2.saglab.uk.oracle.com;
SERVERS = "vm1.saglab.uk.oracle.com","vm2.saglab.uk.oracle.com";
MASTER_SERVER = "vm1.saglab.uk.oracle.com";
```

4.3.3 Server Configuration

Configuring the Oracle BI Server to communicate in a clustered environment consists of modifying parameters in the `NQSConfig.INI` file located in the following directory:

```
/space/oracle/product/OBIEE/server/Config
```

Open the `NQSConfig.INI` file where the BI Server has been deployed (machines 1 and 2) and make the following changes:

In the `[Cache]` section:

```
ENABLE = NO;
```

In the `[Server]` section:

```
#SERVER_HOSTNAME_OR_IP_ADDRESSES = "ALLNICS";
CLUSTER_PARTICIPANT = YES;
REPOSITORY_PUBLISHING_DIRECTORY                                    =
"/space/oracle/oradata/OBIEE/share/repository";
REQUIRE_PUBLISHING_DIRECTORY = YES;
```

4.3.4 Presentation Services Configuration

Configuring the Oracle BI Presentation Services to communicate in a clustered environment consists of modifying parameters in the `instanceconfig.xml` file located in the following directory:

```
/space/oracle/oradata/OBIEE/web/config
```

Open the `instanceconfig.xml` file where BI Presentation Services has been deployed (machines 1 and 2) and make the following changes:

Modify the `<CatalogPath>` element to point to the shared Presentation Catalog:

```
<CatalogPath>/space/oracle/oradata/OBIEE/share/catalog/paint</C
atalogPath>
```

Copy the `paint` catalog from `/space/oracle/oradata/OBIEE/web/catalog` on machine 1 to `/space/oracle/oradata/OBIEE/share/catalog` on machine 7.

Add the following after the `<CatalogPath>` tag:

```
<Catalog>
   <AccountIndexRefreshSecs>120</AccountIndexRefreshSecs>
   <AccountCacheTimeoutSecs>180</AccountCacheTimeoutSecs>
   <CacheTimeoutSecs>1</CacheTimeoutSecs>
   <CacheCleanupSecs>600</CacheCleanupSecs>
   <PrivilegeCacheTimeoutSecs>180</PrivilegeCacheTimeoutSecs>
</Catalog>
```

4.3.5 Presentation Services Plug-In Configuration

The process of configuring the Oracle BI Presentation Services Plug-In to communicate in a clustered environment consists of modifying parameters in the `web.xml` file. This file is located in the following directory:

```
/space/oracle/product/10gAS/10g_J2EE/j2ee/home/applications/ana
lytics/analytics/WEB-INF
```

Open the `web.xml` file where BI Presentation Services Plug-In has been deployed (machine 5) and replace the existing entries:

```
<init-param>
     <param-name>oracle.bi.presentation.sawserver.Host</param-name>
     <param-value>vm1.saglab.uk.oracle.com</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.presentation.sawserver.Port</param-name>
     <param-value>9710</param-value>
</init-param>
```

With:

```
<init-param>
     <param-name>oracle.bi.presentation.Sawservers</param-name>
     <param-value>vm1.saglab.uk.oracle.com:9710;
vm2.saglab.uk.oracle.com:9710</param-value>
     <param-name>
oracle.bi.presentation.sawconnect.loadbalance.AlwaysKeepSessionAffiliation
     </param-name>
     <param-value>Y</param-value>
</init-param>
```

4.3.6 BI ODBC Data Source Configuration (Linux)

On a Linux environment the process of configuring the Oracle BI ODBC Data Source to communicate in a clustered environment consists of modifying parameters in the odbc.ini file. This file is located in the following directory:

```
/space/oracle/product/OBIEE/setup
```

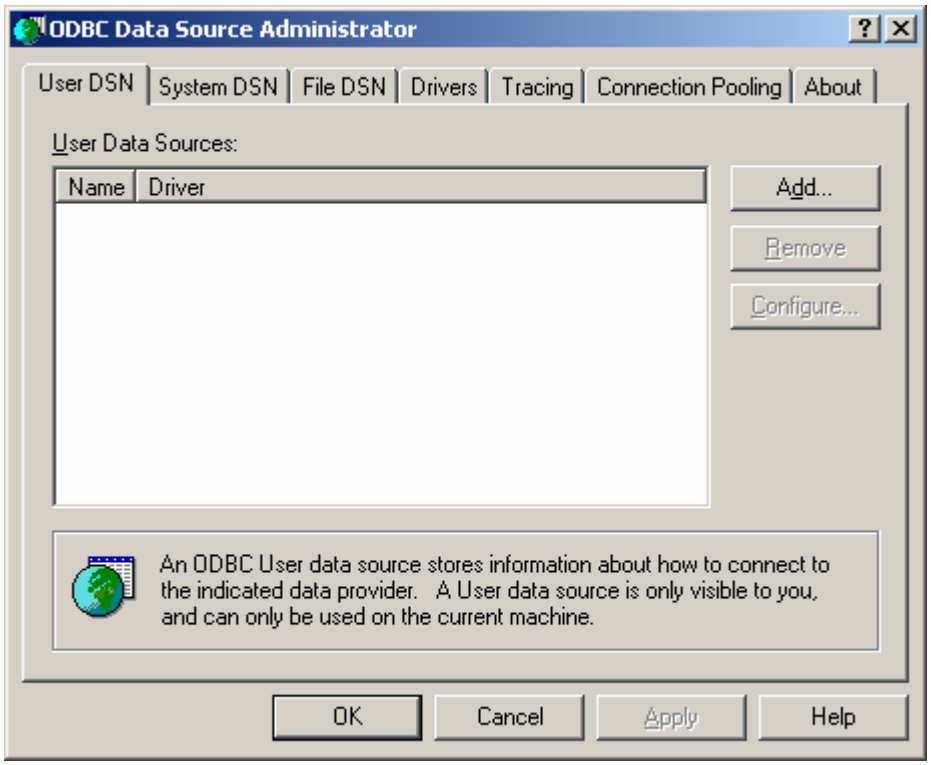
Open the `odbc.ini` file where the BI ODBC Data Source has been deployed (machines 1 and 2) and make the following changes to the `[Cluster]` section:

```
IsClusteredDSN=Yes
PrimaryCCS=vm1.saglab.uk.oracle.com
PrimaryCCSPort=9706
SecondaryCCS=vm2.saglab.uk.oracle.com
SecondaryCCSPort=9706
Regional=No
```

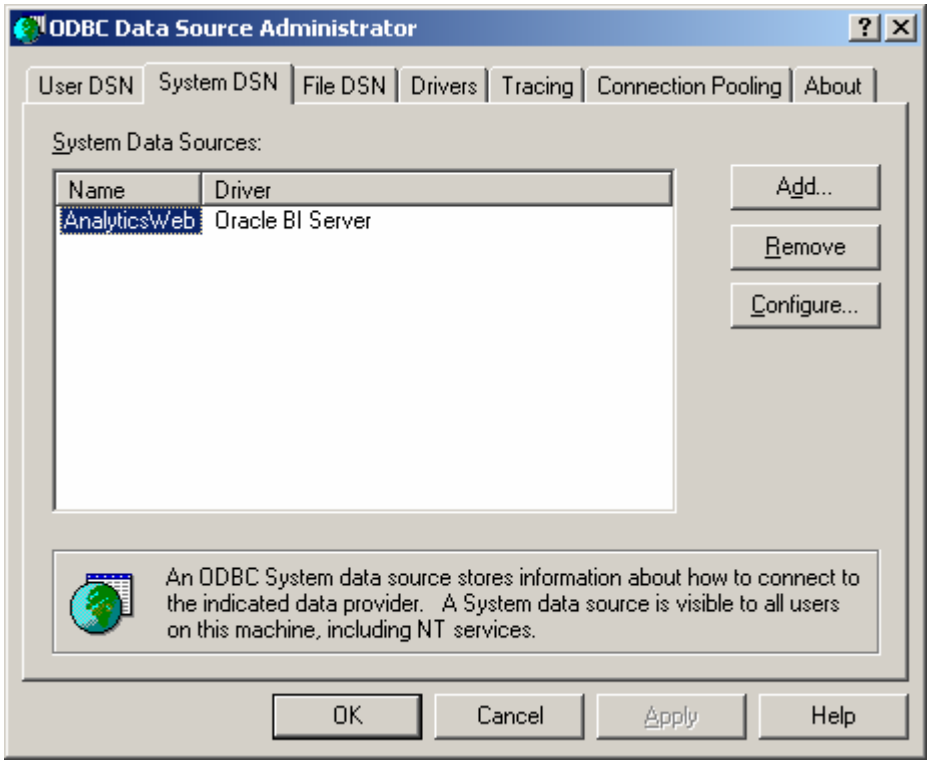
4.3.7 BI ODBC Data Source Configuration (Windows)

On a Windows environment the process of configuring the Oracle BI ODBC Data Source to communicate in a clustered environment consists of creating new ODBC Data Source.

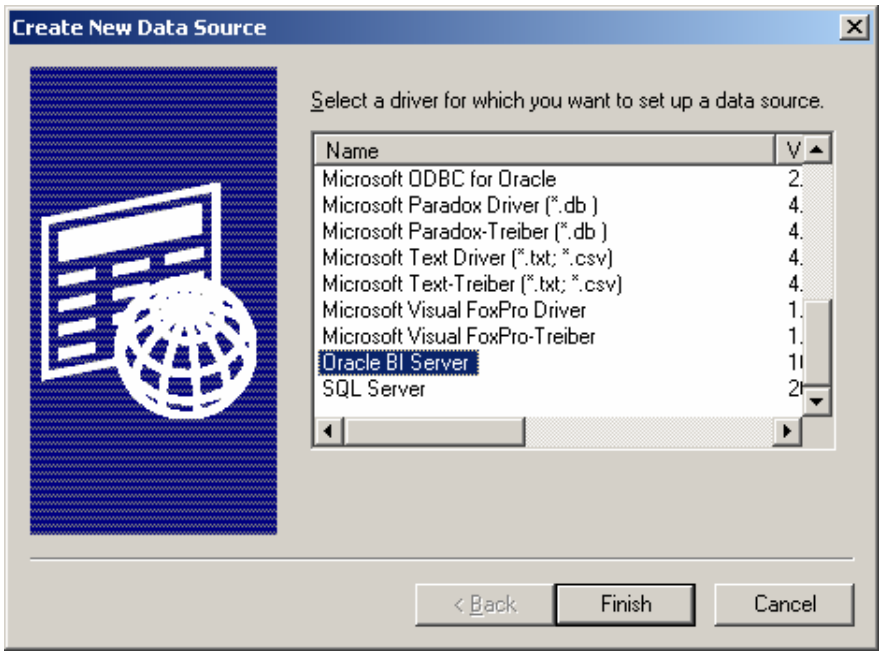
Perform this configuration on all machines where the BI ODBC Data Source has been deployed on a Windows environment (machine 6). Navigate to Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)



Click the **'System DSN'** tab

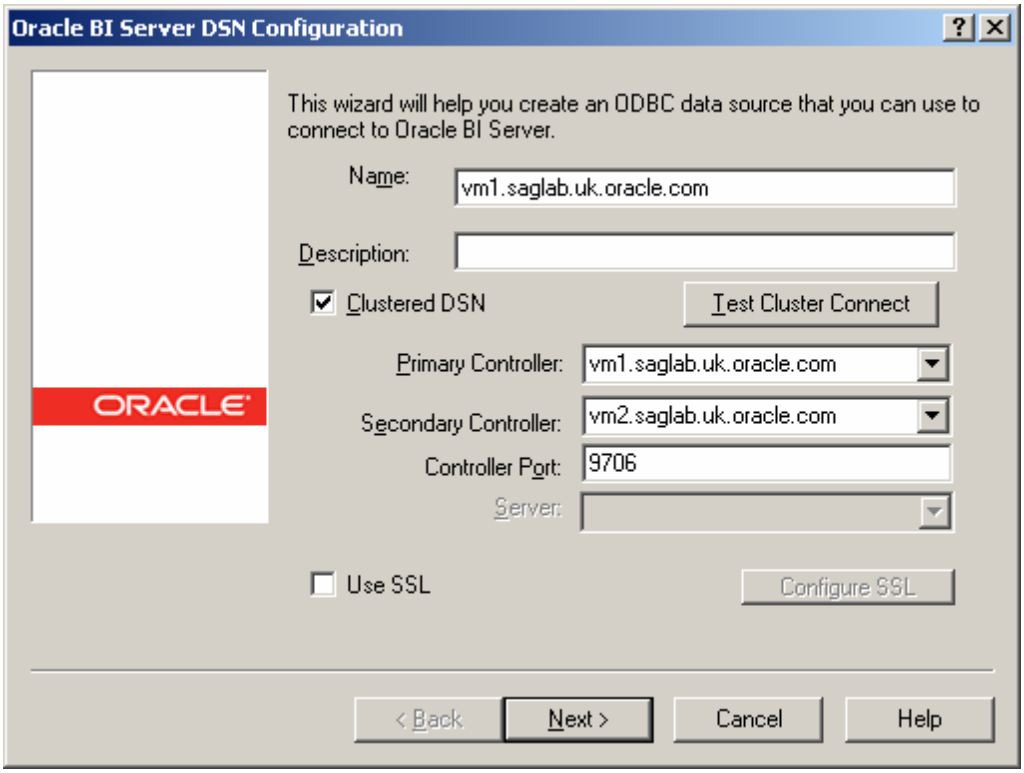


Click the **'Add…'** button.



Scroll to the bottom and select **'Oracle BI Server'**.

Click Finish.



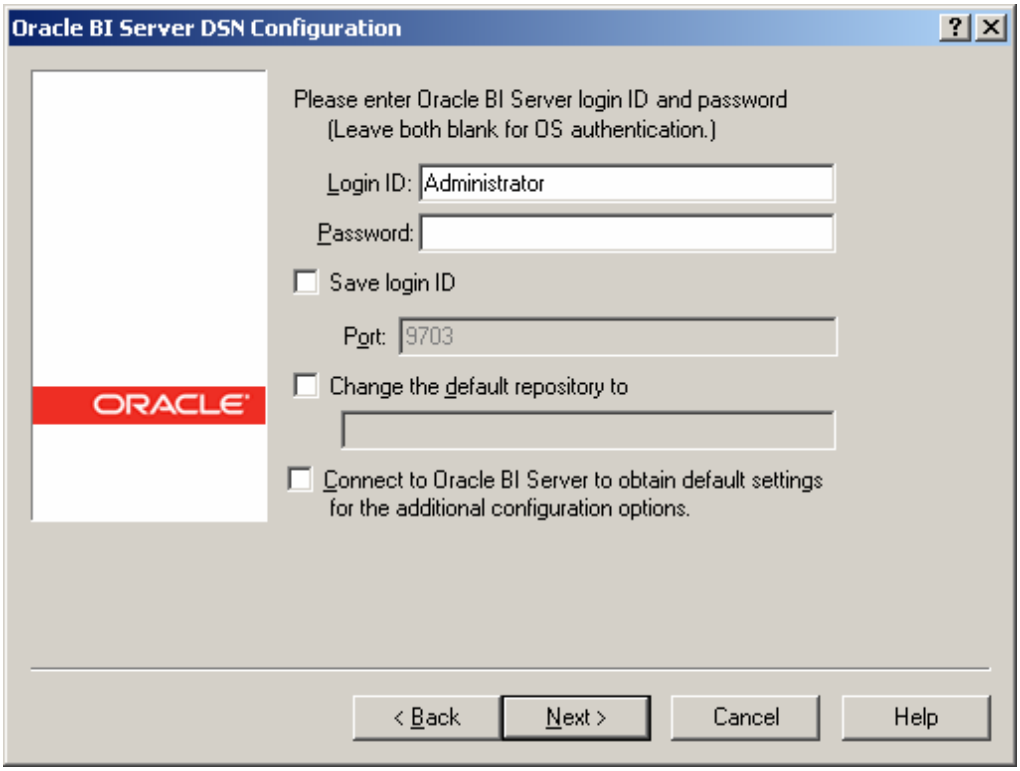
Enter a name for the data source.

Tick the **'Clustered DSN'** check box

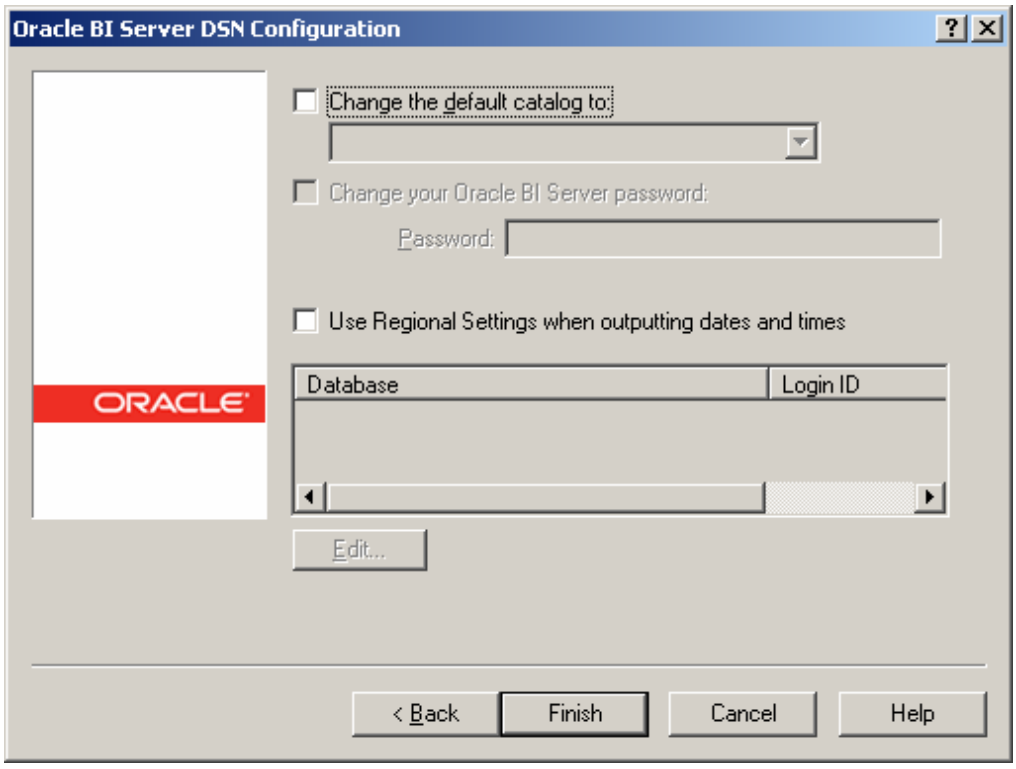
Enter the FQDN for the primary & secondary cluster controllers.

Accept the default entry for the **'Controller Port'**.

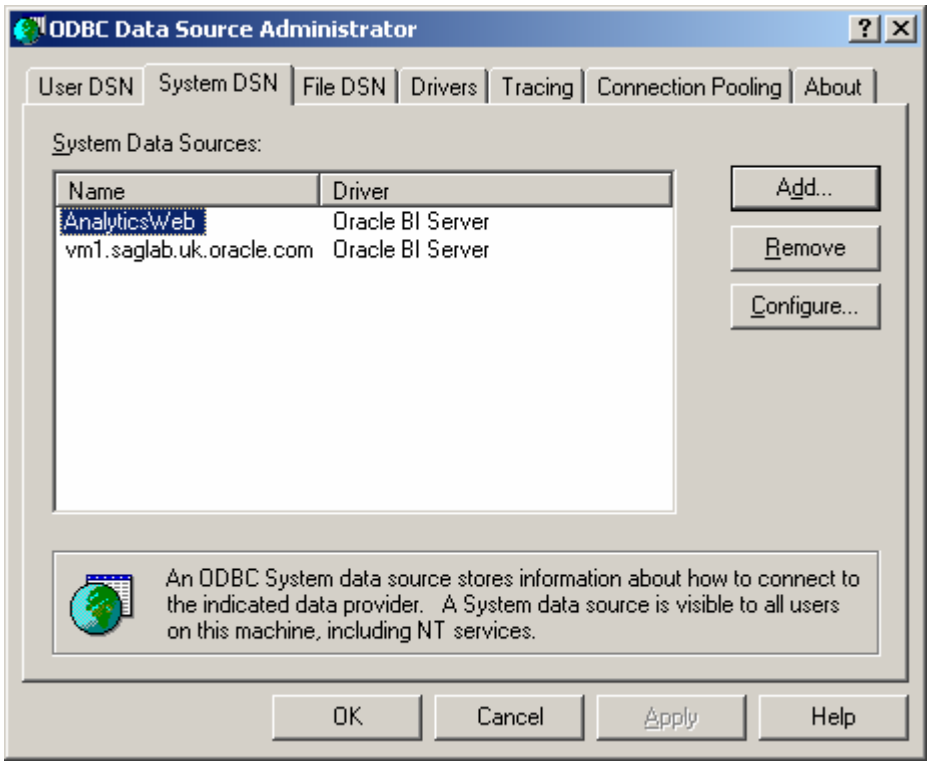
Click Next.



Click Next.



Click Finish.



Click OK. The BI ODBC DSN has been created.

4.4 SSL Configuration

This section describes the steps required to configure SSL for Oracle Business Intelligence Enterprise Edition.

NOTE: The SSL configuration below describes how to create a Certificate Authority (CA) certificate used to sign certificates. This is included for the sake of completion and should not be used in a commercial environment. Certificates should be submitted for signing to Certificate Authorities such as VeriSign or Thawte.

NOTE: If a private CA is required, signing with the CA private key should always be performed in an offline environment to maintain the security of the key and thus the TOE.

4.4.1 Create Directory Structure

On the master server (machine 1) issue the following commands:

```
cd /space/oracle/product/OBIEE/server/Config
mkdir –p ssl/demoCA
mkdir –p ssl/private
mkdir –p ssl/newcerts
cp ../../web/bin/openssl* ssl/
touch ssl/demoCA/.oid
touch ssl/index.txt
touch ssl/serial
cd ssl/
```

Edit the `serial` file and input the number **‘01’**.

4.4.2 Create Certificate Authority (CA) Certificate

Create a CA certificate by issuing the following command:

```
./openssl req -new -x509 –newkey rsa:2048 -keyout
private/cakey.pem -out cacert.pem -config openssl.cnf -days 365
```

The command will output the following:

```
Generating a 2048 bit RSA private key
..+++
.........................................+++
writing new private key to 'private/cakey.pem'
Enter PEM pass phrase: *****
Verifying - Enter PEM pass phrase: *****
-----
```

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: GB
State or Province Name (full name) [Some-State]: Berkshire
Locality Name (eg, city) []: Reading
Organization Name (eg, company) [Some-Organization Pty Ltd]:
Oracle
Organizational Unit Name (eg, section) []: BI
Common Name (eg, YOUR name) []: CA
Email Address []:
```

Make a note of the passphrase entered as it will be required when signing new requests.

The command generates a Certificate Authority (CA) certificate named `cacert.pem`. This certificate verifies the certificates signed by the private key. The validity period for the CA certificate generated is 365 days.

The `cakey.pem` file stores the private key and is generated in the `ssl/private` directory. This key is used to sign certificate requests.

4.4.3 Generate Server Certificate and Server Private Key

The following procedures generate the server certificate and server private key that BI components acting as servers must possess. The server certificate and private key will be used by the Oracle BI Cluster Controller, Oracle BI Server, and Oracle BI Presentation Services components.

Issue the following command:

```
./openssl req -new –newkey rsa:2048 -keyout server-key.pem -out
server-req.pem -config openssl.cnf -days 365
```

The command generates the following dialog:

```
Generating a 2048 bit RSA private key
..........................+++
.............................................................+++
writing new private key to 'server-key.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
```

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: GB
State or Province Name (full name) [Some-State]: Berkshire
Locality Name (eg, city) []: Reading
Organization Name (eg, company) [Some-Organization Pty Ltd]:
Oracle
Organizational Unit Name (eg, section) []: BI
Common Name (eg, YOUR name) []: Server
Email Address []:

Please enter the following 'extra' attributes to be sent with
your certificate request
A challenge password []:
An optional company name []:
```

Make a note of the passphrase entered as it will be needed to decrypt the private key.

The command generates the server private key file `server-key.pem` and the certificate request `server-req.pem`.

4.4.4 Create the Server Certificate

Issue the following command to sign the certificate request:

```
./openssl ca -policy policy_anything -out server-cert.pem -
config openssl.cnf -infiles server-req.pem
```

The command generates the following dialog:

```
Using configuration from openssl.cnf
Enter pass phrase for ./private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'GB'
stateOrProvinceName       :PRINTABLE:'Berkshire'
localityName              :PRINTABLE:'Reading'
organizationName          :PRINTABLE:'Oracle'
organizationalUnitName    :PRINTABLE:'Business Intelligence'
commonName                :PRINTABLE:'Server Certificate'
Certificate is to be certified until Jul 1 08:24:33 2009 GMT
(365 days)
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

When prompted, enter the passphrase for the private key of the CA. This is the passphrase that was supplied when creating the private key cakey.pem in section 4.4.2 “Create Certificate Authority (CA) Certificate”.

4.4.5 Generate Client Certificate and Client Private Key

The following procedures generate the client certificate and client private key that BI components acting as clients must possess. The client certificate and private key will be used by the Oracle BI Administration Tool.

Issue the following command:

```
./openssl req -new –newkey rsa:2048 -keyout client-key.pem -out
client-req.pem -config openssl.cnf -days 365
```

The command generates the following dialog:

```
Generating a 2048 bit RSA private key
..........................+++
.............................................................+++
writing new private key to 'client-key.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: GB
State or Province Name (full name) [Some-State]: Berkshire
Locality Name (eg, city) []: Reading
Organization Name (eg, company) [Some-Organization Pty Ltd]:
Oracle
Organizational Unit Name (eg, section) []: BI
Common Name (eg, YOUR name) []: Client
Email Address []:

Please enter the following 'extra' attributes to be sent with
your certificate request
A challenge password []:
```

```
An optional company name []:
```

Make a note of the passphrase entered as it will be needed to decrypt the private key.

The command generates the client private key file client-key.pem and the certificate request (unsigned client certificate) client-req.pem.

4.4.6 Create the Client Certificate

Issue the following command to sign the certificate request:

```
./openssl ca -policy policy_anything -out client-cert.pem -
config openssl.cnf -infiles client-req.pem
```

The command generates the following dialog:

```
Using configuration from openssl.cnf
Enter pass phrase for ./private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'GB'
stateOrProvinceName       :PRINTABLE:'Berkshire'
localityName              :PRINTABLE:'Reading'
organizationName          :PRINTABLE:'Oracle'
organizationalUnitName    :PRINTABLE:'Business Intelligence'
commonName                :PRINTABLE:'Client Certificate'
Certificate is to be certified until Jul 1 08:33:03 2009 GMT
(365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

This command generates the signed client certificate client-cert.pem.

4.4.7 Create Passphrase Files

Under the ssl directory, create a passphrase file called `serverpwd.txt`. In this file, input the passphrase used to encrypt the server private key.

Under the ssl directory, create a passphrase file called `clientpwd.txt`. In this file, input the passphrase used to encrypt the client private key.

Copy the files cacert.pem, server-cert.pem, server-key.pem and serverpwd.txt to the `/space/oracle/product/OBIEE/server/Config` directory on machines 1 and 2.

Copy the files cacert.pem, client-cert.pem, client-key.pem and clientpwd.txt to the `C:\oracle\product\OBIEE\server\Config` directory on machine 6.

4.4.8 Create Java Keystore and Generate Certificate

For BI components that are Java-based, a Java certificate store must be created that contains certificates and key files.

This procedure creates a Java Keystore that will store the certificate and private key used by the Oracle BI Presentation Services Plug-in (Java Servlet) and Oracle BI Javahost components.

The keystore is generated and managed using the keytool command-line executable that ships with JDK. The keytool command-line executable to be used is located in the Oracle Application Server home jdk/bin directory.

In the terminal being used issue the following commands:

```
export ORACLE_HOME=/space/oracle/product/10gAS/10g_J2EE
export PATH=$ORACLE_HOME/jdk/bin:$PATH
```

Generate Private Key

To generate the private key, use the genkey subcommand of the keytool command with inputs as shown:

```
keytool -genkey -v -alias javahostkey -keyalg rsa -keysize 2048
-validity 365 -keystore javahost.keystore -storepass oracle
```

The command generates the following dialog:

```
What is your first and last name?
  [Unknown]: Javahost
What is the name of your organization unit?
  [Unknown]: BI
What is the name of your organization?
  [Unknown]: Oracle
What is the name of your City or Locality?
  [Unknown]: Reading
What is the name of your State or Province?
  [Unknown]: Berkshire
What is the two-letter country code for this unit?
```

```
  [Unknown]: GB
Is   CN=Server   Certificate,   OU=BI,   O=Oracle,   L=Reading,
ST=Berkshire, C=GB correct?
  [no]: YES

Generating 2,048 bit rsa key pair and self-signed certificate
(MD5withRSA)
        for:   CN=Javahost,   OU=BI,   O=Oracle,   L=Reading,
ST=Berkshire, C=GB
Enter key password for <javahostkey>
        (RETURN if same as keystore password):
[Storing javahost.keystore]
```

In this example, the keystore called `javahost.keystore` stores the private key with an alias of `javahostkey` and with a password of `analytics`.

The alias and password values are referenced when setting SSL-related parameters for the Oracle BI Presentation Service Plug-in component.

Generate the Certificate Request

To generate the certificate, use the certreq subcommand of the keytool command with the inputs as shown:

```
keytool -certreq -v -alias javahostkey -file javahost-req.pem –
keystore javahost.keystore -storepass oracle
```

The command generates the following output:

```
Certification request stored in file <javahost-req.pem>
Submit this to your CA
```

The certificate request must be signed by a CA, as shown in the following procedure.

Sign the Client Certificate

Issue the following command to sign the certificate request:

```
./openssl ca -policy policy_anything -out javahost-cert.pem -
config openssl.cnf –infiles javahost-req.pem
```

The command generates the following dialog:

```
Using configuration from openssl.cnf
```

```
Enter pass phrase for ./private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'GB'
stateOrProvinceName       :PRINTABLE:'Berkshire'
localityName              :PRINTABLE:'Reading'
organizationName          :PRINTABLE:'Oracle'
organizationalUnitName    :PRINTABLE:'BI'
commonName                :PRINTABLE:'Javahost'
Certificate is to be certified until Jul 1 09:05:57 2009 GMT
(365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

This command will create a certificate called `javahost-cert.pem`.

Convert to X509 File

Copy the `javahost-cert.pem` file to `javahost-cert-x509.pem`. Open the `javahost-cert-x509.pem` file and remove all lines that appear before the text:

```
----BEGIN CERTIFICATE----
```

The certificate file should be similar to the following example:

```
-----BEGIN CERTIFICATE-----
MIICcjCCAdugAwIBAgIBEjANBgkqhkiG9w0BAQQFADBkMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCQ0ExEjAQBgNVBAcTCVNhbiBNYXRlbzEPMA0GA1UEChMGU2llYmVs
MRIwEAYDVQQLEwlBbmFseXRpY3MxDzANBgNVBAMTBkNBQ2VydDAeFw0wNjAzMDYx
OTU2NTFaFw0wNzAzMDYxOTU2NTFaMGcxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJD
QTESMBAGA1UEBxMJU2FuIE1hdGVvMQ8wDQYDVQQKEwZTaWViZWwxEjAQBgNVBAsT
CUFuYWx5dGljczESMBAGA1UEAxMJSm9iTWFuZ2VyMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDBIR0ATYE6UtEL4W/bQ1xPIHsT7S5EcmfpezZQCeumBSg00/5U
nIYFfPHBjcjgJKChVG+DSZRxPJOAifLeKTb6pk3lHoJJ9Gr/HuryYOc46Efd/q0+
cXMQ+fPC+0M/0caohryfSAjcW+O0IwycHjbmj4VXc4L4OTgRHIQv0oVRkQIDAQAB
ozEwLzAtBglghkgBhvhCAQ0EIBYeR2VuZXJhdGVkIHdpdGggUlNBIEJTQUZFIFNT
TC1DMA0GCSqGSIb3DQEBBAUAA4GBAC81Hi77GChZYyiYXTNIN0oEVS4CiKpAMUg9
55QMaQU/RsdWYe8ne34EpXDWY6LVdBi8nxL41l/VLckM2Gbn72LZx5KelzPuzgwy
qC8Z4HGOvjAzYHA8AQhRHaFSYWZoUkbay/6/8bYofJJarkjD68rdz1i0m9L3/sWM
MmEQmHNo
-----END CERTIFICATE-----
```

Import the Certificate Authority File to Java Keystore

The Certificate Authority (CA) certificate that was used to sign the certificate request as described in the topic "Generating the Certificate" on page 91 must be imported to a Java keystore. Use the keytool utility as shown in the following procedure.

Issue the following command to import the CA certificate to the Java keystore:

```
keytool -import -keystore javahost.keystore -storepass oracle –
alias cacertificates -file cacert.pem
```

The command generates the following dialog:

```
Owner: CN=CA, OU=BI, O=Oracle, L=Reading, ST=Berkshire, C=GB
Issuer: CN=CA, OU=BI, O=Oracle, L=Reading, ST=Berkshire, C=GB
Serial number: d72b86888f4f7028
Valid from: Tue Jul 01 09:08:26 BST 2008 until: Wed Jul 01 09:08:26 BST
2009
Certificate fingerprints:
    MD5:  35:75:43:5F:A5:00:3A:18:F8:AB:0D:2B:F2:0C:C0:22
    SHA1: 08:1C:6A:62:BD:A9:36:2E:B6:12:76:D3:FB:AE:71:9B:2B:83:6A:C2
Trust this certification? [no]: YES
Certificate was added to keystore
```

Import the Certificate to the Java Keystore

The certificate `javahost-cert-x509.pem`, created above, must be imported to the Java keystore.

Issue the following command to import the certificate:

```
keytool -import -keystore javahost.keystore -storepass oracle –
alias javahostkey -file javahost-cert-x509.pem
```

The command generates the following output:

```
Certificate reply was installed in keystore
```

Copy the `javahost.keystore` file to the `/space/oracle/product/OBIEE/server/Config` directory on machine 5.

4.4.9 Oracle Wallets

The Oracle HTTP Server, Database Server, OID Server and Client use the certificate stored within a wallet to communicate over SSL. The `orapki` utility is used to create the wallet and is located in the `$ORACLE_HOME/bin` directory.

On machine 1, open a new terminal window and issue the following commands to create the wallets:

```
export ORACLE_HOME=/space/oracle/product/10.2.0/client
export PATH=$ORACLE_HOME/bin:$PATH
```

Create the Oracle Wallet:

```
orapki wallet create –wallet vm1 -auto_login
```

Enter a password for the wallet when prompted.

Add a Certificate Request to the Wallet:

```
orapki wallet add –wallet vm1 –dn "CN=vm1.saglab.uk.oracle.com,
OU=BI, O=Oracle, L=Reading, ST=Berkshire, C=GB" -keysize 2048 -
validity 365
```

Enter the wallet password when prompted.

Export the Certificate Request from the Oracle Wallet:

```
orapki wallet export -wallet vm1 -dn
"CN=vm1.saglab.uk.oracle.com, OU=BI, O=Oracle, L=Reading,
ST=Berkshire, C=GB" -request vm1-req.pem
```

Sign the Certificate Request:

```
./openssl ca -policy policy_anything -out vm1-cert.pem -config
openssl.cnf –infiles vm1-req.pem
```

Add the CA Certificate to the Oracle Wallet:

```
orapki wallet add -wallet vm1 -trusted_cert –cert cacert.pem
```

Enter the wallet password when prompted.

Add the Signed Certificate Request to the Oracle Wallet:

```
orapki wallet add -wallet vm1 -user_cert -cert vm1-cert.pem
```

Enter the wallet password when prompted.

View the Contents of the Oracle Wallet:

```
orapki wallet display -wallet vm1
```

Repeat this process creating wallets for machines 2 to 6, adjusting the wallet name (specified after the -wallet option) and the CN and then copy the wallets to the respective machines. This process should be repeated for the components that require a wallet – the Oracle Database Server (machine 3), Oracle OID Server (machine 4), Oracle HTTP Server (machine 5), and Oracle Clients (machines 1, 2 and 6).

4.4.10 Create CMS Key Database File

On the Windows XP client machine (machine 6) open a command prompt and issue the following commands:

```
cd \
cd Program Files\IBM\gsk7\bin
```

Create the CMS Key Database File:

```
gsk7cmd -keydb -create -db key.kdb -pw oracle -type cms -expire
365
```

Add a Certificate Request to the CMS Key Database File:

```
gsk7cmd -certreq -create -db key.kdb -pw oracle -label "LDAP Client" -dn
"CN=vm6.saglab.uk.oracle.com,OU=BI,O=Oracle,L=Reading,ST=Berkshire,C=GB"  -
size 1024 -file ldap-client-req.pem
```

The `ldap-client-req.pem` certificate request file should be copied to the `/space/oracle/product/OBIEE/server/Config/ssl` directory on machine

1 so that the request can be signed using the command below. The request must be signed from machine 1.

Sign the Certificate Request:

```
./openssl ca -policy policy_anything -out ldap-client-cert.pem
-config openssl.cnf –infiles ldap-client-req.pem
```

Once the certificate request has been signed copy the `ldap-client-cert.pem` and `cacert.pem` files to the `C:\Progam Files\IBM\gsk7\bin` directory on machine 6.

Add the CA Certificate to the CMS Key Database File:

```
gsk7cmd -cert -add -db key.kdb -pw oracle -label "CA
Certificate" -format binary -trust enable -file cacert.pem
```

Add the Signed Certificate Request to the CMS Key Database File:

```
gsk7cmd -cert -receive -file ldap-client-cert.pem -db key.kdb -
pw oracle -format binary -default_cert yes
```

Note: The `ldap-client-cert.pem` must be in X509 format.

After creating the CMS key database file, store it in the BI Server configuration directory `C:\oracle\product\OBIEE\server\Config`.

Repeat the process above to create CMS Key Database Files for machines 1 and 2, storing the `key.kdb` in the BI Server configuration directory `/space/oracle/product/OBIEE/server/Config`.

4.4.11 Configure Oracle BI Cluster Controller

Configuring the Oracle BI Cluster Controller to communicate over SSL consists of modifying parameters in the `NQClusterConfig.INI` file located in the following directory:

```
/space/oracle/product/OBIEE/server/Config
```

Open the `NQClusterConfig.INI` file where the BI Cluster Controller has been deployed (machines 1 and 2) and make the following changes:

```
```

```
SSL=YES;
SSL_CERTIFICATE_FILE="server-cert.pem";
SSL_PRIVATE_KEY_FILE="server-key.pem";
SSL_PK_PASSPHRASE_FILE="serverpwd.txt";
SSL_VERIFY_PEER=YES;
SSL_CA_CERTIFICATE_FILE="cacert.pem";
SSL_TRUSTED_PEER_DNS="C=GB/ST=Berkshire/L=Reading/O=Oracle/OU=B
I";
SSL_CERT_VERIFICATION_DEPTH=1;
SSL_CIPHER_LIST="DES-CBC3-SHA";
```

4.4.12 Configure Oracle BI Server

Configuring the Oracle BI Server to communicate over SSL consists of modifying parameters in the `NQSConfig.INI` file located in the following directory:

```
/space/oracle/product/OBIEE/server/Config
```

Open the `NQSConfig.INI` file where the Oracle BI Server has been deployed (machines 1 and 2) and make the following changes:

```
SSL=YES;
SSL_CERTIFICATE_FILE="server-cert.pem";
SSL_PRIVATE_KEY_FILE="server-key.pem";
SSL_PK_PASSPHRASE_FILE="serverpwd.txt";
SSL_VERIFY_PEER=YES;
SSL_CA_CERTIFICATE_FILE="cacert.pem";
SSL_TRUSTED_PEER_DNS="C=GB/ST=Berkshire/L=Reading/O=Oracle/OU=B
I";
SSL_CERT_VERIFICATION_DEPTH=1;
SSL_CIPHER_LIST="DES-CBC3-SHA";
```

4.4.13 Configure Oracle ODBC Data Source (Linux)

On a Linux environment, the process of configuring Oracle ODBC Data Source to communicate over SSL consists of modifying parameters in the odbc.ini file. This file is located in the following directory:

```
/space/oracle/product/OBIEE/setup
```

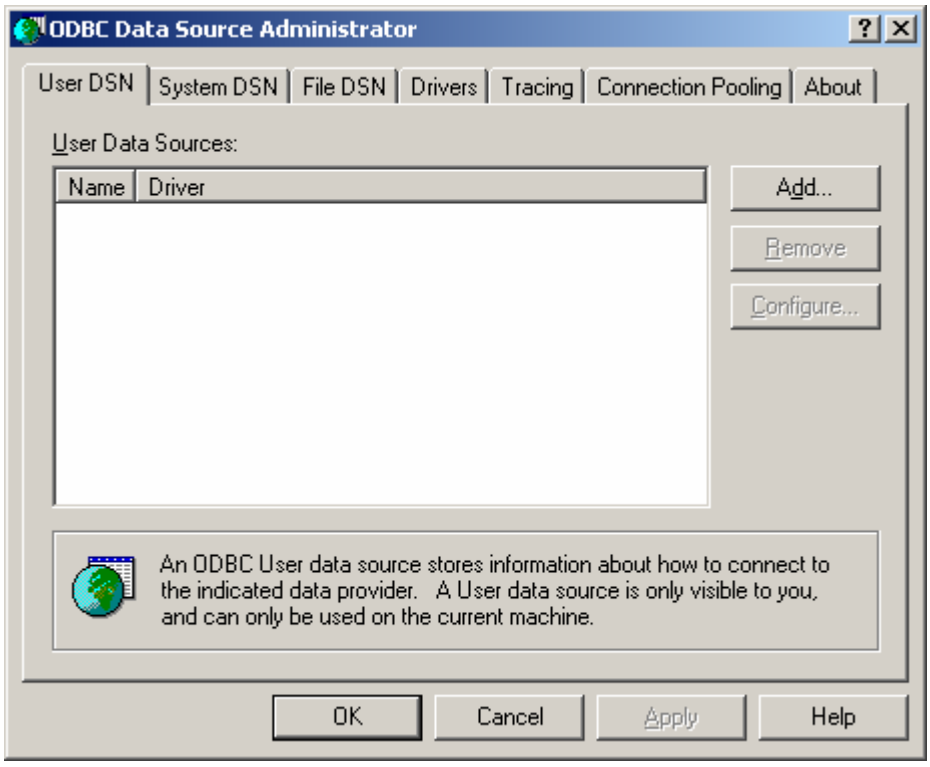
Perform this configuration on all machines where the Oracle ODBC Data Source has been deployed (machines 1 and 2). Open the `odbc.ini` file and add the following to the `[AnalyticsWeb]` section of the file:

```
SSL=YES
SSLCertificateFile=/space/oracle/product/OBIEE/server/Config/se
rver-cert.pem
SSLPrivateKeyFile=/space/oracle/product/OBIEE/server/Config/ser
ver-key.pem
SSLPassphraseFile=/space/oracle/product/OBIEE/server/Config/ser
verpwd.txt
SSLCipherList=DES-CBC3-SHA
SSLVerifyPeer=Yes
SSLCACertificateFile=/space/oracle/product/OBIEE/server/Config/
cacert.pem
SSLTrustedPeerDNs=C=GB/ST=Berkshire/L=Reading/O=Oracle/OU=BI
SSLCertVerificationDepth=1
```

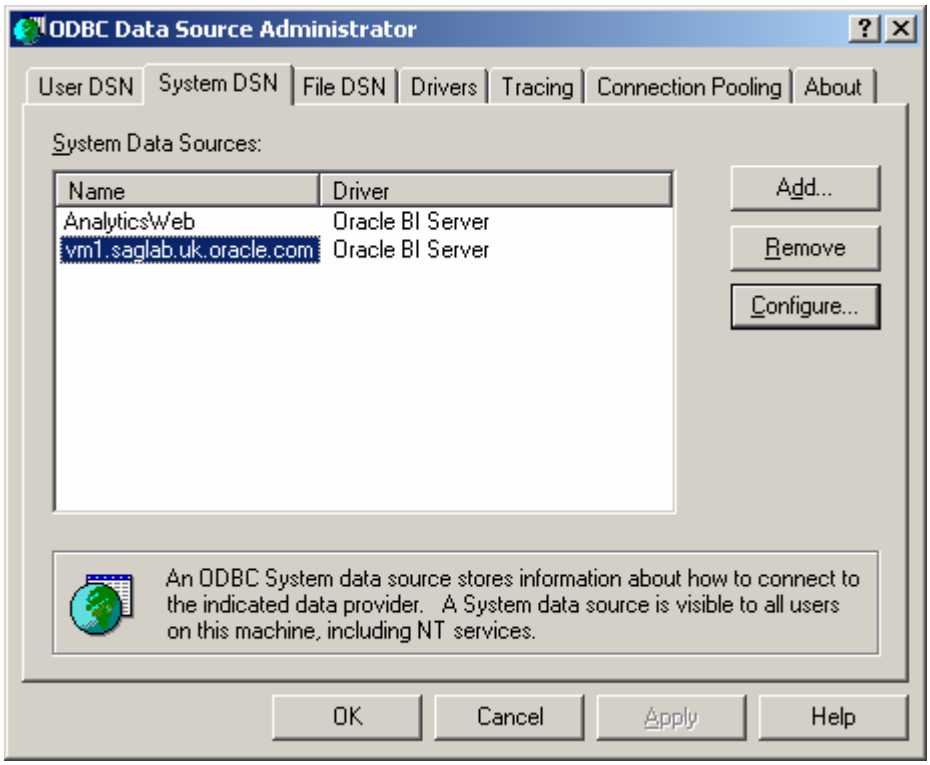
4.4.14 Configure Oracle ODBC Data Source (Windows)

On a Windows environment, the process of configuring the Oracle ODBC Data Source to communicate over SSL consists of modifying the ODBC Data Source created above.

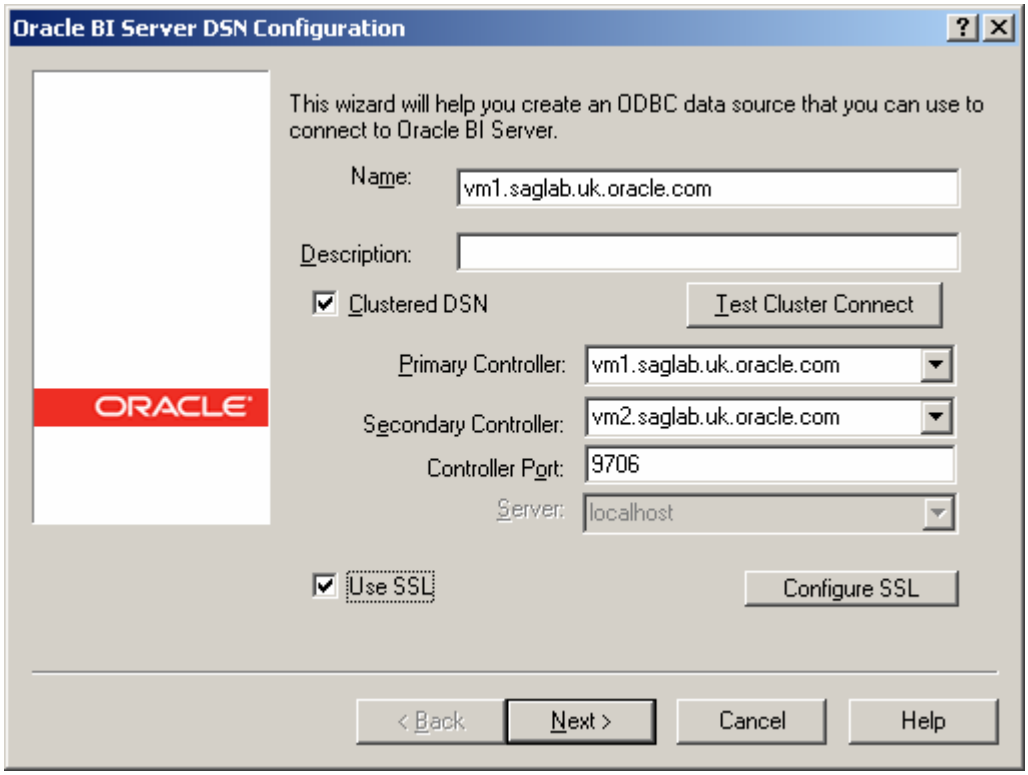
Perform this configuration on all machines where the BI ODBC Data Source has been deployed on a Windows environment (machine 6). Navigate to Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)



Click the **'System DSN'** tab.

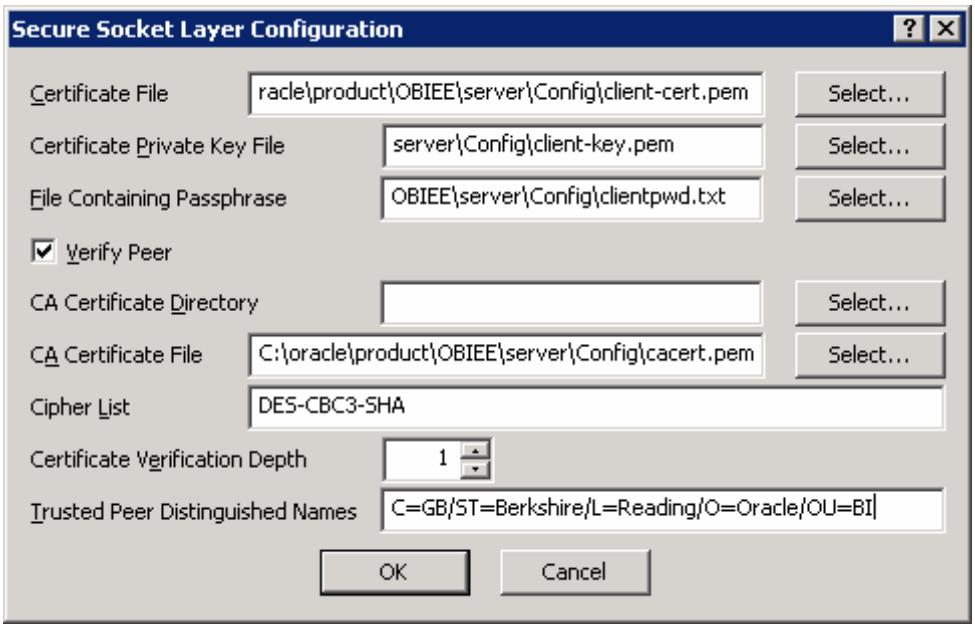


Select the **'vm1.saglab.uk.oracle.com'** entry and click the **'Configure'** button.



Tick the **'Use SSL'** check box.

Click the **'Configure SSL'** button.



Enter the location of the Client Certificate file in the **'Certificate File'** field.

Enter the location of the Client Private Key file in the **'Certificate Private Key File'** field.

Enter the location of the passphrase file for the Client Key in the **'File Containing Passphrase'** field

Tick the **'Verify Peer'** check box.

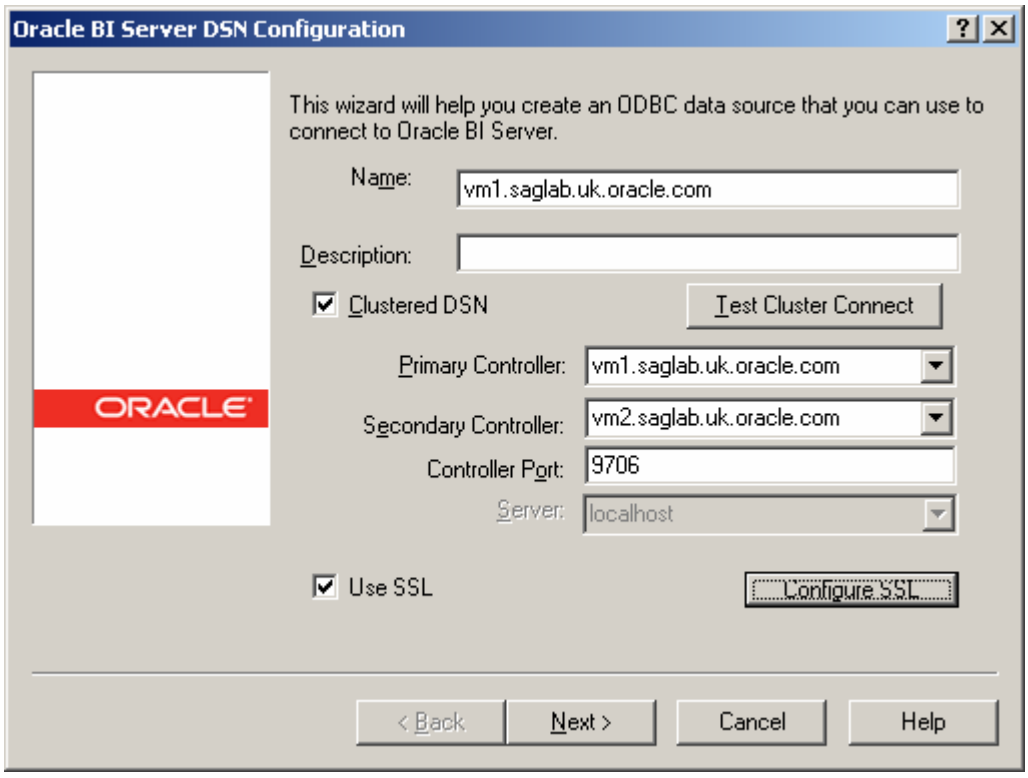
Enter the location of the CA Certificate file in the **'CA Certificate File'** field.

Enter **'DES-CBC3-SHA'** in the **'Cipher List'** field.

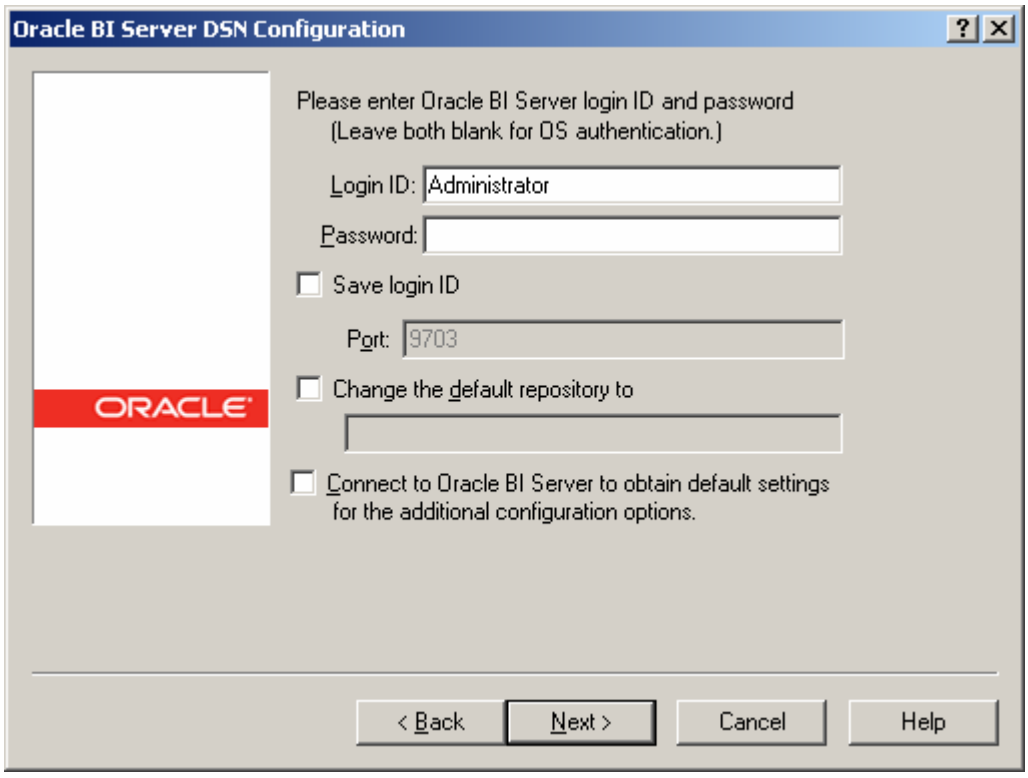
Enter a value of **'1'** in the **'Certificate Verification Depth'** field.

Enter the DNs of servers that will be allowed to connect in the **'Trusted Peer Distinguished Names'** field.

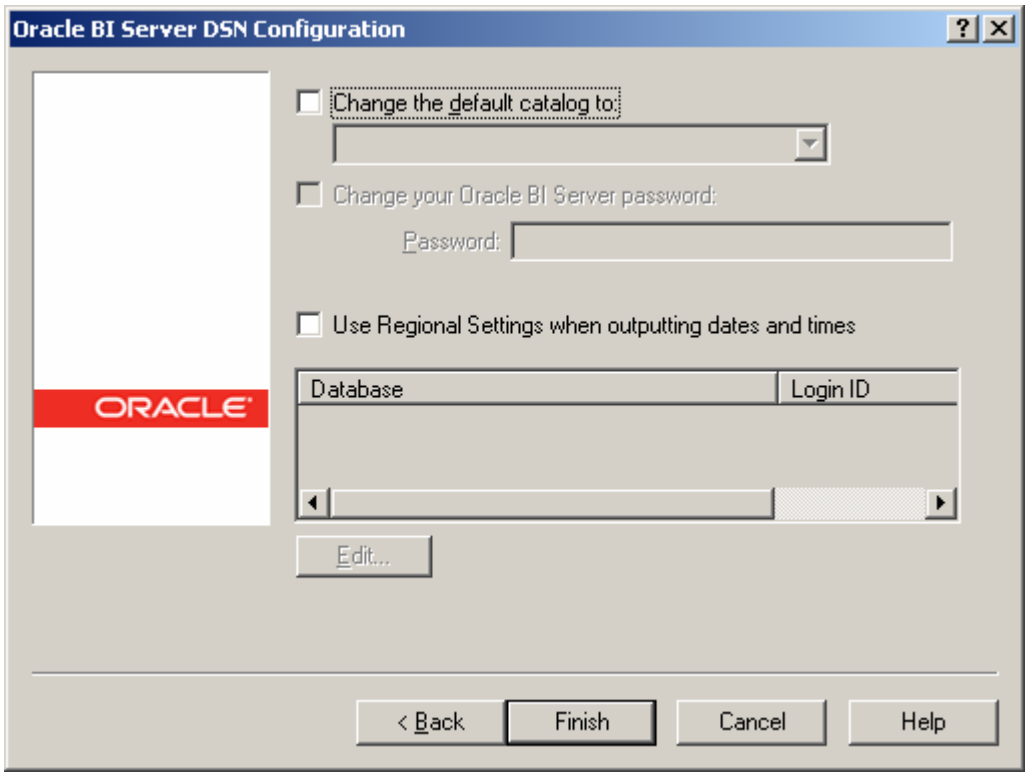
Click OK.



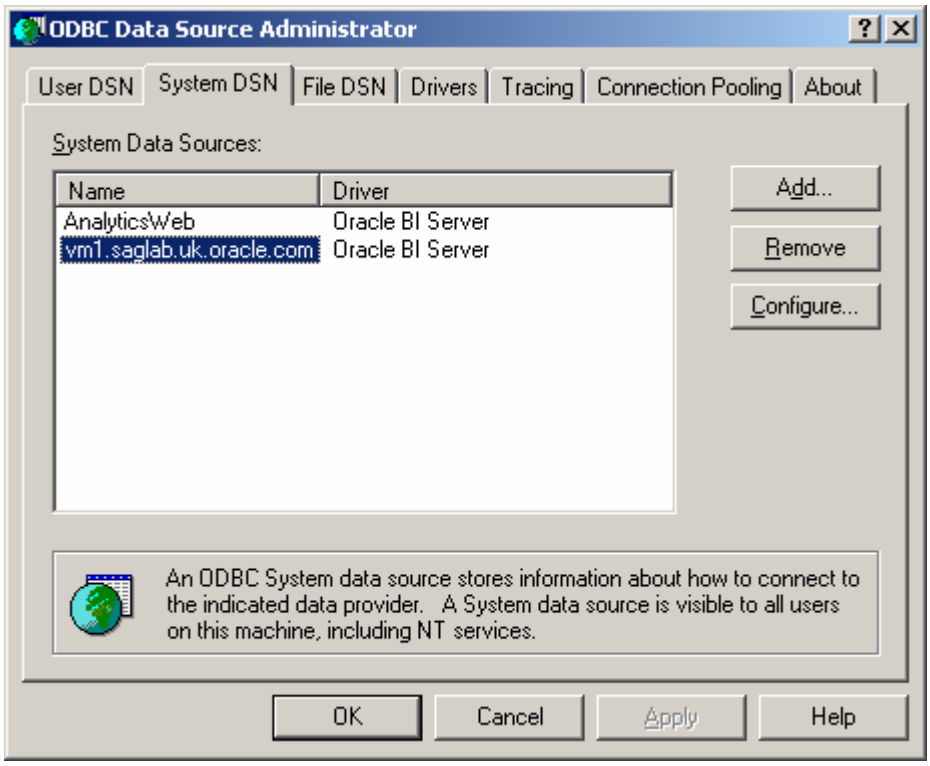
Click Next.



Click Next.



Click Finish.



Click OK.

Copy the client certificate, client private key, passphrase file and CA certificate file to the directory specified in the parameters. In the examples specified, the directory is `C:\oracle\product\OBIEE\server\Config`.

4.4.15 Configure Oracle BI Presentation Services

The process of configuring Oracle BI Presentation Services to communicate over SSL consists of modifying parameters in the `instanceconfig.xml` configuration file. BI Presentation Services accesses certificates and key files from its credential store. The paths to certificates and keys that BI Presentation Services uses must be stored in its credential store `credentialstore.xml`.

Specifying Certificate and Key Paths in BI Presentation Services Credential Store

The `credentialstore.xml` and `instanceconfig.xml` files are located in the following directory:

```
/space/oracle/oradata/OBIEE/web/config
```

Perform this configuration on all machines where the Oracle BI Presentation Services has been deployed (machines 1 and 2).

To specify certificate and key paths in the BI Presentation Services Credential Store edit the `credentialstore.xml` file and add the following to specify the paths to the server certificate, private key and CA certificate files:

```
<sawcs:credential type="x509" alias="obips">
 <sawcs:key
  encoding="pem"
  passphraseFile="/space/oracle/product/OBIEE/server/Config/serverpwd.txt"
  path="/space/oracle/product/OBIEE/server/Config/server-key.pem"/>

 <sawcs:certificate
  encoding="pem"
  path="/space/oracle/product/OBIEE/server/Config/server-cert.pem"/>
</sawcs:credential>

<sawcs:trustedCertificate
 alias="cacert"
 encoding="pem"
 path="/space/oracle/product/OBIEE/server/Config/cacert.pem"/>
```

NOTE: In the above example, the certificate and key paths are stored under the alias “obips” and the trusted CA certificate file is stored under the alias “cacert”.

To configure BI Presentation Services for SSL communication open the `instanceconfig.xml` file and add the following elements between the `<ServerInstance></ServerInstance>` node:

```
<Listener                  ssl="true"                credentialAlias="obips"
certificateVerificationDepth="1" verifyPeers="true" cipherSuites="DES-CBC3-
SHA">
</Listener>

<CredentialStore>
  <CredentialStorage
     type="file"
     path="/space/oracle/oradata/OBIEE/web/config/credentialstore.xml"/>
</CredentialStore>
```

In the preceding example configuration, BI Presentation Services is directed to obtain the certificate and key using the alias “obips”. You must specify the alias under which the certificates and keys were stored in the credential store. In the example, the keystore that contains the certificate, private key, and CA is the XML file store called `credentialstore.xml`.

4.4.16 Configure Oracle BI Presentation Services Plug-In

The process of configuring the BI Presentation Services Plug-in (Java Servlet) deployed on a J2EE container consists of adding SSL-related entries in the web.xml file. This file is located in the following directory:

```
/space/oracle/product/10gAS/10g_J2EE/j2ee/home/applications/ana
lytics/analytics/WEB-INF
```

The BI Presentation Services Plug-In (Java Servlet) uses a Java keystore to store certificates and keys. The keystore created earlier will be used.

Open the `web.xml` file for the analytics application deployed on your J2EE server and insert the following elements and values inside the `<servlet>` tag:

```
<init-param>
     <param-name>oracle.bi.Secure</param-name>
     <param-value>Y</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.CertAlias</param-name>
     <param-value>javahostkey</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.CertStoreFile</param-name>
```

```
     <param-
value>/space/oracle/product/OBIEE/server/Config/javahost.keystore</param-
value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.CertStorePwd</param-name>
     <param-value>oracle</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.TrustStoreFile</param-name>
     <param-
value>/space/oracle/product/OBIEE/server/Config/javahost.keystore</param-
value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.TrustStorePwd</param-name>
     <param-value>oracle</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.Protocol</param-name>
     <param-value>TLS</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.TrustAnyPeer</param-name>
     <param-value>N</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.TrustedPeerDNs</param-name>
     <param-value>C=GB/ST=Berkshire/L=Reading/O=Oracle/OU=BI</param-value>
</init-param>
<init-param>
     <param-name>oracle.bi.ssl.EnabledCipherSuites</param-name>
     <param-value>SSL_RSA_WITH_3DES_EDE_CBC_SHA</param-value>
</init-param>
```

Copy this keystore (named `javahost.keystore`) to all machines where the BI Presentation Services Plug-in is deployed (machine 5).

4.4.17 Configure Oracle BI Java Host

The BI Java Host component is Java based and uses the Java Keystore to store certificates and keys that it uses.

The BI Java Host is configured by setting SSL-related entries in the `config.xml` and `instanceconfig.xml` files.

The `config.xml` file is located in the following directory:

```
/space/oracle/product/OBIEE/web/javahost/config/
```

The `instanceconfig.xml` file is located in the following directory:

```
/space/oracle/oradata/OBIEE/web/config/
```

Perform this configuration on all machines where the Oracle BI Java Host has been deployed (machines 1 and 2).

Open the `config.xml` file and add the following SSL-related elements and values under the `<Listener>` node:

```
<PermittedClientList><Host Name of Machine 1>, <Host Name of Machine
2></PermittedClientList>
<Secure>Yes</Secure>
<SSL>
   <CertAlias>javahostkey</CertAlias>
<CertStoreFile>/space/oracle/product/OBIEE/server/Config/javahost.keystore
</CertStoreFile>
   <CertStorePwd>oracle</CertStorePwd>
   <KeyPwd>oracle</KeyPwd>
   <CertStoreType>JKS</CertStoreType>
<TrustStoreFile>/space/oracle/product/OBIEE/server/Config/javahost.keystore
</TrustStoreFile>
   <TrustStorePwd>oracle</TrustStorePwd>
   <TrustStoreType>JKS</TrustStoreType>
   <TrustesPeersDns>
      OU=BI,O=Oracle,L=Reading,ST=Berkshire,C=GB
   </TrustesPeersDns>
   <TrustAnyPeer>N</TrustAnyPeer>
   <EnabledCipherSuites>SSL_RSA_WITH_3DES_EDE_CBC_SHA</EnabledCipherSuites>
</SSL>
```

NOTE: The `config.xml` file has the above-mentioned elements commented out. You may choose to uncomment the elements and add the corresponding values. Or, you may leave the elements commented out and create new ones as described above.

The `javahost.keystore` file should be copied to the `/space/oracle/product/OBIEE/server/Config` on all machines where the BI Java Host is deployed (machines 1 and 2).

Open the `instanceconfig.xml` file and add the following SSL-related elements and values under the `<ServerInstance>` node:

```
<JavaHostProxy>
  <Hosts>
    <Host address="vm1.saglab.uk.oracle.com" port="9810" ssl="true"
credentialAlias="obips" certificateVerificationDepth="1"
verifyPeers="true"/>
    <Host address="vm2.saglab.uk.oracle.com" port="9810" ssl="true"
credentialAlias="obips" certificateVerificationDepth="1"
verifyPeers="true"/>
```

```
  </Hosts>
</JavaHostProxy>
```

4.4.18 Configure Oracle SOA Suite 10*g*

On the server where Oracle SOA Suite 10*g* has been deployed (machine 5), backup the `opmn.xml` file in the `$ORACLE_HOME/opmn/conf` directory.

Make the following change to the `opmn.xml` file. Locate the `<ias-component id="HTTP_Server">` tag and modify it to:

```
<ias-component id="HTTP_Server" status="disabled">
```

4.4.19 Configure Oracle HTTP Server

On the server where Oracle HTTP Server has been deployed (machine 5), backup the `httpd.conf`, `ssl.conf` and `mod_oc4j.conf` files in the `$ORACLE_HOME/ohs/conf` directory.

Make the following changes to the `ssl.conf` file:

Change the `SSLWallet` directive to the location of the wallet.

Change the `SSLCipherSuite` directive to **'3DES:-DH:-SSLv2'**.

Comment out the `Listen` directive in the `httpd.conf`:

```
Listen 7778
```

Add the following to the `mod_oc4j.conf` file within the `<IfModule mod_oc4j.c>` tag:

```
Oc4jMount /analytics ajp13://localhost:8888
Oc4jMount /analytics/* ajp13://localhost:8888
```

Backup the `opmn.xml` file in the `$ORACLE_HOME/opmn/conf` directory.

In the `opmn.xml` file, locate the `<ias-component id="HTTP_Server">` tag and change `value="ssl-disabled"` to `value="ssl-enabled"`:

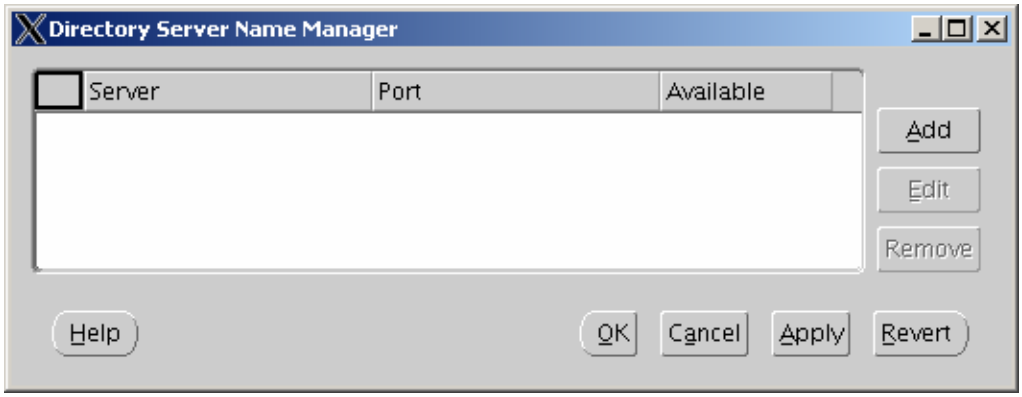
```
<data id="start-mod" value="ssl-enabled"/>
```

4.4.20 Configure Oracle Internet Directory

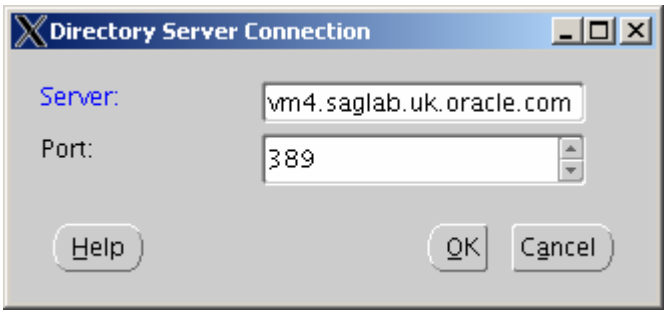
To configure SSL on the OID server an SSL configuration set must be created using Oracle Directory Manager. Issue the following commands to configure OID on machine 4:

```
export ORACLE_HOME=/space/oracle/product/10gAS/10g_OIM
export PATH=$ORACLE_HOME/bin:$PATH
oidadmin &
```

Click OK.

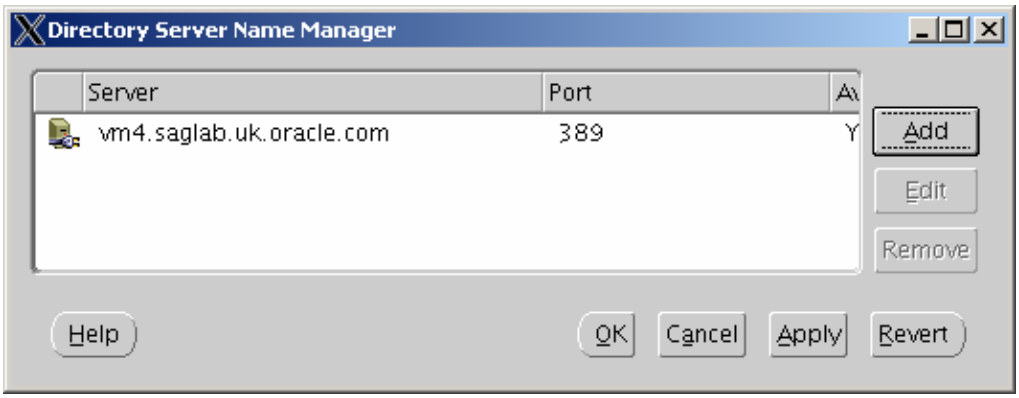


Click Add.

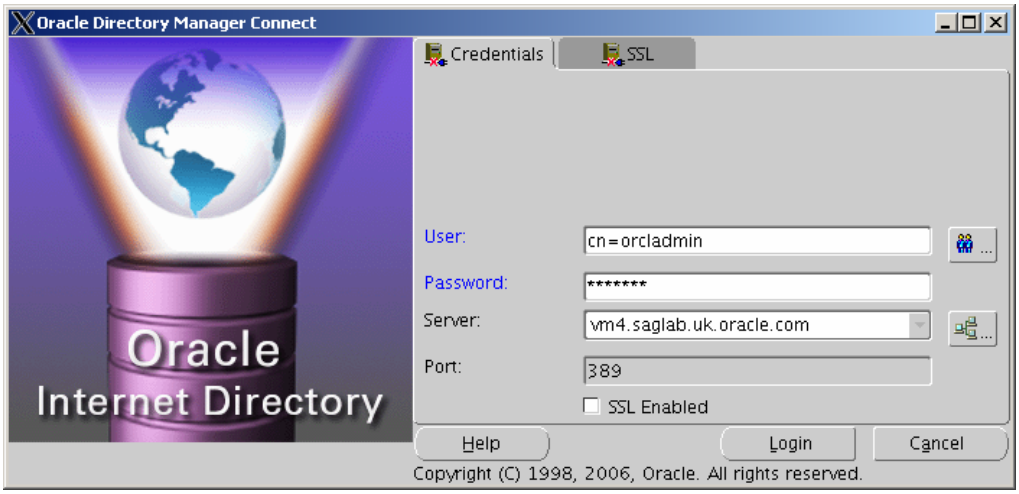


Enter the server name in the **'Server'** field.

Click OK.



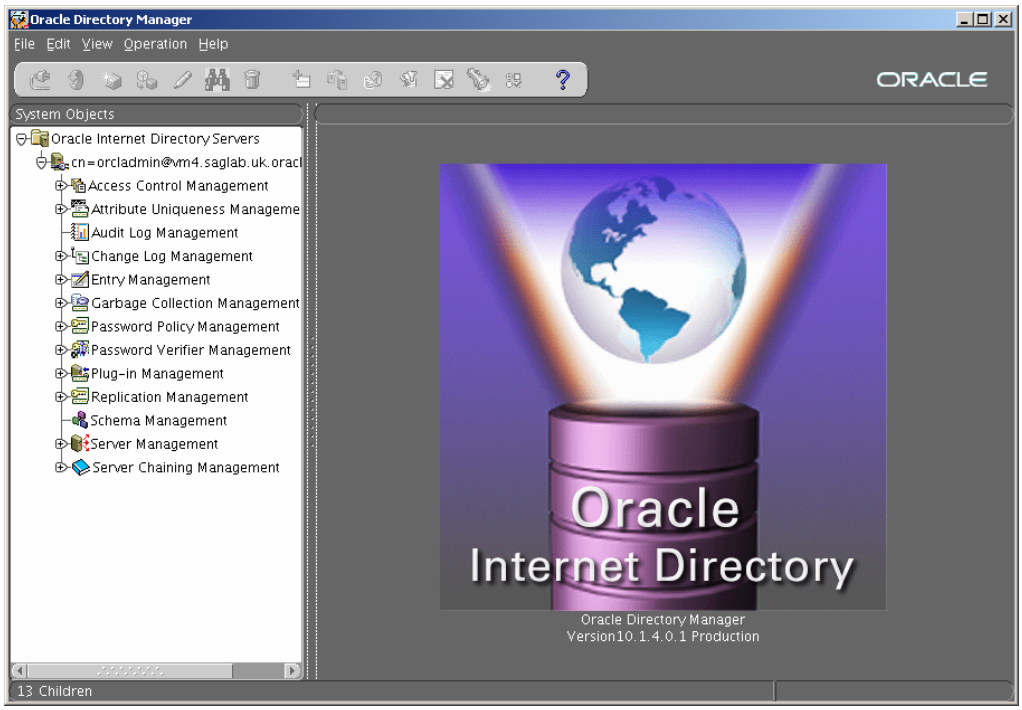
Click Apply and then click OK.



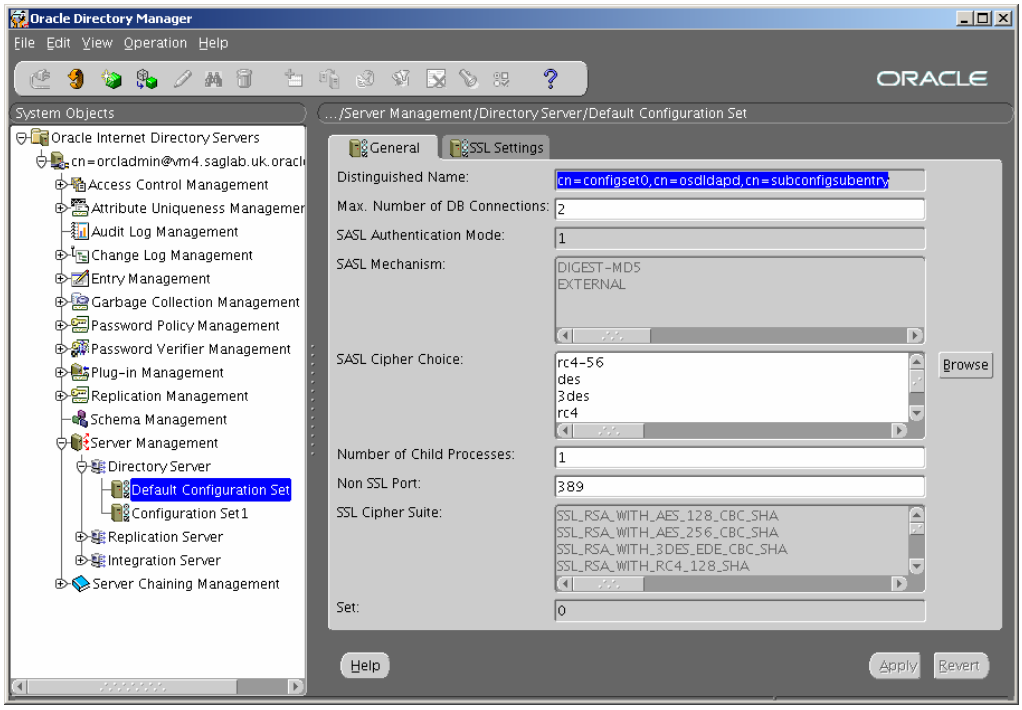
Enter **'cn=orcladmin'** in the **'User'** field.

Enter the password for the **'cn=orcladmin'** user in the **'Password'** field.

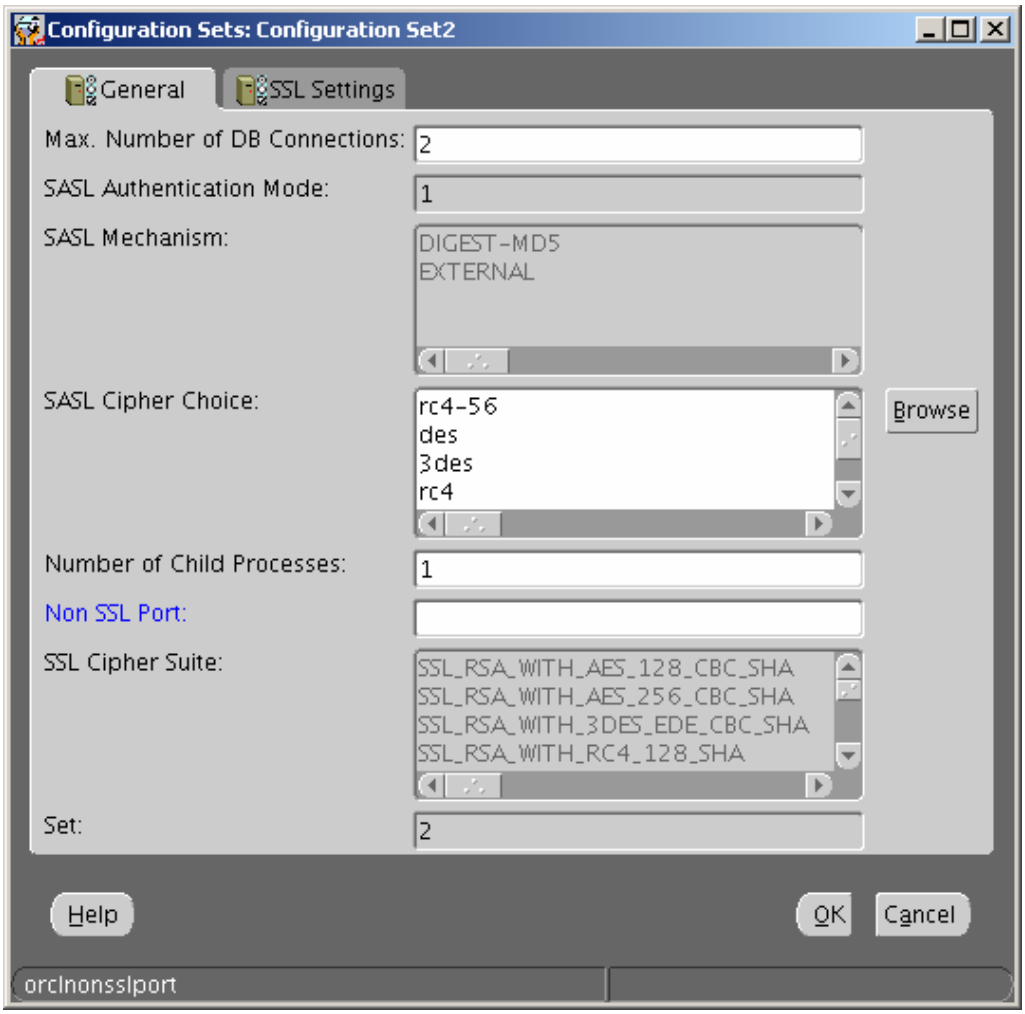
Click Login.



Expand the Server Management > Directory Server tree.

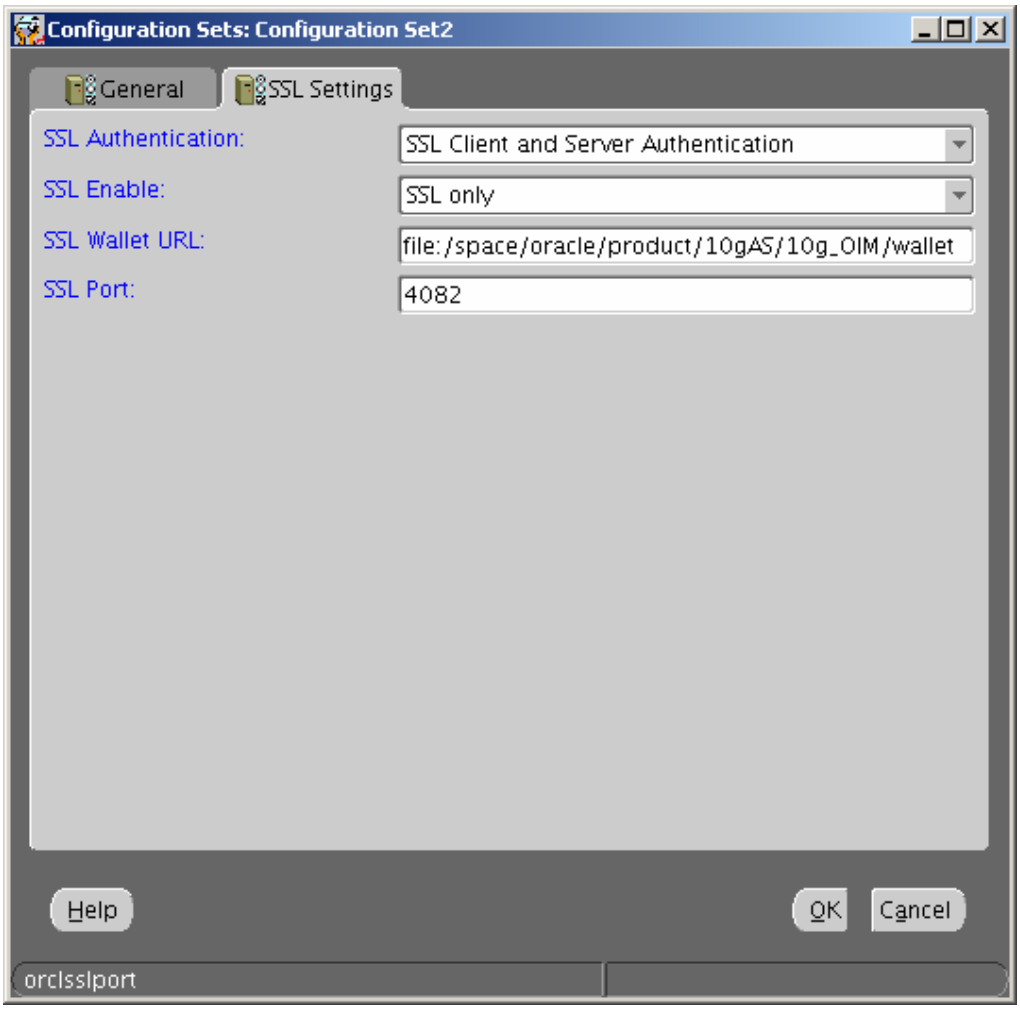


Right-click **'Default Configuration Set'** and select **'Create Like'**.



Remove **'389'** from the **'Non SSL Port'** field.

Click the **'SSL'** tab.



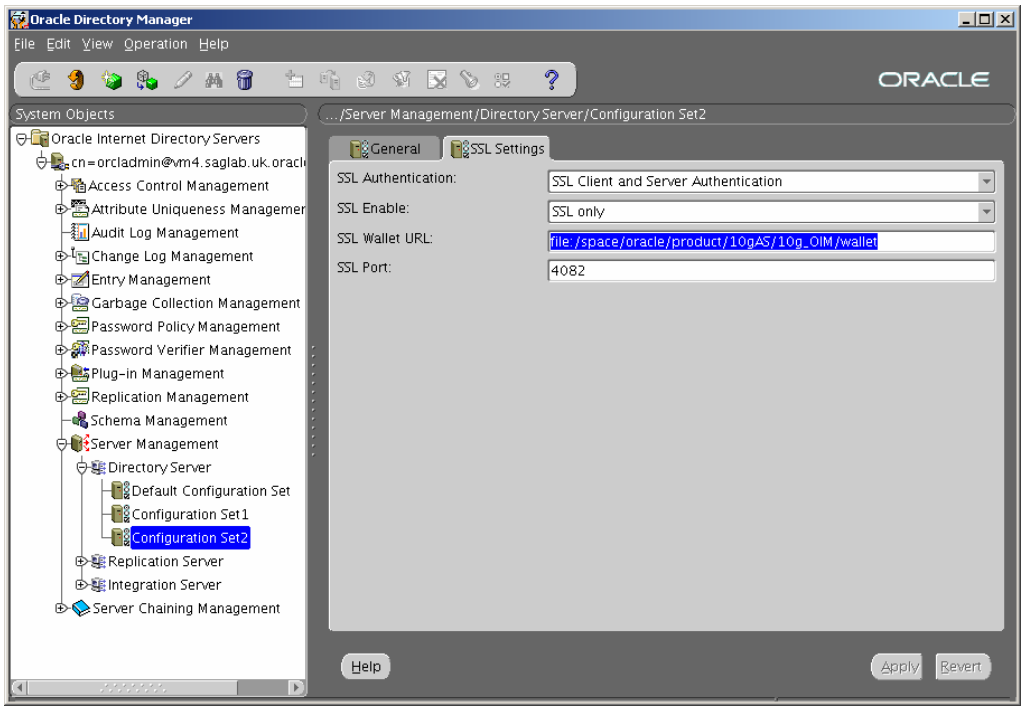
Select **'SSL Client and Server Authentication'** from the **'SSL Authentication'** select list.

Select **'SSL only'** from the **'SSL Enable'** select list.

Append the location of the SSL Wallet in the **'SSL Wallet URL'** field.

Enter **'4082'** in the **'SSL Port'** field.

Click OK.



Close Oracle Directory Manager.

Start a new OID process by issuing the following command:

```
oidctl connect=OID server=oidldapd instance=2 configset=2 start
```

Verify successful connection to OID using `ldapbind`:

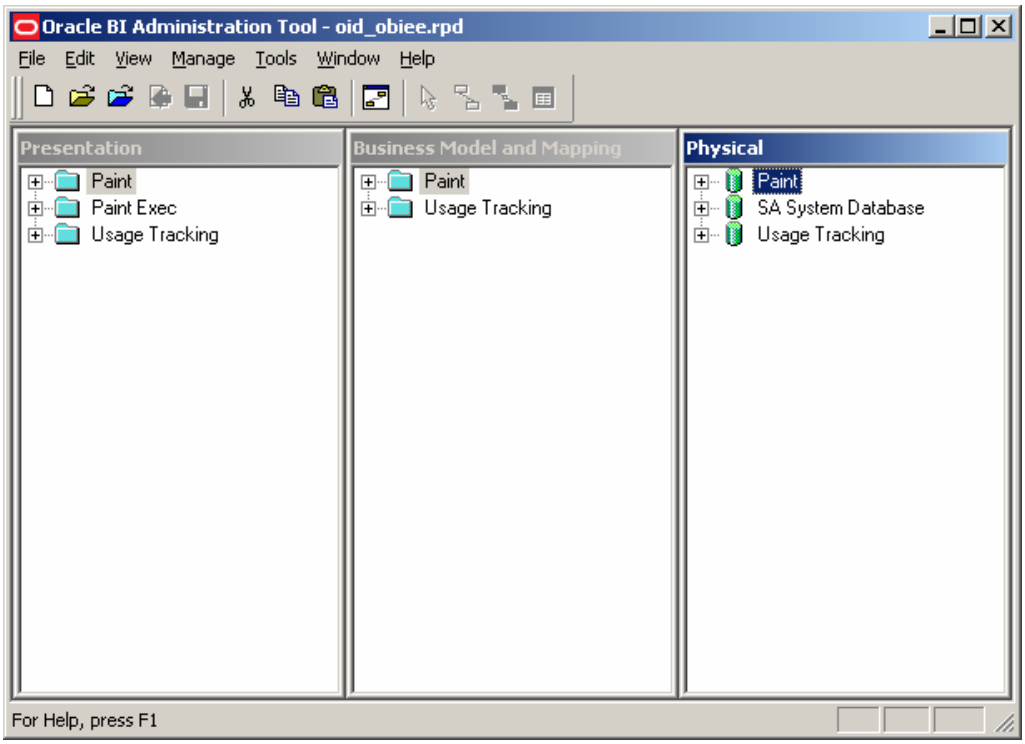
```
ldapbind -D cn=orcladmin -w oracle1 -U 3 -h localhost -p 4082 -
W file://space/oracle/product/10gAS/10g_OIM/wallet -P oracle
```

Where the arguments passed to `ldapbind` are:

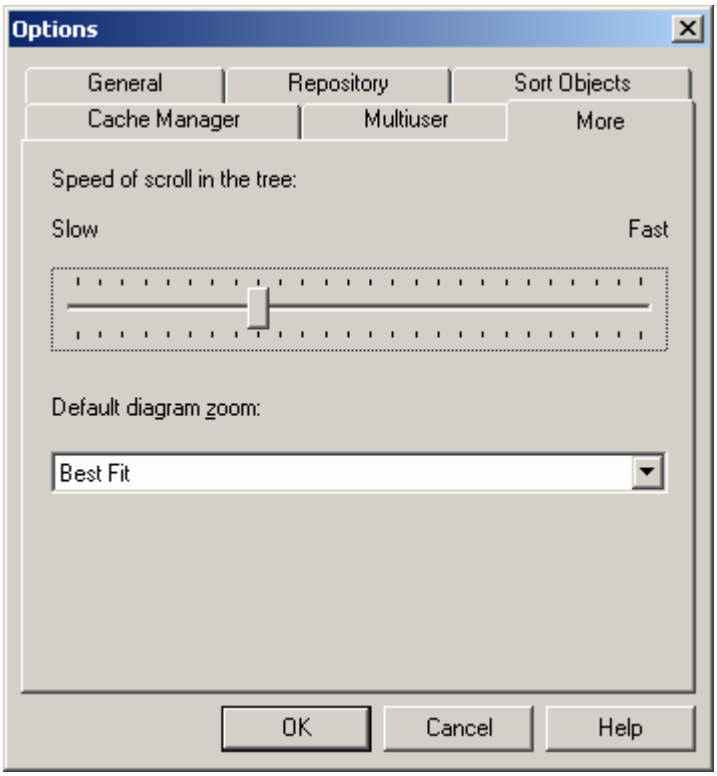
-D The OID user needed to bind to the directory.
-w The OID user password needed to bind to the directory.
-U The SSL authentication mode
-h The host name or IP address of the OID server
-p The port number used to connect to the OID server
-W The location of the wallet file containing the server's SSL certificates
-P The wallet password for the wallet specified in the -W argument

4.4.21 Configure OBIEE Repository

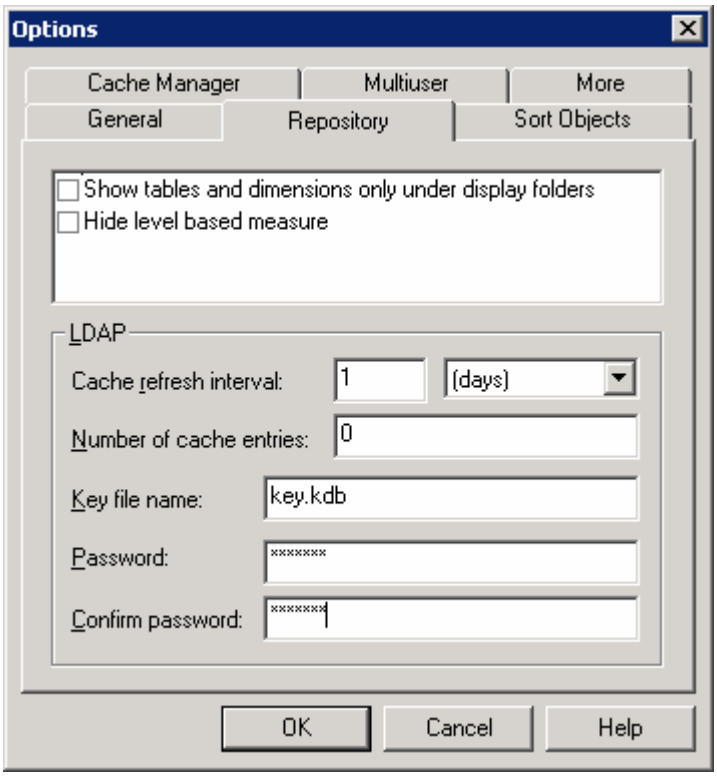
Open the `oid_obiee.rpd` repository file using the Administration Tool (machine 6) to configure SSL communication between the BI Server and OID.



Click Tools > Options



Click the **'Repository'** tab.

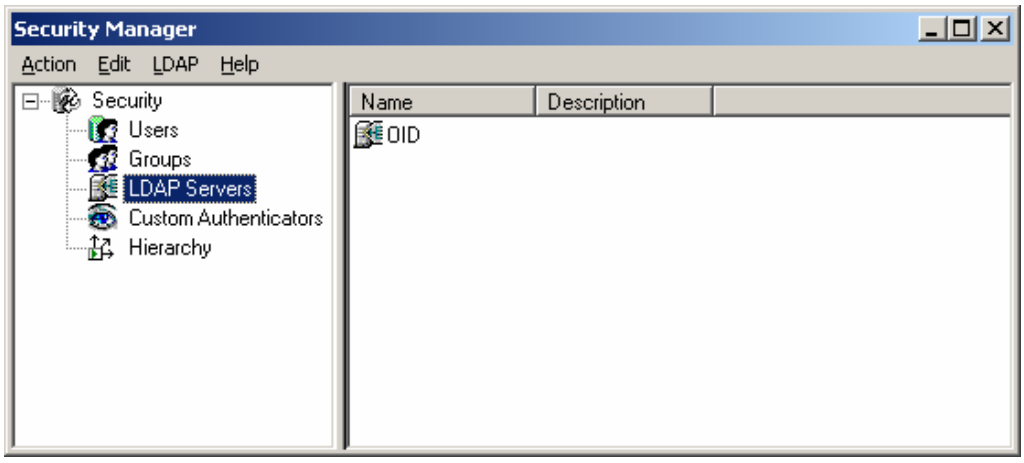


Enter the name of the key file in the **'Key file name'** field.

Enter the password to open the key file in the **'Password'** and the **'Confirm password'** fields.

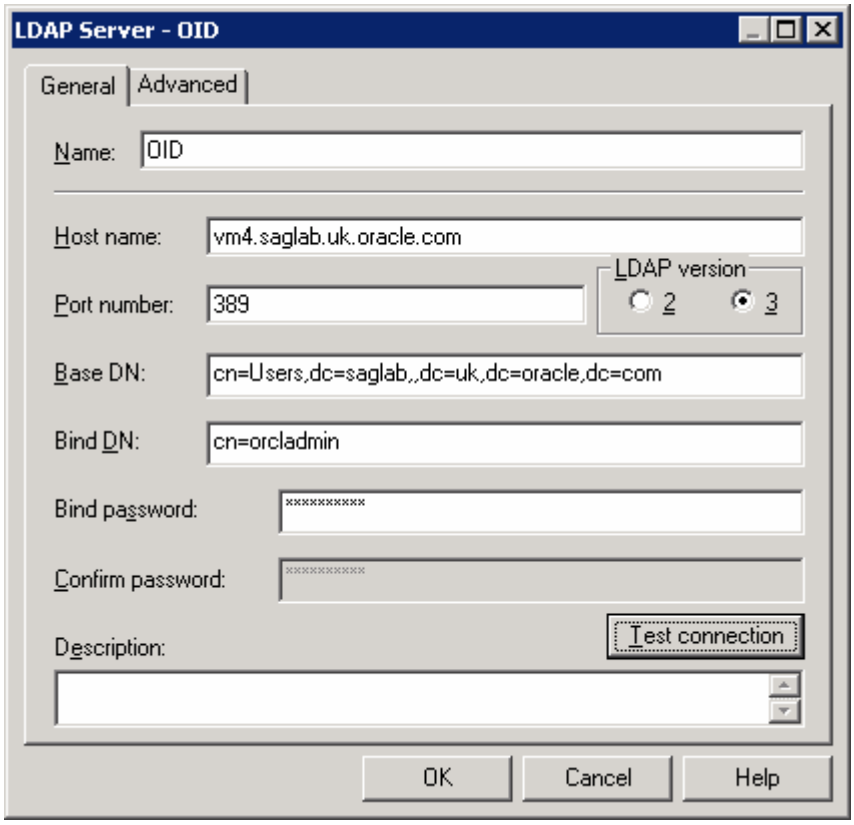
Click OK.

Click Manage > Security



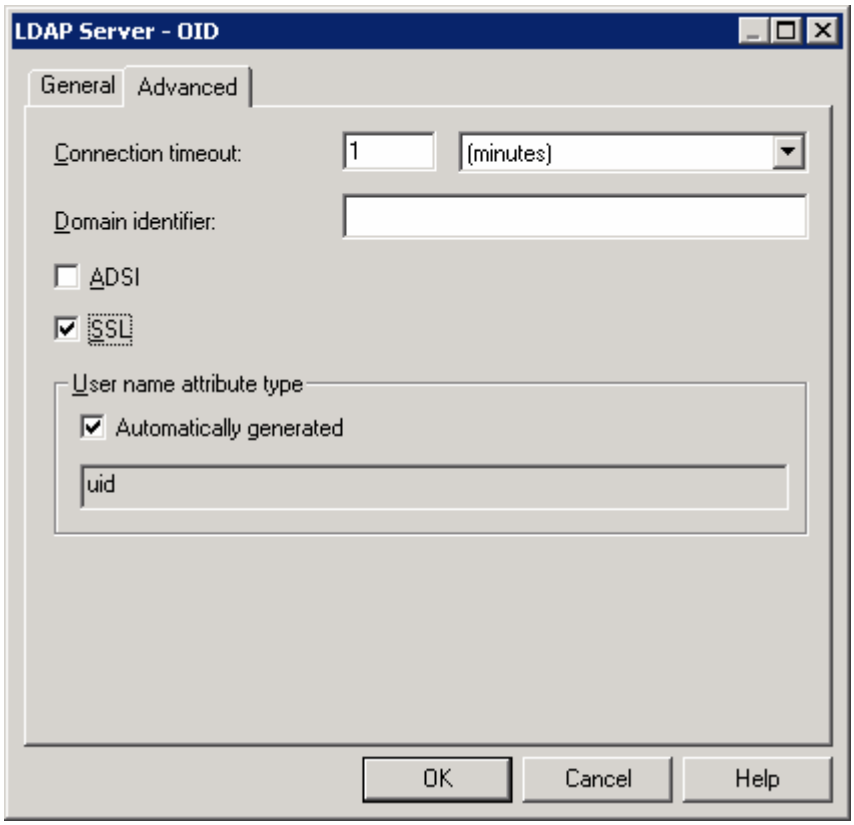
Click **'LDAP Servers'** in the left-hand pane.

Right-click **'OID'** and select **'Properties'**.



Enter **'4082'** in the **'Port number'** field.

Click the **'Advanced'** tab.



Tick the **'SSL'** check box.

Click OK. Close the Security Manager and save the repository.

4.4.22 Configure Oracle Database Server

To configure SSL on the database server the network configuration files, `sqlnet.ora` and `listener.ora`, must be edited. The files are located in the `$ORACLE_HOME/network/admin` directory.

Add the following entry to the `sqlnet.ora` and `listener.ora` files:

```
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = /space/oracle/product/10.2.0/db/wallet)
    )
  )
```

Add the following entries to the `sqlnet.ora` file:

```
SSL_CIPHER_SUITES = (SSL_RSA_WITH_3DES_EDE_CBC_SHA)
SSL_VERSION = 3.0
```

Modify the `LISTENER` entry in the `listener.ora` file from:

```
(ADDRESS       =       (PROTOCOL       =       TCP)(HOST       =
vm3.saglab.uk.oracle.com)(PORT = 1521))
```

To:

```
(ADDRESS       =       (PROTOCOL       =       TCPS)(HOST       =
vm3.saglab.uk.oracle.com)(PORT = 2484))
```

Modify the `SID_LIST_LISTENER` entry in the `listener.ora` file to include:

```
(SID_DESC =
  (GLOBAL_DBNAME = orcl.saglab.uk.oracle.com)
  (ORACLE_HOME = /space/oracle/product/10.2.0/db)
  (SID_NAME = orcl)
)
```

Restart the listener so that the new settings are picked up.

4.4.23 Configure Oracle Client

To configure SSL on the client the network configuration files, `sqlnet.ora` and `tnsnames.ora`, must be edited. The files are located in the client `$ORACLE_HOME/network/admin` directory on machines 1 and 2 and in the client `%ORACLE_HOME%\network\admin` directory on machine 6.

Perform the following configuration on machines 1, 2 and 6:

Add the following entry to the `tnsnames.ora` file. Create the file if it does not exist:

```
ORCL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCPS)(HOST = vm3.saglab.uk.oracle.com)(PORT =
2484))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl.saglab.uk.oracle.com)
    )
    (SECURITY=
```

```
      (SSL_SERVER_CERT_DN="CN=vm3.saglab.uk.oracle.com,   OU=BI,   O=Oracle,
L=Reading, ST=Berkshire, C=GB")
    )
  )
```

Perform the following configuration on machines 1 and 2:

Add the following entries to the `sqlnet.ora` file:

```
SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = TRUE
SSL_SERVER_DN_MATCH = Yes
SSL_CIPHER_SUITES = (SSL_RSA_WITH_3DES_EDE_CBC_SHA)

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = /space/oracle/product/10.2.0/client/wallet)
    )
  )
```

Perform the following configuration on machine 6:

Add the following entries to the `sqlnet.ora` file:

```
SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = TRUE
SSL_SERVER_DN_MATCH = Yes
SSL_CIPHER_SUITES = (SSL_RSA_WITH_3DES_EDE_CBC_SHA)

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = C:\oracle\product\10.2.0\client\wallet)
    )
  )
```

4.5 Presentation Services Logging

Auditing for Presentation Services is configured in the `logconfig.xml` file located in the `/space/oracle/oradata/OBIEE/web/config` directory.

Create a new `logconfig.xml` file on machines 1 and 2 with the following contents:

```
<?xml version="1.0" encoding="utf-8"?>
<!-- Siebel Analytics Web log config file -->

<Config>
<Default>
   <Writers>
      <Writer  implementation="CoutWriter"  name="Global  Output    Logger"
writerClassId="1"/>
      <Writer  implementation="FileLogWriter"  name="Global  File  Logger"
writerClassId="2"                              dir="{%SADATADIR%}/share/logs"
filePrefix="<machine>_saw.log" maxFileSizeKb="10000" filesN="10" />
      <Writer    implementation="EventLogWriter"    name="Event    Logger"
writerClassId="3"/>
      <Writer  implementation="FileLogWriter"  name="Security  File  Logger"
writerClassId="5"                              dir="{%SADATADIR%}/share/logs"
filePrefix="<machine>_sawsecurity.log" maxFileSizeKb="10000" filesN="10" />
      <Writer  implementation="FileLogWriter"  name="Catalog  File  Logger"
writerClassId="6"                              dir="{%SADATADIR%}/share/logs"
filePrefix="<machine>_sawcatalog.log" maxFileSizeKb="10000" filesN="10" />
      <Writer   implementation="FileLogWriter"   name="Catalog   ACLs   File
Logger"          writerClassId="7"          dir="{%SADATADIR%}/share/logs"
filePrefix="<machine>_sawcatalog.acls.log"            maxFileSizeKb="10000"
filesN="10" />
   </Writers>
   <WriterClassGroups>
      <WriterClassGroup name="All">1,2,3,4,5,6,7</WriterClassGroup>
      <WriterClassGroup name="File">1</WriterClassGroup>
      <WriterClassGroup name="Cout">2</WriterClassGroup>
      <WriterClassGroup name="EventLog">3</WriterClassGroup>
      <WriterClassGroup name="Crash">4</WriterClassGroup>
      <WriterClassGroup name="Security">5</WriterClassGroup>
      <WriterClassGroup name="Catalog">6</WriterClassGroup>
      <WriterClassGroup name="Catalog Security">7</WriterClassGroup>
   </WriterClassGroups>
   <Filters>
      <FilterRecord writerClassGroup="Cout" path = "saw" information="31"
warning="41" error="41" security="41"/>
      <FilterRecord writerClassGroup="File" path = "saw" information="31"
warning="100" error="100" security="41"/>
      <FilterRecord         writerClassGroup="File"         path         =
"saw.mktgsqlsubsystem.joblog"  information="41"  warning="100"  error="100"
security="41"/>
      <FilterRecord writerClassGroup="EventLog" path="saw" information="31"
warning="41" security="100"/>
      <FilterRecord writerClassGroup="Security" path="saw" information="0"
warning="0" security="100"/>
      <FilterRecord      writerClassGroup="Catalog"      path="saw.catalog"
information="0" warning="100" security="100"/>
      <FilterRecord           writerClassGroup="Catalog           Security"
path="saw.catalog.local.setItemACL"     information="100"     warning="100"
security="100"/>
   </Filters>
</Default>
</Config>
```

Replace the <machine> tag above with the hostname being configured (i.e. if configuring machine 1, vm1 would be entered).

Make the following changes to the `run-saw.sh` file located in the following directory:

```
/space/oracle/product/OBIEE/setup
```

Perform the following configuration on all machines where the Oracle BI Presentation Services has been deployed (machines 1 and 2).

Modify the line:

```
logfile="${SADATADIR}/web/log/sawserver.out.log"
```

To:

```
logfile="${SADATADIR}/share/logs/<machine>_sawserver.out.log"
```

Replace the <machine> tag above with the hostname being configured (i.e. if configuring machine 1, vm1 would be entered).

Modify the line:

```
echo "Please go to the '${SADATADIR}/web/log' directory for
Oracle BI Presentation Services log files."
```

To:

```
echo "Please go to the '${SADATADIR}/share/logs' directory for
Oracle BI Presentation Services log files."
```

Presentation Services log files will be created on machine 7.

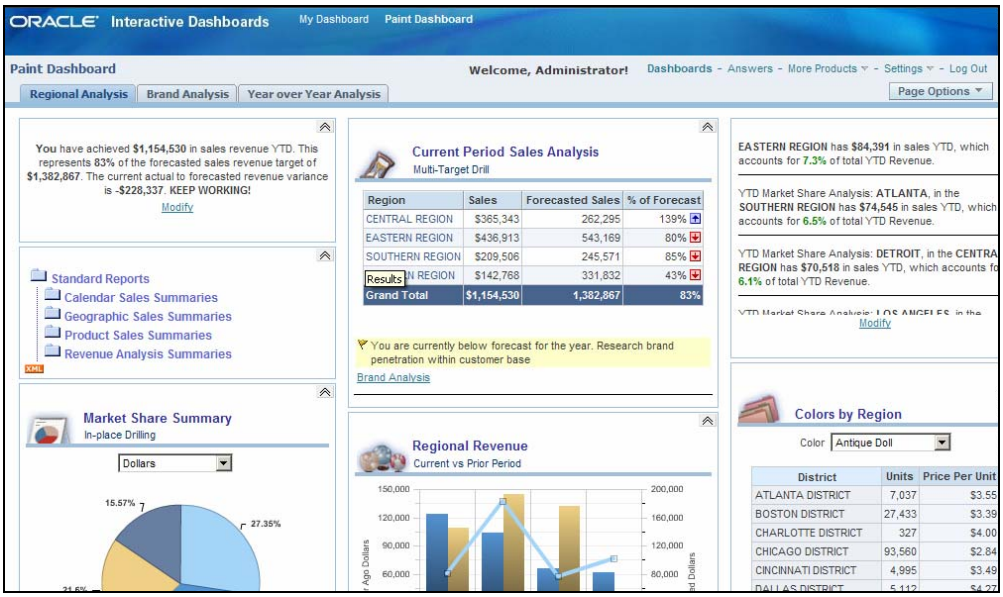
4.6 Presentation Catalog Configuration

4.6.1 Configuration

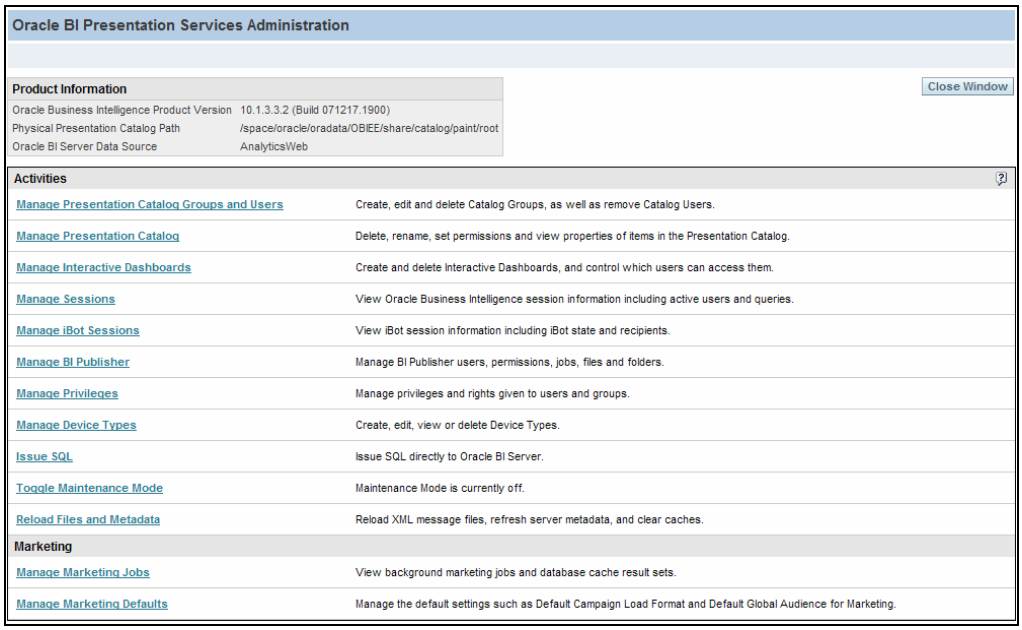
Start the TOE according to annex B and then login to Oracle Business Intelligence Enterprise Edition using the following URL:

https://vm5.saglab.uk.oracle.com:4444/analytics

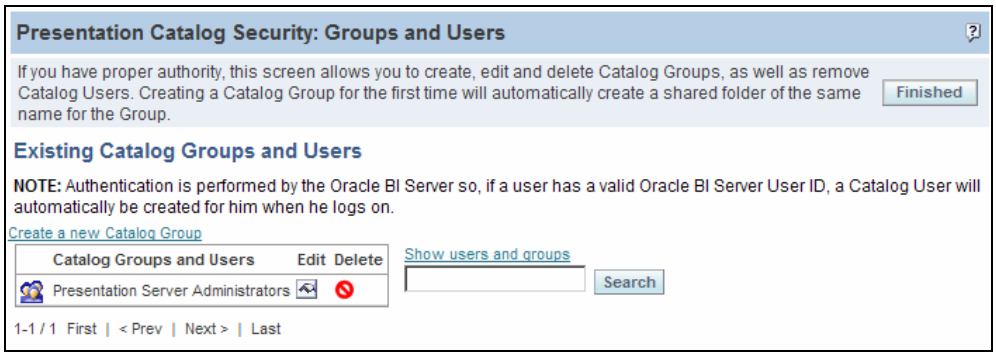
Enter User ID and Password. Click Log In.



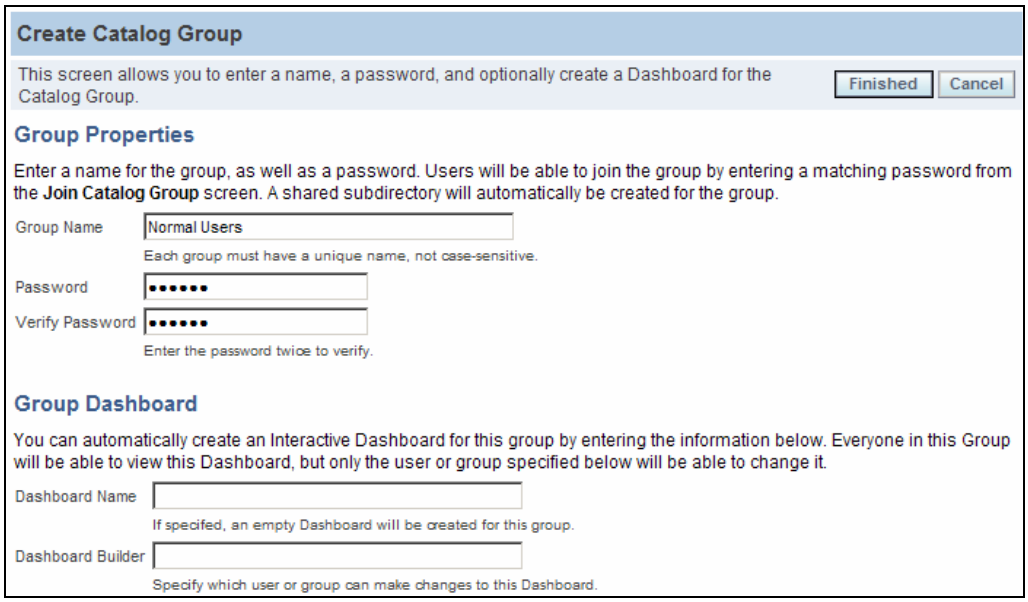
Click **Settings** > **Administration**



Click the **'Manage Presentation Catalog Groups and Users'** link.



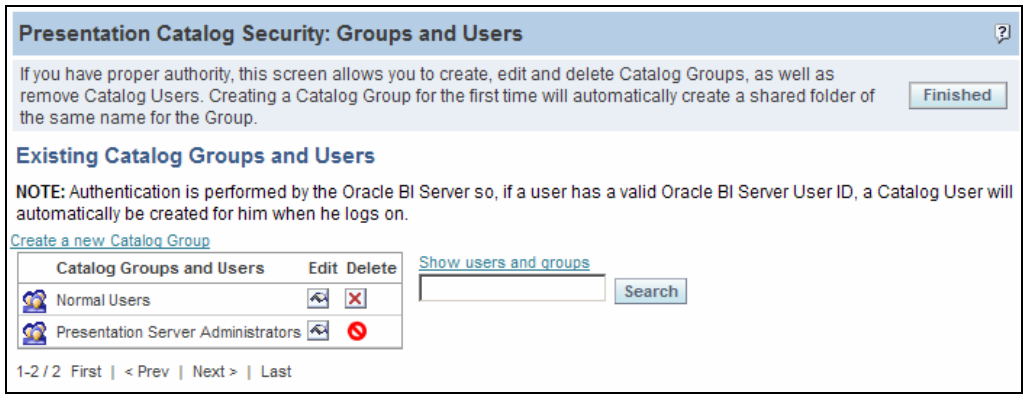
Click the **'Create a new Catalog Group'** link.



Enter **'Normal Users'** in the **'Group Name'** field.

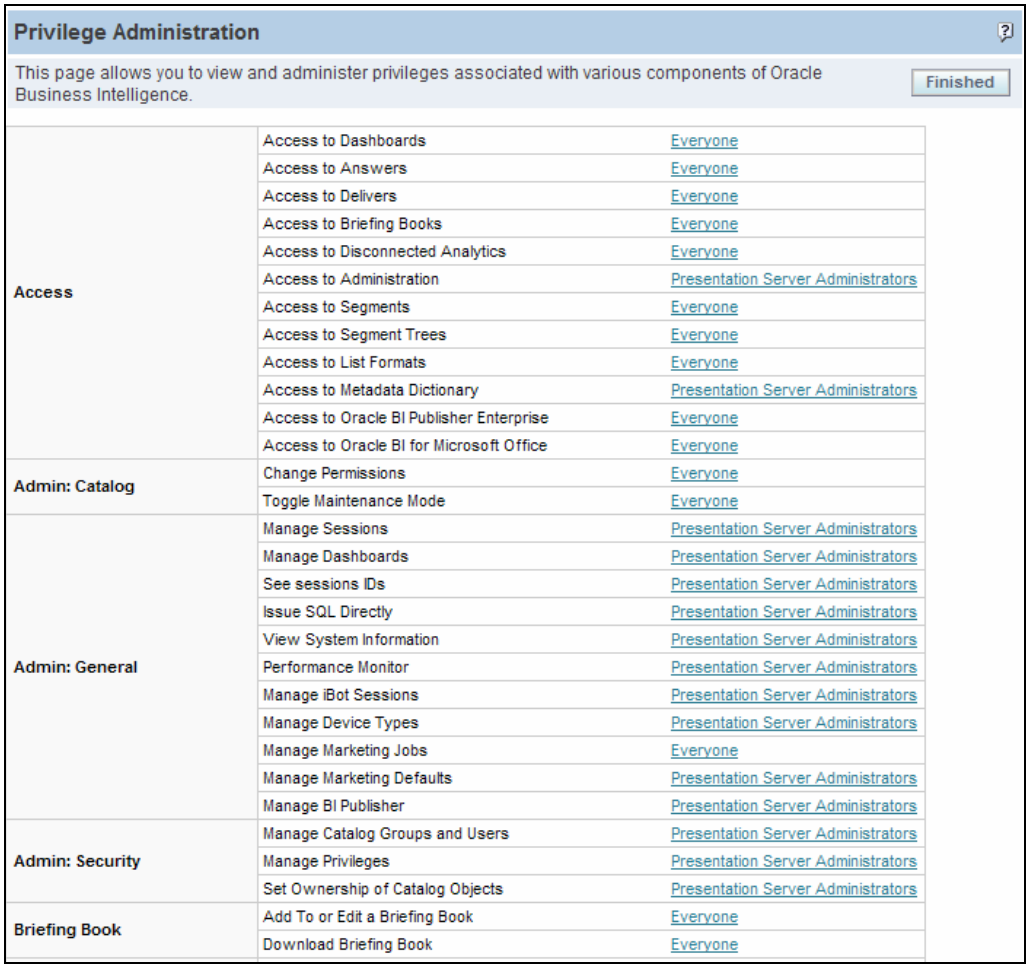
Enter a password for the group into the **'Password'** field.

Click the **'Finished'** button.



Click the **'Finished'** button.

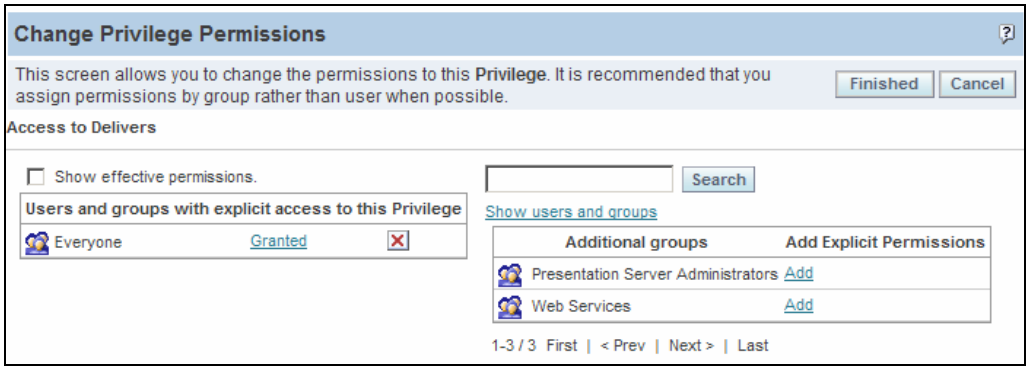
Click the **'Manage Privileges'** button.



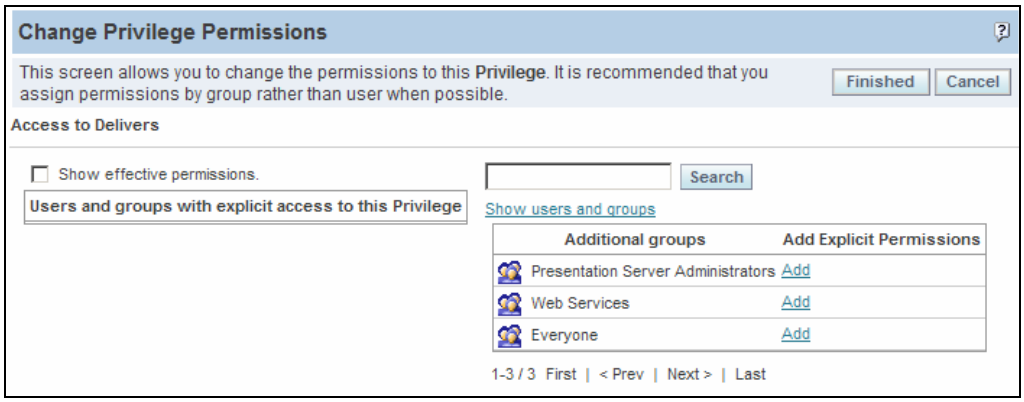
Access	Access to Dashboards	Everyone
	Access to Answers	Everyone
	Access to Delivers	Everyone
	Access to Briefing Books	Everyone
	Access to Disconnected Analytics	Everyone
	Access to Administration	Presentation Server Administrators
	Access to Segments	Everyone
	Access to Segment Trees	Everyone
	Access to List Formats	Everyone
	Access to Metadata Dictionary	Presentation Server Administrators
	Access to Oracle BI Publisher Enterprise	Everyone
	Access to Oracle BI for Microsoft Office	Everyone
Admin: Catalog	Change Permissions	Everyone
	Toggle Maintenance Mode	Everyone
Admin: General	Manage Sessions	Presentation Server Administrators
	Manage Dashboards	Presentation Server Administrators
	See sessions IDs	Presentation Server Administrators
	Issue SQL Directly	Presentation Server Administrators
	View System Information	Presentation Server Administrators
	Performance Monitor	Presentation Server Administrators
	Manage iBot Sessions	Presentation Server Administrators
	Manage Device Types	Presentation Server Administrators
	Manage Marketing Jobs	Everyone
	Manage Marketing Defaults	Presentation Server Administrators
	Manage BI Publisher	Presentation Server Administrators
Admin: Security	Manage Catalog Groups and Users	Presentation Server Administrators
	Manage Privileges	Presentation Server Administrators
	Set Ownership of Catalog Objects	Presentation Server Administrators
Briefing Book	Add To or Edit a Briefing Book	Everyone
	Download Briefing Book	Everyone

4.6.2 Revoke Privileges

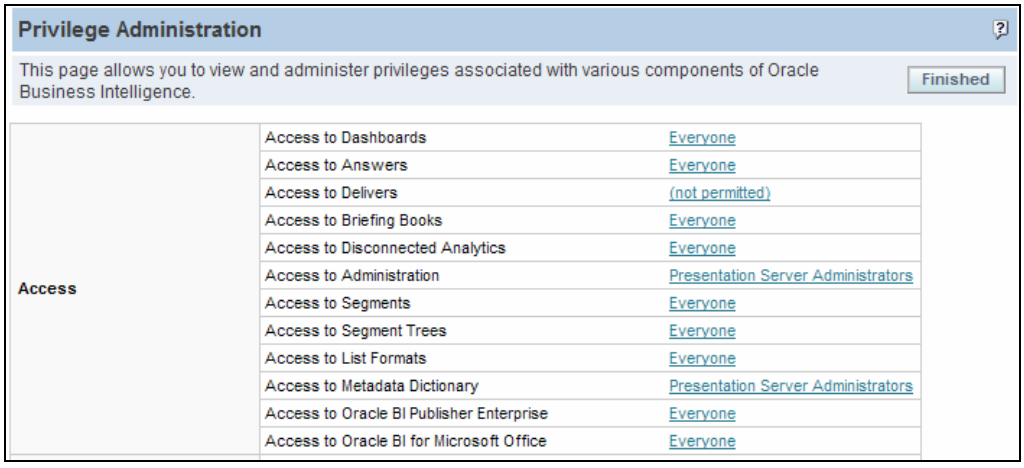
Revoke the **'Access to Dashboards'** privilege by clicking the **'Everyone'** hyperlink.



Click the ☒ button to revoke the privilege.



Click the **'Finished'** button.

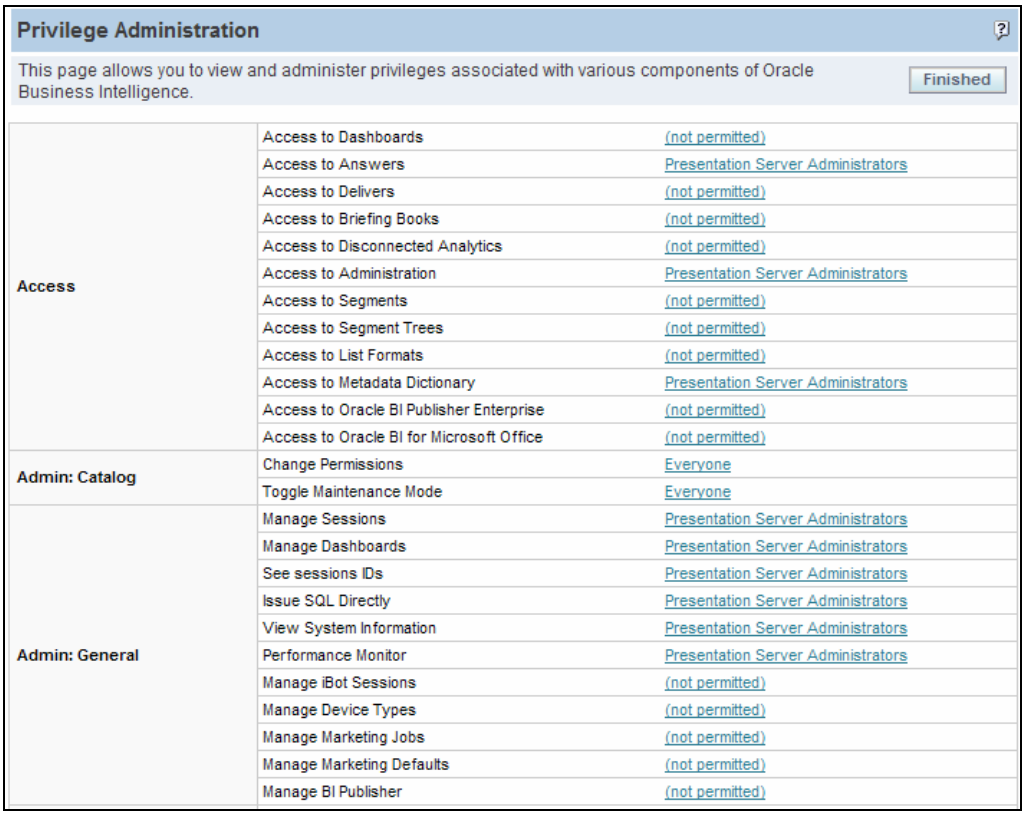


Set privileges according to the following table:

Access	Access to Dashboards	(not permitted)
	Access to Answers	Presentation Server Administrators
	Access to Delivers	(not permitted)
	Access to Briefing Books	(not permitted)
	Access to Disconnected Analytics	(not permitted)
	Access to Administration	Presentation Server Administrators
	Access to Segments	(not permitted)
	Access to Segment Trees	(not permitted)
	Access to List Formats	(not permitted)
	Access to Metadata Dictionary	Presentation Server Administrators
	Access to Oracle BI Publisher Enterprise	(not permitted)
	Access to Oracle BI for Microsoft Office	(not permitted)
Admin: Catalog	Change Permissions	Everyone
	Toggle Maintenance Mode	Everyone
Admin: General	Manage Sessions	Presentation Server Administrators
	Manage Dashboards	Presentation Server Administrators
	See sessions IDs	Presentation Server Administrators
	Issue SQL Directly	Presentation Server Administrators
	View System Information	Presentation Server Administrators
	Performance Monitor	Presentation Server Administrators
	Manage iBot Sessions	(not permitted)
	Manage Device Types	(not permitted)
	Manage Marketing Jobs	(not permitted)
	Manage Marketing Defaults	(not permitted)
	Manage BI Publisher	(not permitted)
Admin: Security	Manage Catalog Groups and Users	Presentation Server Administrators
	Manage Privileges	Presentation Server Administrators
	Set Ownership of Catalog Objects	Presentation Server Administrators
Briefing Book	Add To or Edit a Briefing Book	(not permitted)
	Download Briefing Book	(not permitted)
Catalog	Personal Storage (My Folders and My Dashboard)	Everyone
	Reload Metadata	Presentation Server Administrators
	See Hidden Items	Everyone
	Create Folders	Everyone
	Archive Catalog	Presentation Server Administrators
Dashboards	Save Selections	Everyone
	Assign Default Selections	Everyone
Formatting	Save System-Wide Column Formats	Presentation Server Administrators

My Account	Access to My Account	Everyone
	Change Preferences	Everyone
	Change Delivery Options	Everyone
Answers	Create Views	Everyone
	Create Prompts	Everyone
	Access Advanced Tab	Everyone
	Edit Column Formulas	Everyone
	Save Content with HTML Markup	Presentation Server Administrators
	Enter XML and Logical SQL	Everyone
	Edit Direct Database Requests	Presentation Server Administrators
	Create Advanced Filters and Set Operations	Everyone
	Save Filters	Everyone
	Execute Direct Database Requests	(not permitted)
Delivers	Retrieve Delivery Destinations for iBots (system call)	(not permitted)
	Create iBots	(not permitted)
	Publish iBots for Subscription	(not permitted)
	Deliver iBots to Specific or Dynamically Determined Users	(not permitted)
	Chain iBots	(not permitted)
	Chain iBots to Custom Scripts	(not permitted)
	See iBot Instance Errors	(not permitted)
	Modify Current Subscriptions for iBots	(not permitted)
Proxy	Act As Proxy	(not permitted)
RSS Feeds	Access to RSS Feeds	Everyone
Oracle BI Publisher Enterprise	Add BI Publisher Reports to Dashboard	(not permitted)
	View BI Publisher Reports	(not permitted)
	Schedule BI Publisher Reports	(not permitted)
	Send BI Publisher Reports	(not permitted)
	Build BI Publisher Reports	(not permitted)
	Analyze BI Publisher Reports	(not permitted)
List Formats	Create List Formats	Everyone
	Create Headers and Footers	Everyone
	Access Options Tab	Everyone
	Add/Remove List Format Columns	Presentation Server Administrators
Segmentation	Create Segments	(not permitted)
	Create Segment Trees	(not permitted)
	Create/Purge Saved Result Sets	(not permitted)
	Access Segment Advanced Options Tab	(not permitted)
	Access Segment Tree Advanced Options Tab	(not permitted)
	Change Target Levels within Segment Designer	(not permitted)
SOAP	Access SOAP	Normal Users, Presentation Server Administrators
Subject Area: "Paint Exec"	Access within Oracle BI Answers	Everyone
Subject Area: "Usage Tracking"	Access within Oracle BI Answers	Everyone
Subject Area: Paint	Access within Oracle BI Answers	Everyone

View Column Filter Prompt	Add/Edit Column Filter Prompt View	Everyone
View Column Selector	Add/Edit Column Selector View	Everyone
View Compound	Add/Edit Compound View	Everyone
View Filters	Add/Edit Filters View	Everyone
View Funnel Chart	Add/Edit Funnel Chart View	Everyone
View Gauge	Add/Edit Gauge View	Everyone
View Dashboard Prompt	Add/Edit Dashboard Prompt View	Everyone
View Static Text	Add/Edit Static Text View	Everyone
View Image	Add/Edit Image View	Everyone
View Legend	Add/Edit Legend View	Everyone
View Narrative	Add/Edit Narrative View	Everyone
View Nested Request	Add/Edit Nested Request View	Everyone
View No Results	Add/Edit No Results View	Everyone
View Pivot Table	Add/Edit Pivot Table View	Everyone
View Create Segment	Add/Edit Create Segment View	Everyone
View Logical SQL	Add/Edit Logical SQL View	Everyone
View Chart	Add/Edit Chart View	Everyone
View Table	Add/Edit Table View	Everyone
View Create Target List	Add/Edit Create Target List View	Everyone
View Ticker	Add/Edit Ticker View	Everyone
View Title	Add/Edit Title View	Everyone
View View Selector	Add/Edit View Selector View	Everyone
Write Back	Write Back to Database Manage Write Back	(not permitted) Presentation Server Administrators

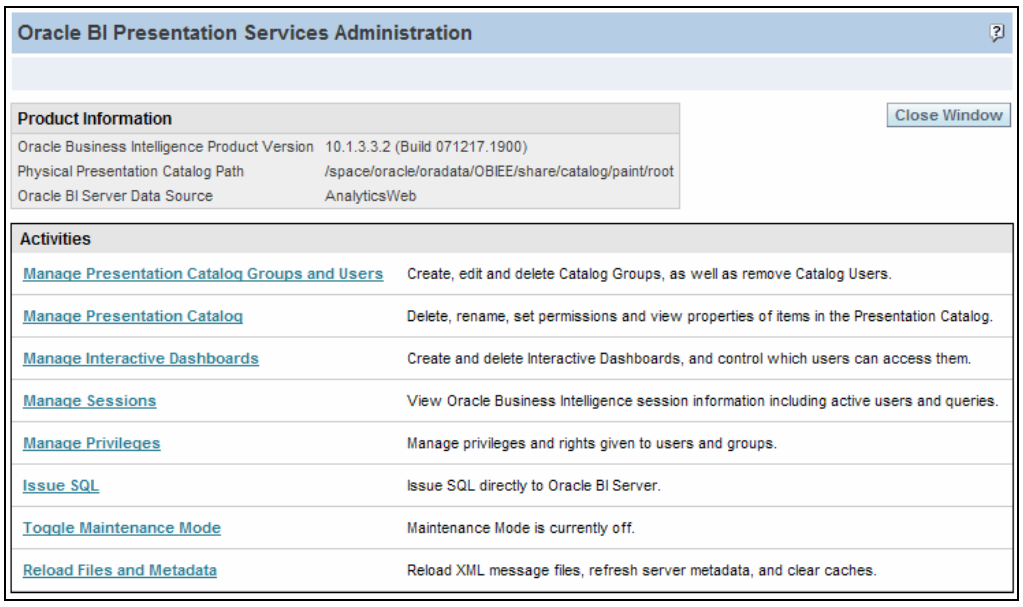


Privilege Administration

This page allows you to view and administer privileges associated with various components of Oracle Business Intelligence. Finished

Access	Access to Dashboards	(not permitted)
	Access to Answers	Presentation Server Administrators
	Access to Delivers	(not permitted)
	Access to Briefing Books	(not permitted)
	Access to Disconnected Analytics	(not permitted)
	Access to Administration	Presentation Server Administrators
	Access to Segments	(not permitted)
	Access to Segment Trees	(not permitted)
	Access to List Formats	(not permitted)
	Access to Metadata Dictionary	Presentation Server Administrators
	Access to Oracle BI Publisher Enterprise	(not permitted)
	Access to Oracle BI for Microsoft Office	(not permitted)
Admin: Catalog	Change Permissions	Everyone
	Toggle Maintenance Mode	Everyone
Admin: General	Manage Sessions	Presentation Server Administrators
	Manage Dashboards	Presentation Server Administrators
	See sessions IDs	Presentation Server Administrators
	Issue SQL Directly	Presentation Server Administrators
	View System Information	Presentation Server Administrators
	Performance Monitor	Presentation Server Administrators
	Manage iBot Sessions	(not permitted)
	Manage Device Types	(not permitted)
	Manage Marketing Jobs	(not permitted)
	Manage Marketing Defaults	(not permitted)
	Manage BI Publisher	(not permitted)

Click the **'Finished'** button when done.



Oracle BI Presentation Services Administration

Close Window

Product Information	
Oracle Business Intelligence Product Version	10.1.3.3.2 (Build 071217.1900)
Physical Presentation Catalog Path	/space/oracle/oradata/OBIEE/share/catalog/paint/root
Oracle BI Server Data Source	AnalyticsWeb

Activities	
Manage Presentation Catalog Groups and Users	Create, edit and delete Catalog Groups, as well as remove Catalog Users.
Manage Presentation Catalog	Delete, rename, set permissions and view properties of items in the Presentation Catalog.
Manage Interactive Dashboards	Create and delete Interactive Dashboards, and control which users can access them.
Manage Sessions	View Oracle Business Intelligence session information including active users and queries.
Manage Privileges	Manage privileges and rights given to users and groups.
Issue SQL	Issue SQL directly to Oracle BI Server.
Toggle Maintenance Mode	Maintenance Mode is currently off.
Reload Files and Metadata	Reload XML message files, refresh server metadata, and clear caches.

Click the **'Close Window'** button.

The changes will take effect immediately.

The following URL must be invoked to access BI Answers:

https://vm5.saglab.uk.oracle.com:4444/analytics/saw.dll?Answers

If the default URL is used when logging into Presentation Services, after successful authentication, BI Interactive Dashboards are displayed.

BI Interactive Dashboards are out of scope in the evaluated configuration and therefore access is prohibited, and the URL above must be used to access BI Answers.

4.7 TOE Start Procedure

Refer to Annex B.

4.8 Firewall Configuration

4.8.1 Machine 1

As the `root` user, issue the following command to create the `iptables` configuration file:

```
vi /etc/sysconfig/iptables
```

Insert the following entries in the `iptables` configuration file:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 9700 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 9701 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 9703 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 9706 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 9710 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 9810 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 5> -m state --state NEW -m tcp -p tcp
--dport 9710 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 6> -m state --state NEW -m tcp -p tcp
--dport 9703 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 6> -m state --state NEW -m tcp -p tcp
--dport 9706 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Start the firewall using the following command:

```
/sbin/service iptables start
```

4.8.2 Machine 2

As the `root` user, issue the following command to create the `iptables` configuration file:

```
vi /etc/sysconfig/iptables
```

Insert the following entries in the `iptables` configuration file:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 9700 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 9701 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 9703 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 9706 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 9710 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 9810 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 5> -m state --state NEW -m tcp -p tcp
--dport 9710 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 6> -m state --state NEW -m tcp -p tcp
--dport 9703 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 6> -m state --state NEW -m tcp -p tcp
--dport 9706 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Start the firewall using the following command:

```
/sbin/service iptables start
```

4.8.3 Machine 3

As the `root` user, issue the following command to create the `iptables` configuration file:

```
vi /etc/sysconfig/iptables
```

Insert the following entries in the `iptables` configuration file:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 2484 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 2484 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Start the firewall using the following command:

```
/sbin/service iptables start
```

4.8.4 Machine 4

As the `root` user, issue the following command to create the `iptables` configuration file:

```
vi /etc/sysconfig/iptables
```

Insert the following entries in the `iptables` configuration file:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 4082 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 4082 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Restart the firewall using the following command:

```
/sbin/service iptables restart
```

4.8.5 Machine 5

As the `root` user, issue the following command to create the `iptables` configuration file:

```
vi /etc/sysconfig/iptables
```

Insert the following entries in the `iptables` configuration file:

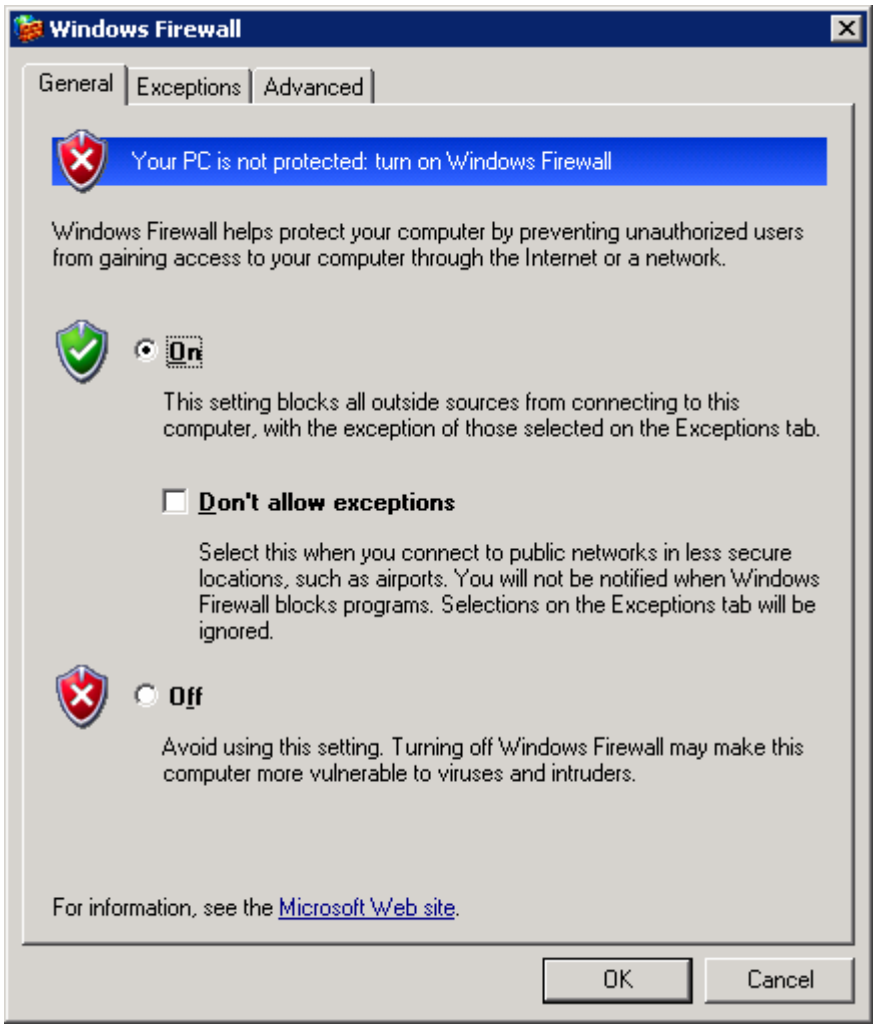
```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 4444 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Start the firewall using the following command:

```
/sbin/service iptables start
```

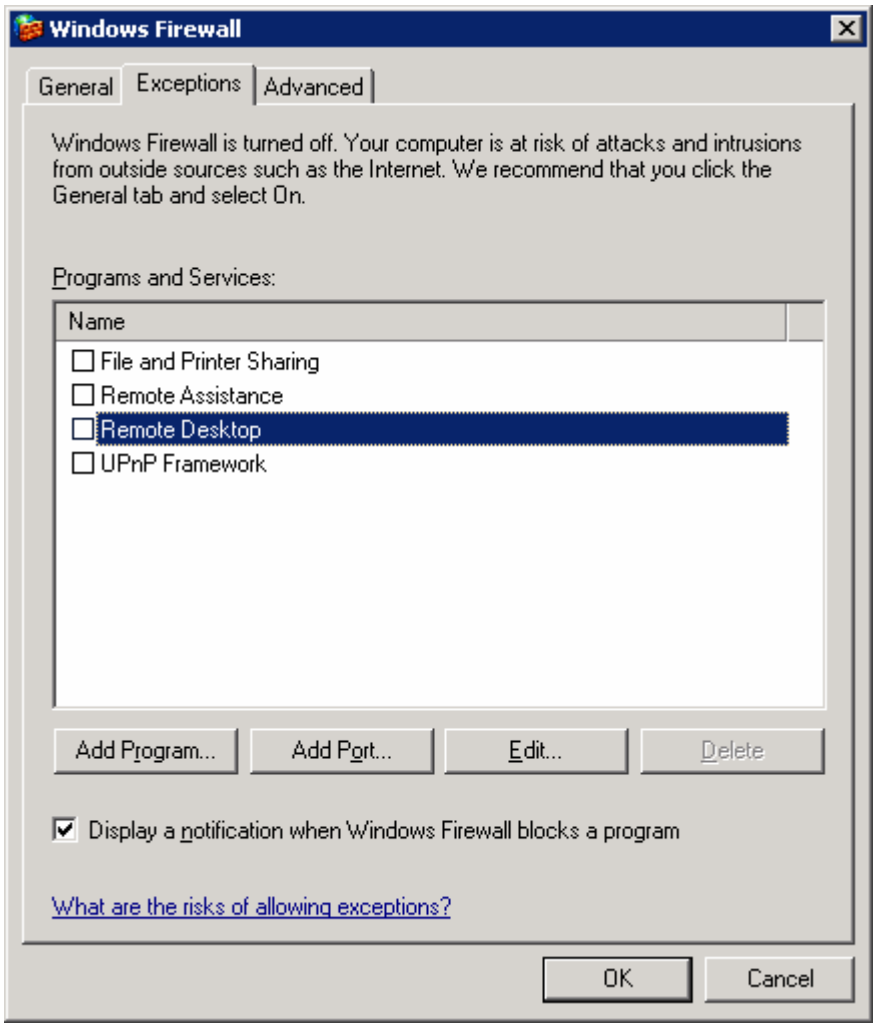
4.8.6 Machine 6

Navigate to Start > Settings > Control Panel and double-click on the Windows Firewall link.



Click the **'On'** radio button.

Click the Exceptions tab.



Clear the tick in the **'File and Printer Sharing'**, **'Remote Assistance'** and **'Remote Desktop'** Programs and Services.

Click OK.

4.8.7 Machine 7

As the `root` user, issue the following command to create the `iptables` configuration file:

```
vi /etc/sysconfig/iptables
```

Insert the following entries in the `iptables` configuration file:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m udp -p udp
--dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m udp -p udp
--dport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 2050 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m udp -p udp
--dport 2050 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 2051 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m udp -p udp
--dport 2051 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m tcp -p tcp
--dport 2052 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 1> -m state --state NEW -m udp -p udp
--dport 2052 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m udp -p udp
--dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m udp -p udp
--dport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 2050 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m udp -p udp
--dport 2050 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 2051 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m udp -p udp
--dport 2051 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m tcp -p tcp
--dport 2052 -j ACCEPT
-A RH-Firewall-1-INPUT -s <IP machine 2> -m state --state NEW -m udp -p udp
--dport 2052 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Start the firewall using the following command:

```
/sbin/service iptables start
```

4.9 User Administration

Users are administered within the TOE via either Oracle Internet Directory or Oracle Database Server depending on how the Oracle BI Server Repository has been configured (refer to section 4.1.10 for details).

4.9.1 Oracle Internet Directory

Users can be created using the following LDIF file:

```
dn: cn=<Username>,cn=Users,dc=saglab,dc=uk,dc=oracle,dc=com
cn: <Username>
sn: <Username>
objectclass: top
objectclass: person
objectclass: inetorgperson
objectclass: organizationalPerson
objectclass: orcluser
objectclass: orcluserv2
userpassword: <Password>
departmentnumber: <Group 1>, <Group 2>
```

The parameters in chevrons should be replaced with the following values:

<Username> The desired username

<Password> The password associated with <Username>

<Group n> The Presentation Catalog Group, defined in section 4.6.1, that the user should have access to – if the user requires access to multiple groups they should be entered comma-delimited

4.9.2 Oracle Database Server

Users can be created using the following SQL:

```
sqlplus / as sysdba

create <Username> identified by <Password>;

grant create session to <Username>;

insert    into    sa.sa_user_group    values    ('<Group    1>,
upper('<Username>'));
insert    into    sa.sa_user_group    values    ('<Group    2>,
upper('<Username>'));

commit;
```

The parameters in chevrons should be replaced with the following values:

<Username> The desired username

<Password> The password associated with <Username>

<Group n> The Presentation Catalog Group, defined in section 4.6.1, that the user should have access to – if the user requires access to multiple groups, multiple insert statements should be used - one per group access required

Annex A TOE Components

A.1 Oracle Application Server 10*g* Release 3 (10.1.3.1.0) Components

Agent Required Support Files 10.1.0.2.0
Agent Required Support Files Patch 10.1.0.5.0
Apache Module for Oracle Distributed Authoring and Versioning 10.1.2.1.0
Assistant Common Files 10.1.0.2.0
Assistant Common Files Patch 10.1.0.5.0
Bali Share 1.1.18.0.0
DataDirect Connect JDBC Drivers 10.1.2.0.1
DBJAVA Required Support Files 10.1.0.2.0
DBJAVA Required Support Files Patch 10.1.0.5.0
Documentation Required Support Files 10.1.0.3.0
Enterprise Manager Minimal Integration 10.1.0.2.0 Beta
Enterprise Manager plugin Common Files 10.1.0.2.0 Beta
Enterprise Manager plugin Common Files 10.1.0.5.0
Extended Windowing Toolkit 3.3.18.0.0 Beta
HTTP Server Files 1.3.31.0.0
Identity Management Required Support Files 10.1.4.0.1
Installation Common Files 10.1.0.3.0
Installation Common Files Patch 10.1.0.5.0
Installer SDK Component 10.1.0.5.0
Java Runtime Environment 1.4.2.0.4
JDBC Common Files 10.1.0.2.0
JDBC Common Files Patch 10.1.0.5.0
JDBC/OCI Common Files 10.1.0.2.0
JDBC/OCI Common Files for Instant Client 10.1.0.2.0
JDBC/OCI Common Files for Instant Client Patch 10.1.0.5.0
JDBC/OCI Common Files Patch 10.1.0.5.0
LDAP Required Support Files 10.1.4.0.1
Netca Patch 10.1.0.5.0
Oracle ADF 10.1.3.1.0
Oracle Apache Modules 10.1.3.0.0
Oracle Application Server Guard 10.1.3.1.0
Oracle Application Server Guard Client 10.1.3.1.0
Oracle Application Server Guard Common 10.1.3.1.0
Oracle Application Server Guard Server 10.1.3.1.0
Oracle Application Server High availability components (BR, AFC, DR) 10.1.3.0.0
Oracle Application Server SOA Suite 10.1.3.1.0
Oracle ASkernel Common 10.1.3.0.0
Oracle Business Rules 10.1.3.0.0 Development
Oracle Client Required Support Files 10.1.0.2.0
Oracle Client Required Support Files Patch 10.1.0.5.0
Oracle Code Editor 1.2.1.0.0I

Oracle Core Required Support Files 10.1.0.2.0
Oracle Core Required Support Files 10.1.0.5.0
Oracle Display Fonts 10.1.2.0.0
Oracle Dynamic Monitoring Service 10.1.3.1.0
Oracle Enterprise Manager Application Server Control 10.1.3.0.0
Oracle Enterprise Manager Change IP 10.1.3.0.0
Oracle Extended Windowing Toolkit 3.4.43.0.0
Oracle Globalization Support 10.1.0.2.0
Oracle Globalization Support Patch 10.1.0.5.0
Oracle Help For Java 4.2.9.0.0
Oracle HTTP Server 10.1.3.0.0
Oracle iappcore 10.1.3.0.0
Oracle Ice Browser 5.2.3.6.0
Oracle interMedia Java Client 10.1.0.2.0
Oracle interMedia Java Client Patch 10.1.0.5.0
Oracle Java Object Cache 10.1.3.0.0
Oracle JDBC Development Drivers 10.1.0.2.0
Oracle JDBC Development Drivers for Instant Client 10.1.0.2.0
Oracle JDBC Development Drivers for Instant Client Patch 10.1.0.5.0
Oracle JDBC Development Drivers Patch 10.1.0.5.0
Oracle JDBC Thin Driver for JDK 1.4 10.1.0.2.0
Oracle JDBC Thin Driver for JDK 1.4 10.1.0.5.0
Oracle JDBC Thin Driver for JDK 1.4 for Instant Client 10.1.0.2.0
Oracle JDBC Thin Driver for JDK 1.4 for Instant Client Patch 10.1.0.5.0
Oracle JFC Extended Windowing Toolkit 4.2.36.0.0
Oracle Locale Builder 10.1.0.2.0
Oracle Locale Builder Patch 10.1.0.5.0
Oracle Mod PL/SQL Gateway 10.1.3.0.0
Oracle Net 10.1.0.2.0
Oracle Net Configuration Assistant 10.1.0.2.0
Oracle Net Manager 10.1.0.2.0
Oracle Net Manager Patch 10.1.0.5.0
Oracle Net Patch 10.1.0.5.0
Oracle Net Required Support Files 10.1.0.2.0
Oracle Net Required Support Files Patch 10.1.0.5.0
Oracle Notification Service 10.1.3.1.0
Oracle OC4J Module 10.1.3.0.0
Oracle One-Off Patch Installer 10.1.0.5.0
Oracle Process Management Notification 10.1.3.1.0
Oracle Security Developer Tools 10.1.4.0.1
Oracle TopLink Runtime 10.1.3.1.0
Oracle UIX 2.2.20.0.0
Oracle Universal Installer 10.1.0.5.0
Oracle Wallet Manager 10.1.0.2.0
Oracle Wallet Manager Patch 10.1.0.5.0
Oracle XML Query Service 10.1.3.0.0
Oracle XML SQL Utility 10.1.3.1.0
Oracle10g Real Application Clusters Common Files 10.1.0.2.0

Oracle10g Real Application Clusters Common Files Patch 10.1.0.5.0
OracleAS J2EE 10.1.3.0.0
OracleAS Port Tunnel 10.1.3.0.0
OracleAS Welcome Pages 10.1.3.1.0
Parser Generator Required Support Files 10.1.0.2.0
Parser Generator Required Support Files Patch 10.1.0.5.0
Perl Interpreter 5.8.3.0.5
PL/SQL Required Support Files 10.1.0.2.0
PL/SQL Required Support Files 10.1.0.5.0
Platform Required Support Files 10.1.0.2.0
Platform Required Support Files Patch 10.1.0.5.0
Precompiler Required Support Files 10.1.0.2.0
Precompiler Required Support Files Patch 10.1.0.5.0
RDBMS Required Support Files 10.1.0.2.0
RDBMS Required Support Files Patch 10.1.0.5.0
regexp 2.1.9.0.0
Required Support Files 10.1.0.2.0
Secure Socket Layer 10.1.0.2.0
Secure Socket Layer 10.1.0.2.0
Secure Socket Layer Patch 10.1.0.5.0
SQL*Plus 10.1.0.2.0
SQL*Plus 10.1.0.5.0
SQL*Plus Required Support Files 10.1.0.2.0
SQL*Plus Required Support Files Patch 10.1.0.5.0
SSL Required Support Files 10.1.0.2.0
SSL Required Support Files for InstantClient 10.1.0.2.0
SSL Required Support Files for InstantClient Patch 10.1.0.5.0
SSL Required Support Files Patch 10.1.0.5.0
Sun JDK 1.5.0.0.6
XDK Required Support Files 10.1.3.1.0
XML Parser for Java 10.1.3.1.0

A.2 Oracle Client 10*g* Release 2 (10.2.0.3.0) Components

Agent Required Support Files 10.2.0.1.0
Agent Required Support Files Patch 10.2.0.3.0
Assistant Common Files 10.2.0.1.0
Assistant Common Files Patch 10.2.0.3.0
Bali Share 1.1.18.0.0
Buildtools Common Files 10.2.0.1.0
DBJAVA Required Support Files 10.2.0.1.0
DBJAVA Required Support Files Patch 10.2.0.3.0
Enterprise Manager Minimal Integration 10.2.0.1.0
Enterprise Manager plugin Common Files 10.2.0.1.0 Beta
HAS Common Files 10.2.0.1.0
HAS Common Files Patch 10.2.0.3.0
Installation Common Files 10.2.0.1.0

Installation Common Files Patch 10.2.0.3.0
Installer SDK Component 10.2.0.3.0
Java 2 SDK 1.4.2.0.8
Java Runtime Environment 1.4.2.8.0
JDBC Common Files 10.2.0.1.0
LDAP Required Support Files 10.2.0.1.0
LDAP Required Support Files Patch 10.2.0.3.0
Oracle Advanced Security 10.2.0.1.0
Oracle Advanced Security Patch 10.2.0.3.0
Oracle Call Interface (OCI) 10.2.0.1.0
Oracle Call Interface (OCI) Patch 10.2.0.3.0
Oracle Client 10.2.0.1.0
Oracle Client Patch 10.2.0.3.0
Oracle Clusterware RDBMS Files 10.2.0.1.0
Oracle Clusterware RDBMS Files Patch 10.2.0.3.0
Oracle Code Editor 1.2.1.0.0I
Oracle Core Required Support Files 10.2.0.1.0
Oracle Core Required Support Files Patch 10.2.0.3.0
Oracle Database 10g Release 2 Patch Set 2 10.2.0.3.0
Oracle Display Fonts 9.0.2.0.0
Oracle Extended Windowing Toolkit 3.4.38.0.0
Oracle Globalization Support 10.2.0.1.0
Oracle Globalization Support Patch 10.2.0.3.0
Oracle Help For Java 4.2.6.1.0
Oracle Ice Browser 5.2.3.6.0
Oracle JDBC Thin Driver for JDK 1.2 10.2.0.1.0
Oracle JDBC Thin Driver for JDK 1.2 Patch 10.2.0.3.0
Oracle JDBC/OCI Instant Client 10.2.0.1.0
Oracle JDBC/OCI Instant Client Patch 10.2.0.3.0
Oracle JFC Extended Windowing Toolkit 4.2.33.0.0
Oracle Locale Builder 10.2.0.1.0
Oracle Net 10.2.0.1.0
Oracle Net Patch 10.2.0.3.0
Oracle Net Required Support Files 10.2.0.1.0
Oracle Net Required Support Files Patch 10.2.0.3.0
Oracle One-Off Patch Installer 10.2.0.3.0
Oracle RAC Required Support Files-HAS 10.2.0.1.0
Oracle RAC Required Support Files-HAS Patch 10.2.0.3.0
Oracle Required Support Files 32 bit 10.2.0.0.0
Oracle Required Support Files 32 bit 10.2.0.3.0
Oracle UIX 2.1.22.0.0
Oracle Universal Installer 10.2.0.3.0
Oracle Wallet Manager 10.2.0.1.0
Oracle Wallet Manager Patch 10.2.0.3.0
Parser Generator Required Support Files 10.2.0.1.0
Perl Interpreter 5.8.3.0.2
Platform Required Support Files 10.2.0.1.0
Platform Required Support Files 10.2.0.3.0

Precompiler Common Files 10.2.0.1.0
Precompiler Common Files Patch 10.2.0.3.0
Precompiler Required Support Files 10.2.0.1.0
Precompiler Required Support Files Patch 10.2.0.3.0
RDBMS Required Support Files 10.2.0.1.0
RDBMS Required Support Files for Instant Client 10.2.0.1.0
RDBMS Required Support Files for Instant Client Patch 10.2.0.3.0
RDBMS Required Support Files Patch 10.2.0.3.0
regexp 2.1.9.0.0
Required Support Files 10.2.0.1.0
Secure Socket Layer 10.2.0.1.0
Secure Socket Layer Patch 10.2.0.3.0
SQL*Plus Required Support Files 10.2.0.1.0
SQL*Plus Required Support Files Patch 10.2.0.3.0
SSL Required Support Files for InstantClient 10.2.0.1.0
SSL Required Support Files for InstantClient Patch 10.2.0.3.0
Sun JDK extensions 10.1.2.0.0
XDK Required Support Files 10.2.0.1.0
XDK Required Support Files Patch 10.2.0.3.0

A.3 Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) Components

Oracle Business Intelligence Systems Management
Oracle Business Intelligence Server
Oracle Business Intelligence Cluster Controller
Oracle Business Intelligence Client
Oracle Business Intelligence Presentation Services

Annex B Start / Restart Procedure

B.1 Update user.sh

Add the following entries to the `user.sh` script located in the `/space/oracle/product/OBIEE/setup` directory (machines 1 and 2):

```
export ORACLE_HOME=/space/oracle/product/10.2.0/client
export TNS_ADMIN=$ORACLE_HOME/network/admin
export PATH=$ORACLE_HOME/bin:/opt/bin:$PATH
export LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$LD_LIBRARY_PATH
```

B.2 Start Order

The environment must be started in the following order:

- Machine 7
- Machines 1 and 2
- Machines 3, 4, 5 and 6

B.3 Start / Restart Procedure

Machines 1 and 2:

```
/space/oracle/product/OBIEE/setup/run-ccs.sh start
/space/oracle/product/OBIEE/setup/run-sa.sh start
/space/oracle/product/OBIEE/setup/run-saw.sh start
```

Machine 3:

```
export ORACLE_HOME=/space/oracle/product/10.2.0/db
export PATH=%ORACLE_HOME%/bin:$PATH
export ORACLE_SID=orcl
lsnrctl start
sqlplus / as sysdba
startup
exit
```

Machine 4:

```
export ORACLE_HOME=/space/oracle/product/10gAS/10g_OIM
export PATH=$ORACLE_HOME/bin:$ORACLE_HOME/opmn/bin:$PATH
export ORACLE_SID=oid
lsnrctl start
sqlplus / as sysdba
startup
exit
opmnctl startall
```

Machine 5:

```
export ORACLE_HOME=/space/oracle/product/10gAS/10g_J2EE
export PATH=$ORACLE_HOME/bin:$ORACLE_HOME/opmn/bin:$PATH
opmnctl startall

export ORACLE_HOME=/space/oracle/product/10gAS/10g_OHS
export PATH=$ORACLE_HOME/bin:$ORACLE_HOME/opmn/bin:$PATH
opmnctl startall
```

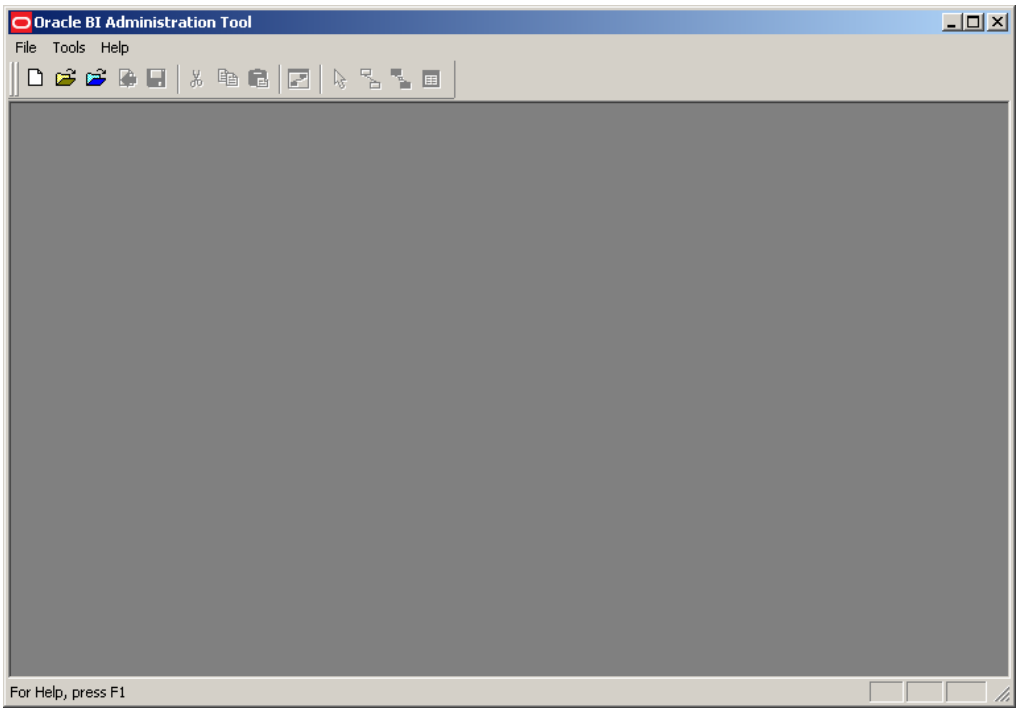
Machines 6 and 7 have no specific start procedure – they only requirement is that they are started.

B.4 User Tracking Data Structure change procedure

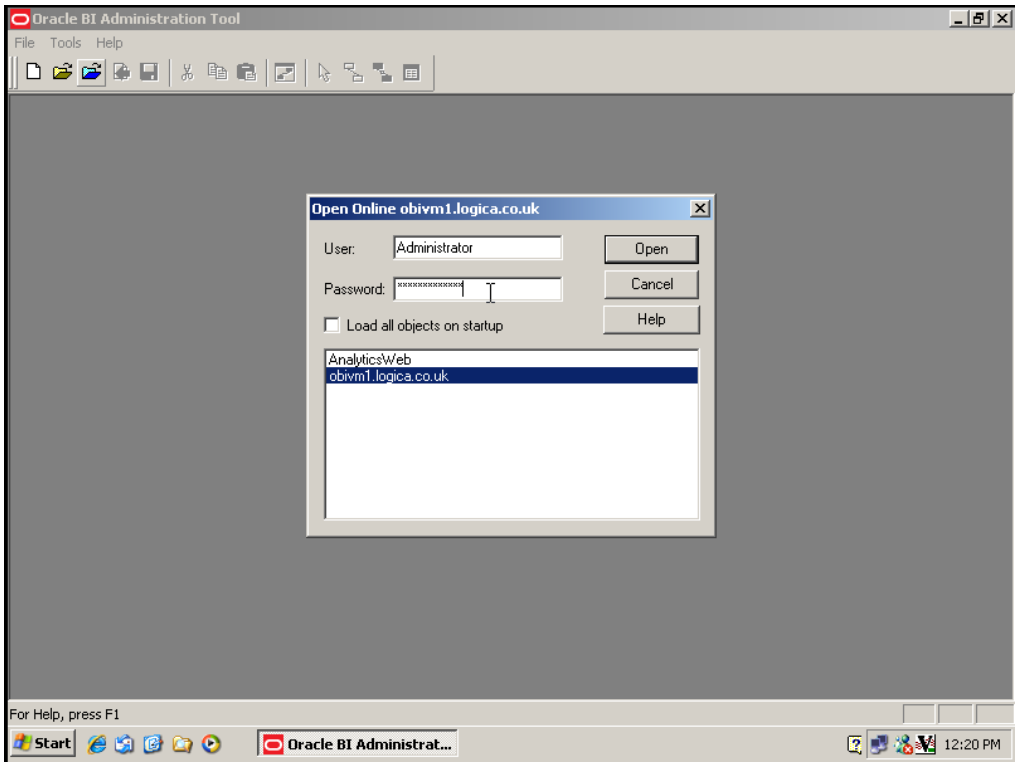
A correction is required in the Usage Tracking Data Structure to ensure that when a user impersonates another user within the Oracle Business Intelligence, the users are identified in terms of logged on username and impersonating user.

The following steps should be followed **once** after the install on Machine 6 followed by a stop and re-start of machines 1 - 5.

Open the BI Administration Tool by navigating to Start > Programs > Oracle Business Intelligence > Administration

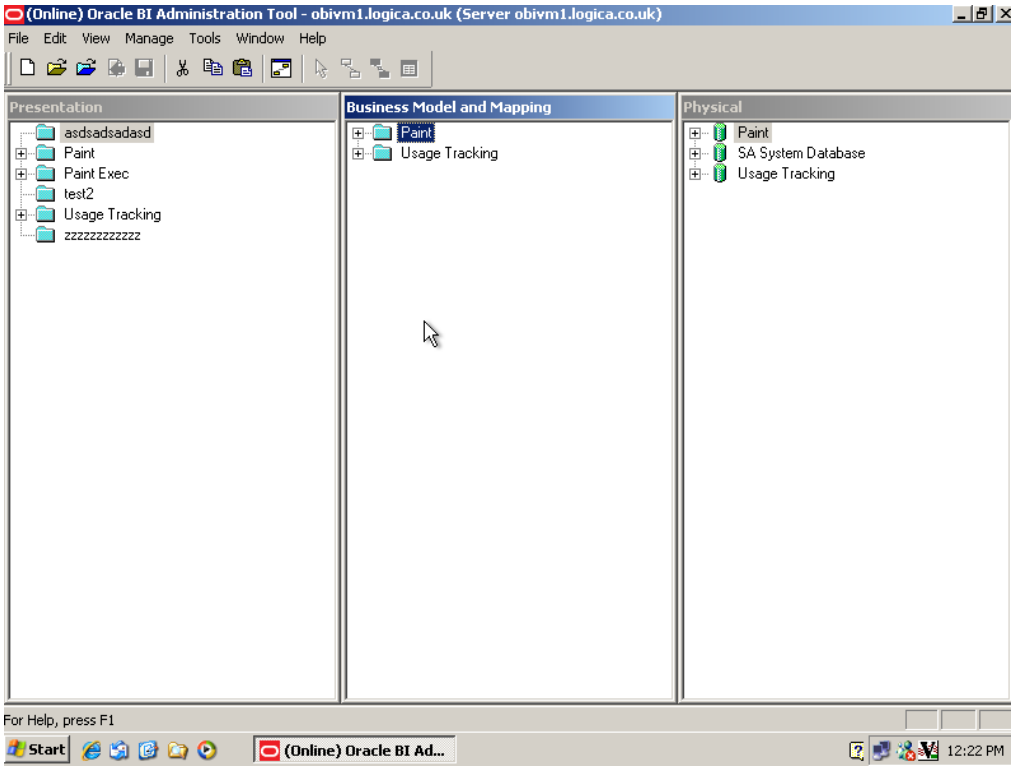


Click Open Online 

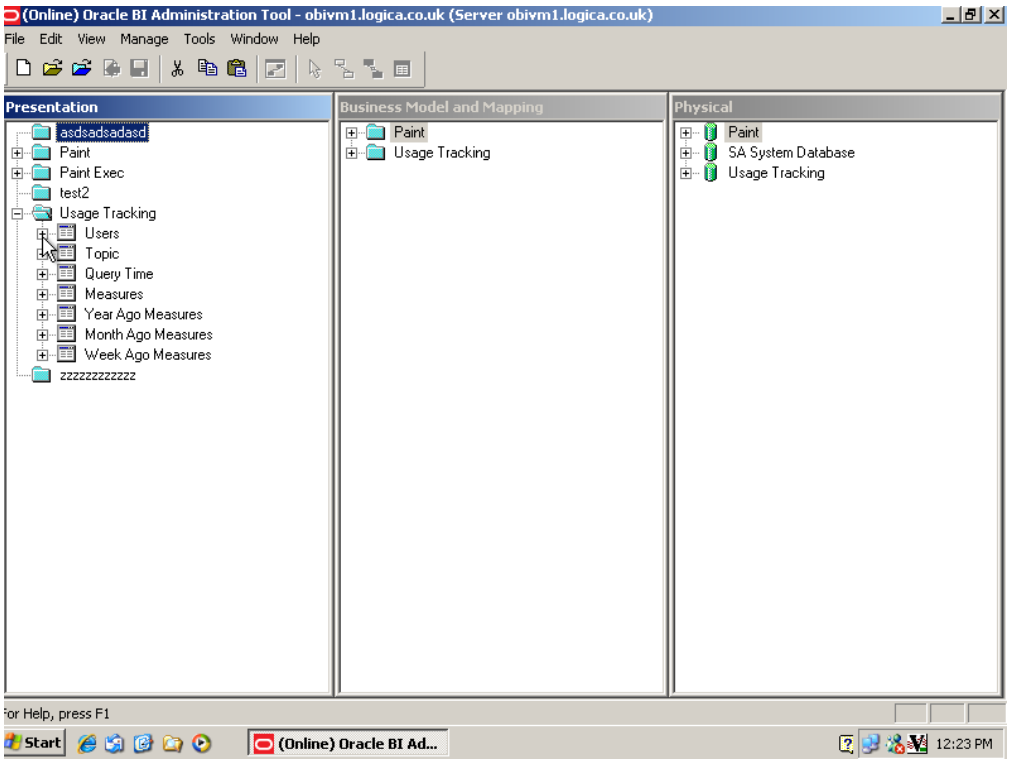


Enter Administrator password in the Password dialog.

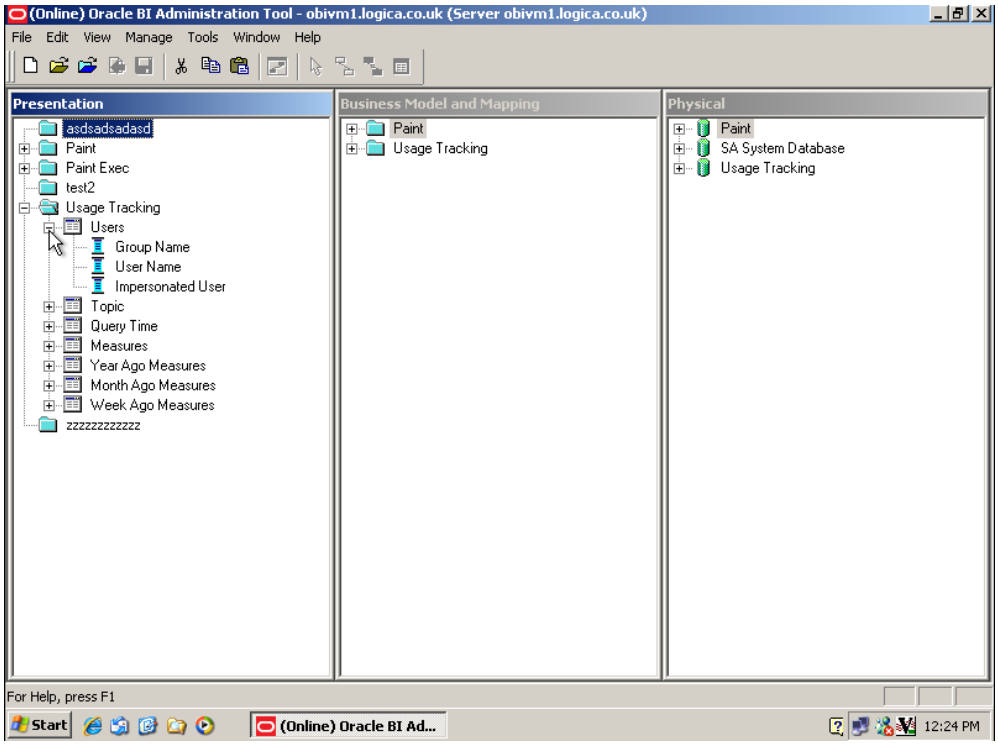
Click Open



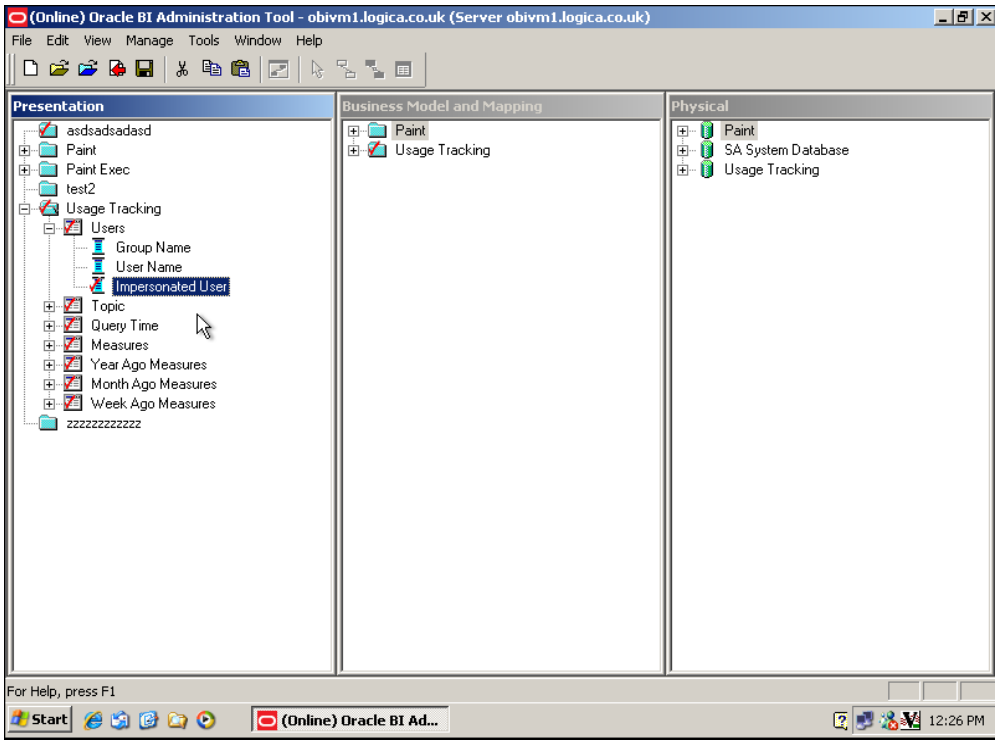
In the Presentation window, click the + next to the “Usage Tracking” folder



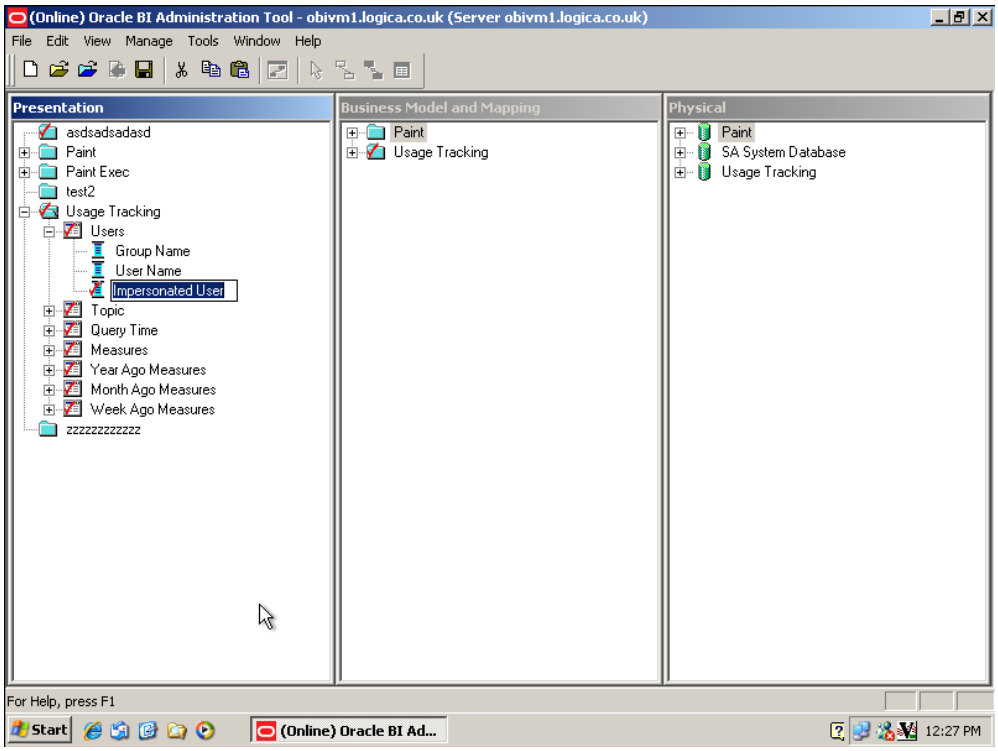
Click on the + next to “Users”



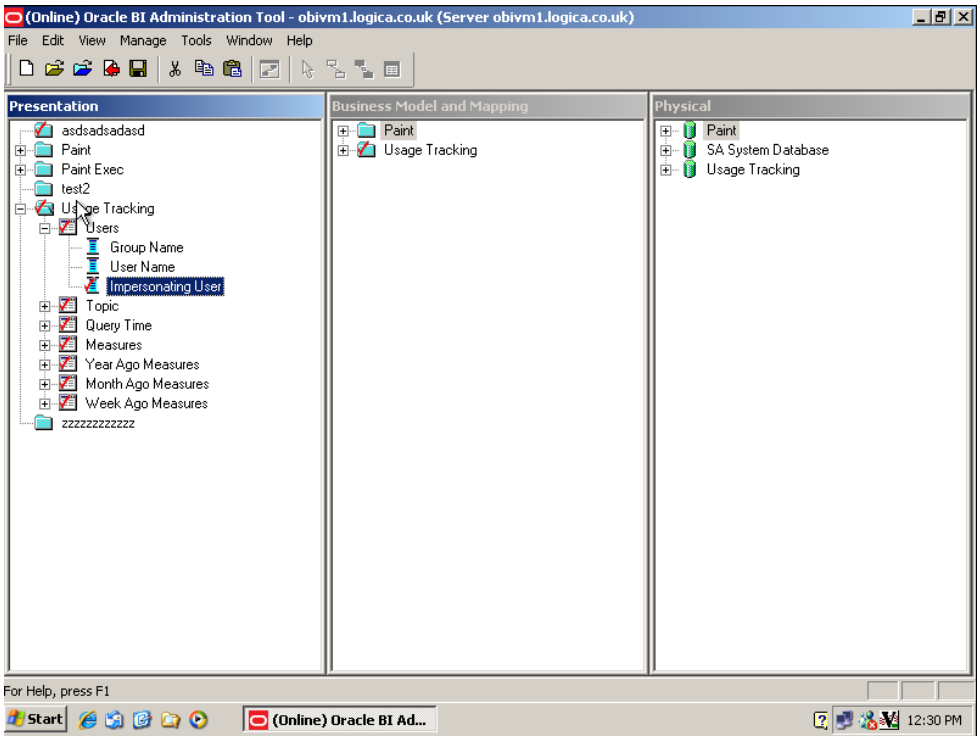
Right click on “Impersonated User” and click on “Check Out”



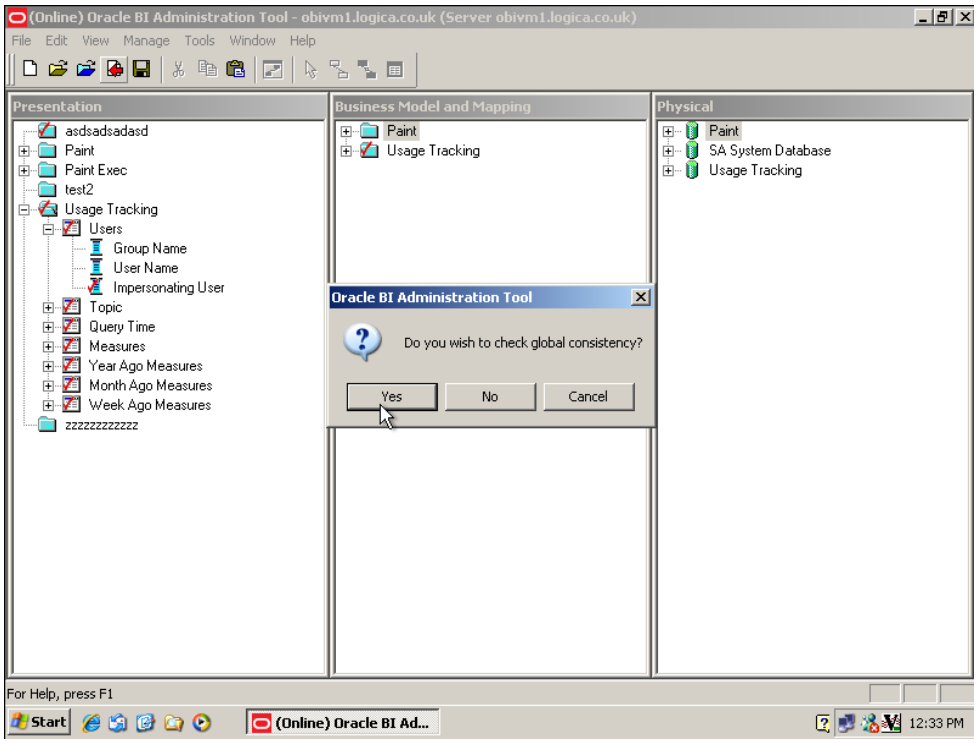
Right click on “Impersonated User” and click on “Rename”



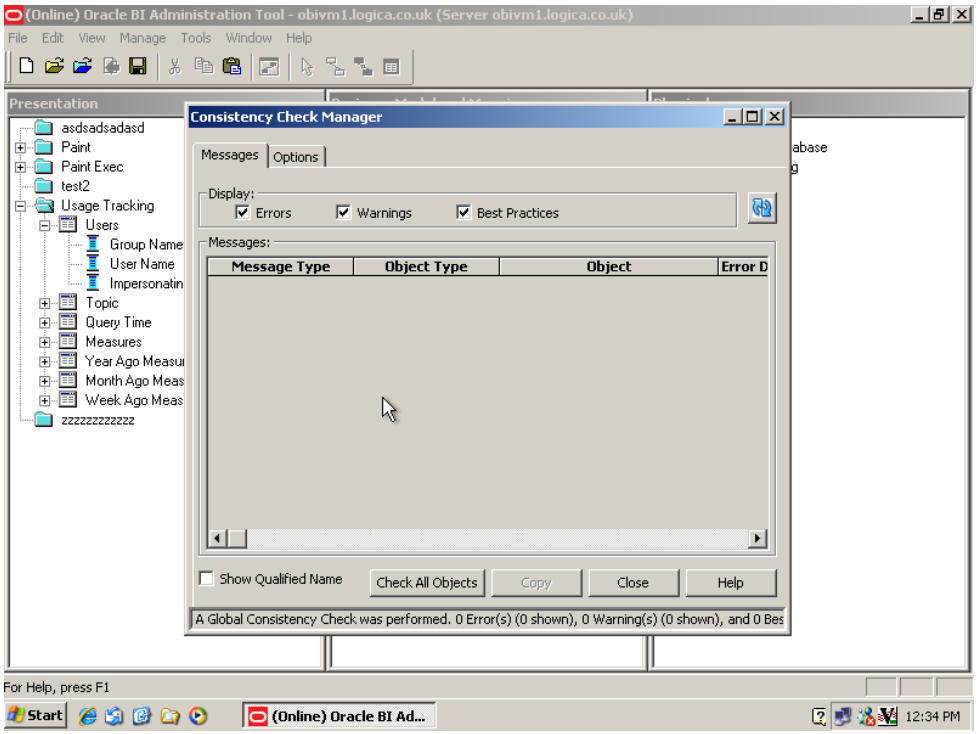
Type “Impersonating User” and press “Enter”



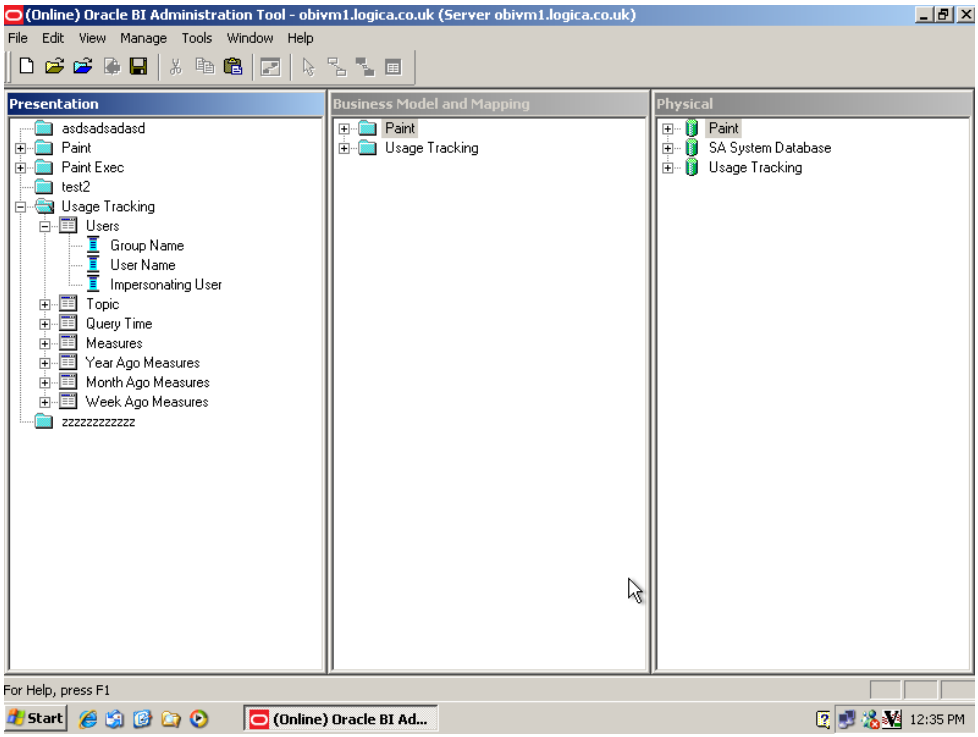
Click on the “Check In Changes” button 



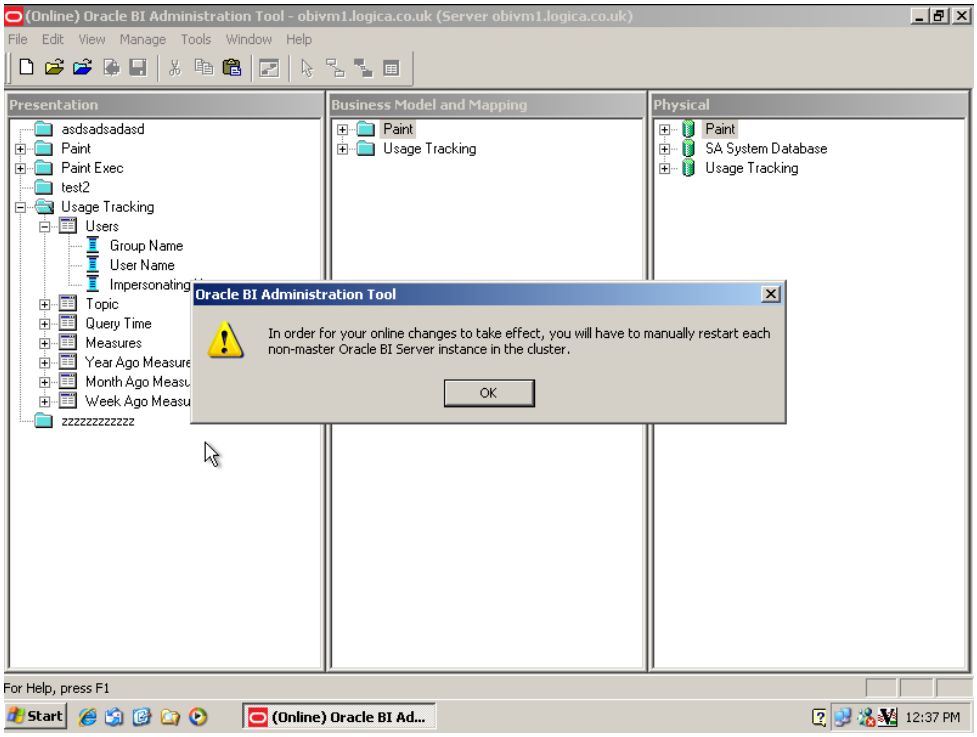
Click “Yes”



Click “Close”



Click File > Save



Click OK, stop machines 1 -5 and re-start machines 1 - 5.

Annex C Oracle Enterprise Linux 4 Update 5 x86_64

This annex describes the steps required to install the evaluated configuration of Oracle Enterprise Linux 4 Update 5 x86_64. [ECGOEL4] may be read for general guidance when installing Oracle Enterprise Linux.

The information that was supplied by the administrator for each step during the installation of the Oracle Enterprise Linux software for the evaluation of the TOE is indicated in the section below.

C.1 Prerequisites

C.1.1 Packages for the Evaluated Configuration

[ECGOEL4, 2] lists the additional packages required for the evaluated configuration. The kickstart file used for the installation was extracted from the `capp-eal4-config-oracle.rpm` package.

C.1.2 Common Customizations

Make the following changes to the `ks-x86_64.cfg` kickstart file:

```
keyboard uk
timezone Europe/London
firewall --disabled
selinux –disabled

logvol / --fstype ext3 --name=LvRoot --vgname=$VGNAME --
size=2048 --grow
logvol swap --fstype swap --name=LvSwap --vgname=$VGNAME --
size=2048
```

C.1.3 Customizations for Machines One and Two

For machines one and two add the following packages to the kickstart file:

```
compat-db.i386                  compat-db.x86_64
compat-libstdc++-33.i386        control-center
gnome-libs                      libstdc++.i386
libstdc++-devel.i386            openmotif21.i386
sysstat                         xorg-x11-xauth
xscreensaver
```

C.1.4 Customizations for Machine Three

For machine three, add the following packages to the kickstart file:

```
compat-db                          compat-libstdc++-33
control-center                     gnome-libs
libaio                             sysstat
xorg-x11-deprecated-libs.i386      xorg-x11-xauth
xscreensaver
```

C.1.5 Customizations for Machine Four

For machine four, add the following packages to the kickstart file:

```
compat-db.i386                     compat-db.x86_64
compat-libstdc++-296.i386          control-center
gnome-libs                         gnome-libs-devel
libstdc++.i386                     libstdc++-devel.i386
libstdc++-devel.x86_64             openmotif21.i386
sysstat                            xorg-x11-xauth
xscreensaver
```

C.1.6 Customizations for Machine Five

For machine five, add the following packages to the kickstart file:

```
compat-db.i386                     compat-db.x86_64
compat-libstdc++-296.i386          control-center
gdbm-1.8.0-24.i386                 gnome-libs
libstdc++.i386                     libstdc++-devel.i386
openmotif21.i386                   sysstat
xorg-x11-xauth                     xscreensaver
```

C.2 Oracle Enterprise Linux 4 Update 5 Installation

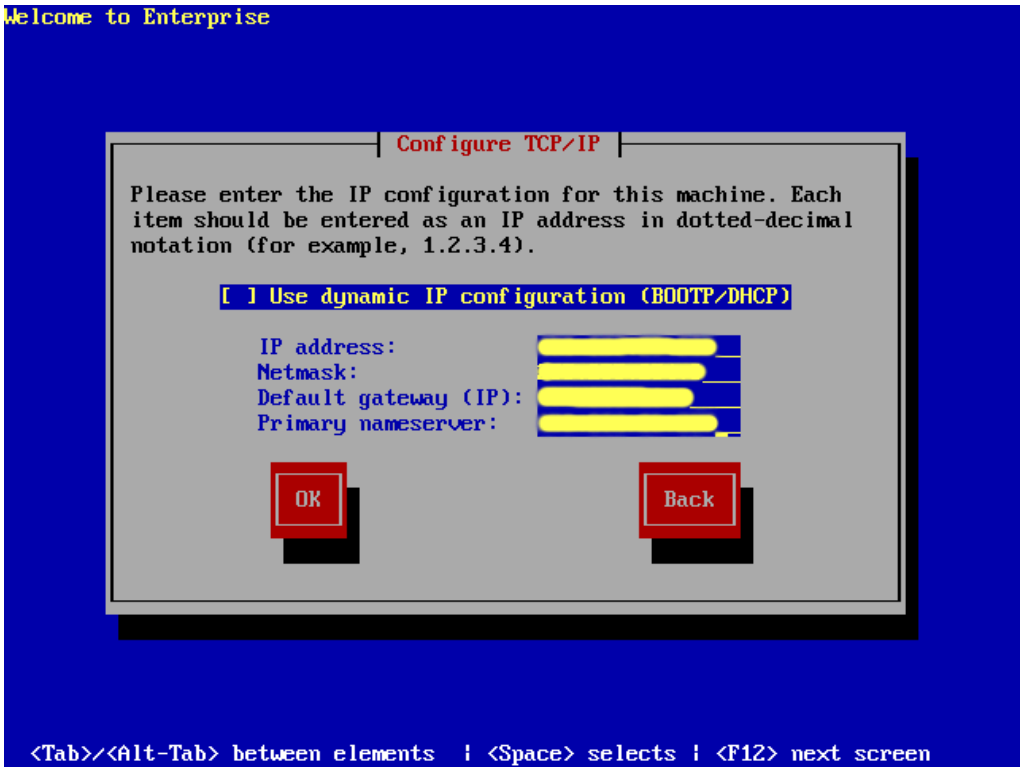
The operating system for machines one to five and seven should be installed according to the method described below. Start the machine.

C.2.1 Boot Prompt

At the boot prompt enter **'linux ks=cdrom:/ks-x86_64.cfg method=nfs:172.20.16.1:/stage/oel4u5_x64'**.

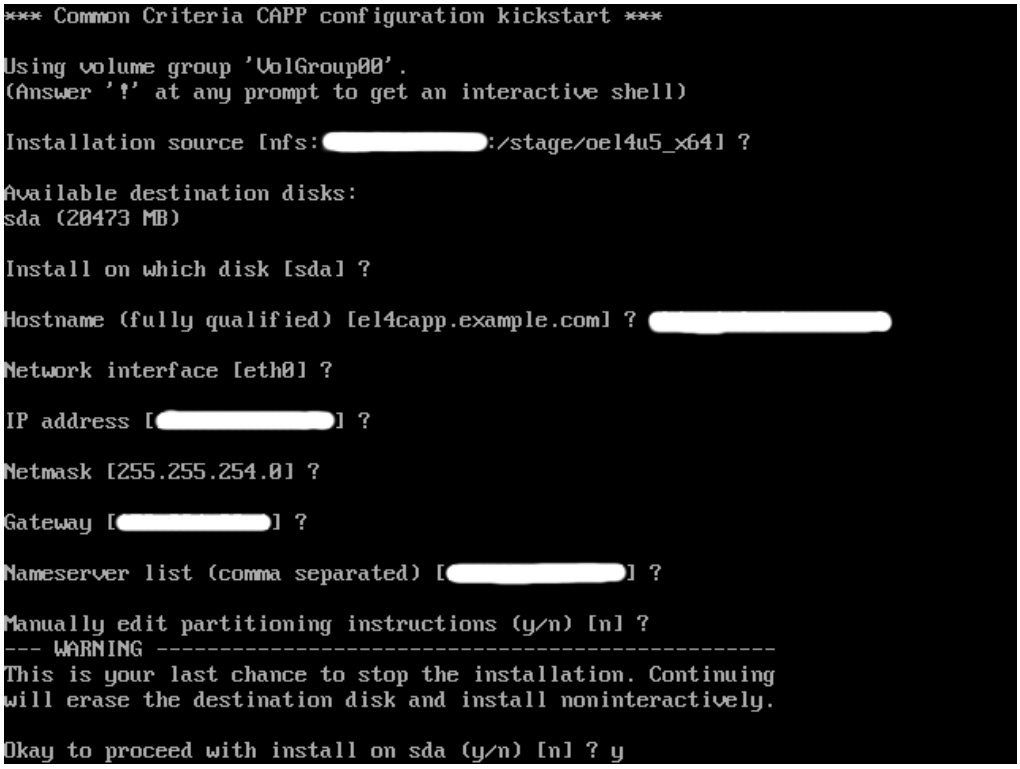
Click the 'Enter' button.

C.2.2 Configure TCP/IP



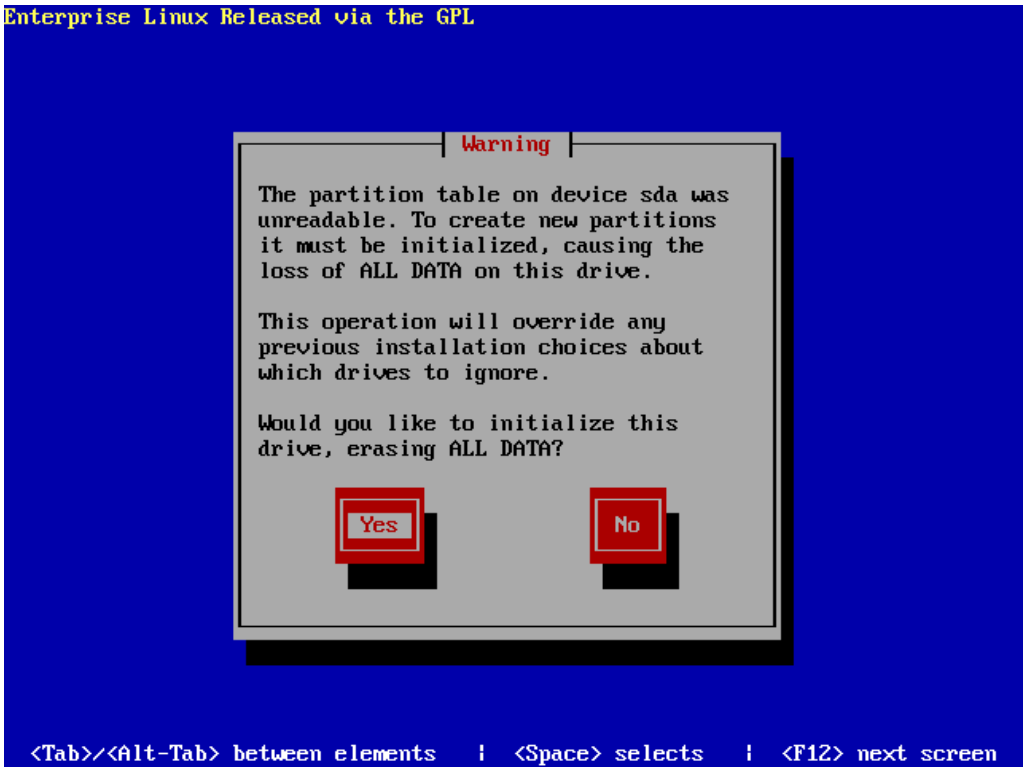
Deselect **'Use dynamic IP configuration (BOOTP/DHCP)'** and enter the required TCP/IP information.

C.2.3 Operating System Settings



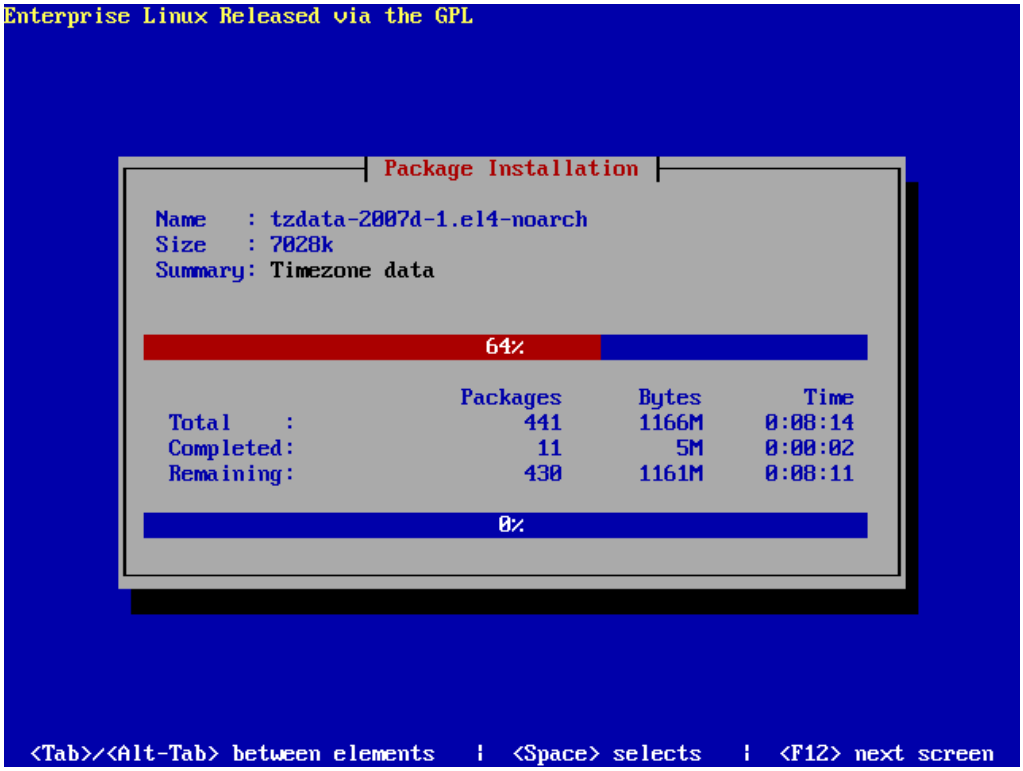
Enter the required information or accept the default values.

C.2.4 Create Partitions



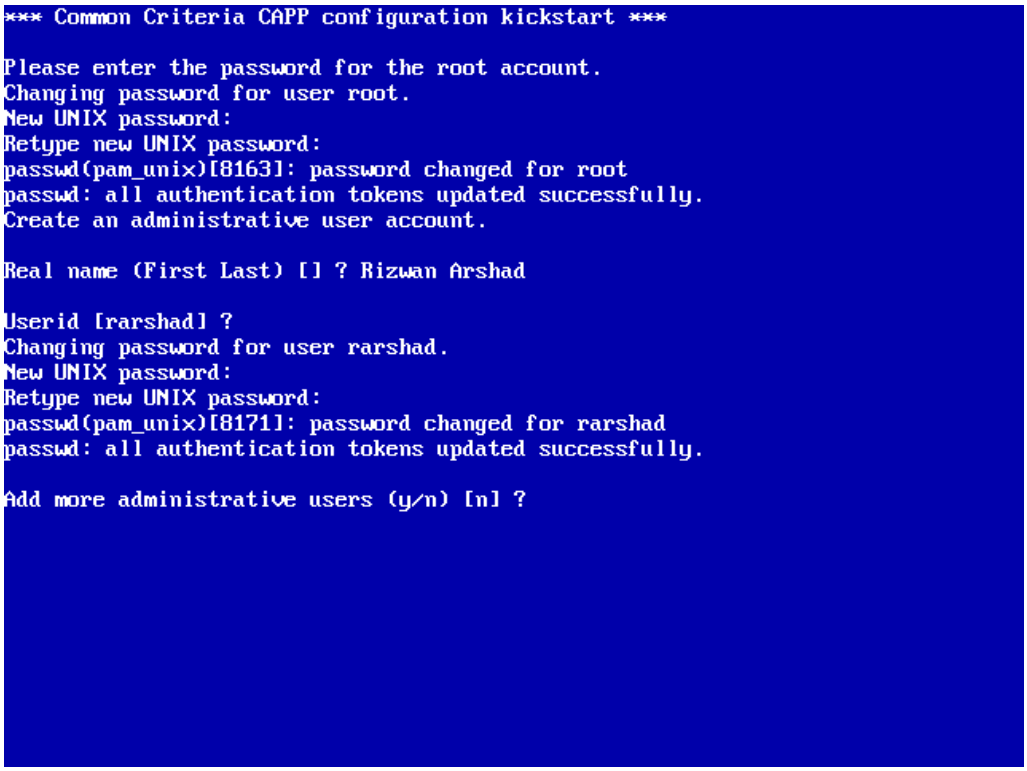
Initialize the drive by accepting to erase all data.

C.2.5 Installation



The operating system and required packages will now be installed.

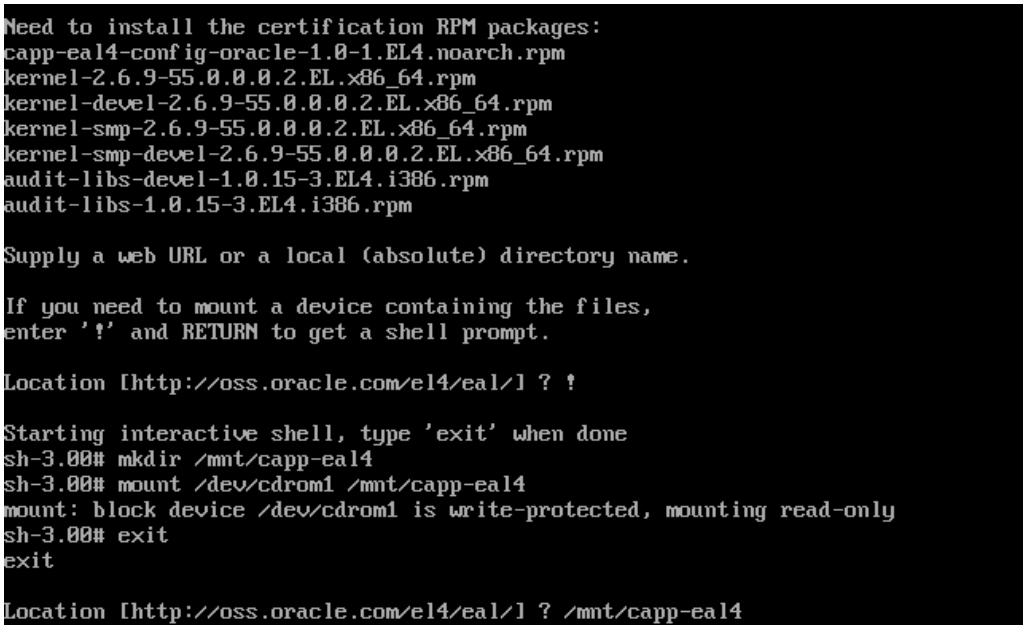
C.2.6 Common Criteria CAPP Configuration (1)



Once the operating system has been installed, the common criteria CAPP configuration script will be executed.

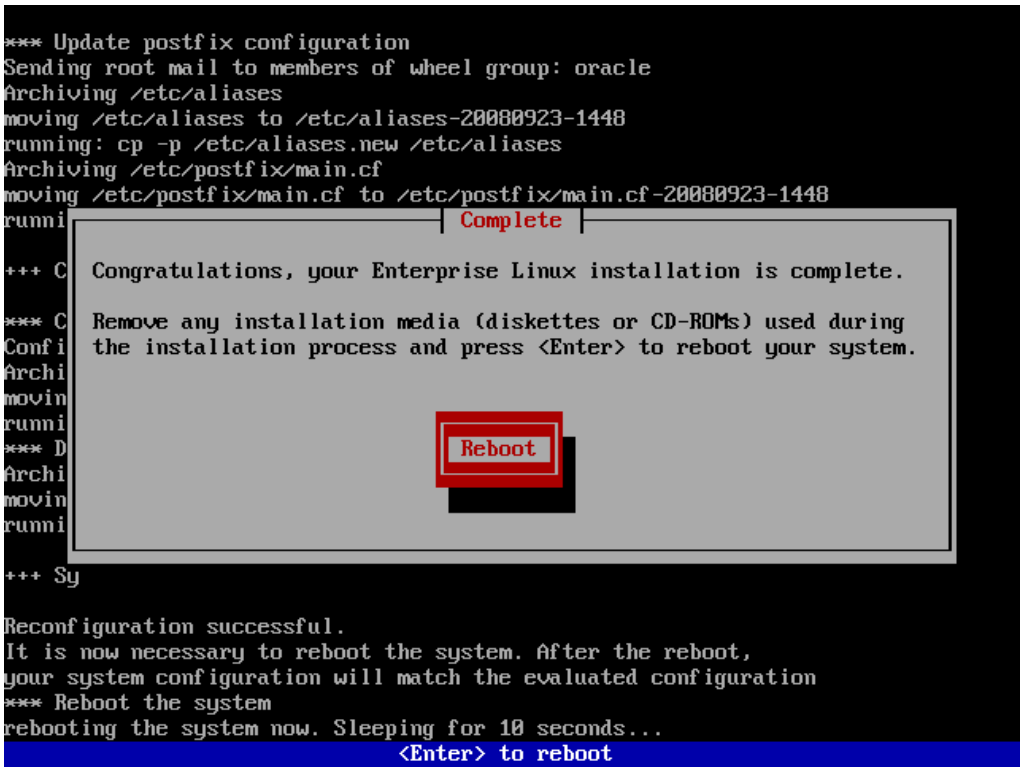
Set a password for the `root` user and create an administrative user.

C.2.7 Common Criteria CAPP Configuration (2)



Enter the location of the certification RPM packages.

C.2.8 Common Criteria CAPP Configuration (3)



Once the operating system has been rebooted the system configuration will match the evaluated configuration.

C.3 Post Installation Steps

The actions **[OS.1]** to **[OS-9]** listed in this section are required for machines one to five before the installation of the TOE can be carried out.

[OS.1] The entry in the file `/etc/redhat-release` must be modified to:

```
Red Hat Enterprise Linux AS release 4 (October Update 5)
```

[OS.2] X11 forwarding is required to run the Oracle GUI programs. Modify the `X11Forwarding` parameter in the `/etc/ssh/sshd_config` file:

```
X11Forwarding yes
```

Restart `sshd`:

```
/etc/init.d/sshd stop
/etc/init.d/sshd start
```

[OS.3] Add the following lines to the `/etc/security/limits.conf` file to increase the shell limits:

```
oracle    soft      nproc    2047
oracle    hard      nproc    16384
oracle    soft      nofile   2048
oracle    hard      nofile   65536
```

[OS.4] The following line must be present in the file `/etc/pam.d/login`:

```
session     required      /lib64/security/pam_limits.so
```

[OS.5] An operating system group, which will be used by the Oracle software owner, must be created before installing the TOE. Any legal name can be used for this group, but the convention is to use `oinstall`. The `oinstall` group can be created using the command:

```
$ /usr/sbin/groupadd oinstall
```

[OS.6] An operating system user that will be the Oracle software owner must be created before installing the TOE. The standard name used is `oracle`. When creating the user a primary group is required. The primary group should be `oinstall`. The `oracle` user can be created using the command:

```
$ /usr/sbin/useradd –g oinstall oracle
```

Set the `oracle` users password with the following command:

```
$ passwd oracle
```

[OS.7] Add the following lines to the `oracle` users `.bash_profile` file:

```
if [ $USER = "oracle" ]; then
     if [ $SHELL = "/bin/ksh" ]; then
          ulimit -p 16384
          ulimit -n 65536
     else
          ulimit -u 16384 -n 65536
     fi
fi
```

[OS.8] Create the installation directories and set the appropriate owner and group permissions on the directories using the following commands:

```
mkdir –p /space/oracle (machines 1 to 5)
mkdir –p /space/oracle/product/OBIEE (machines 1, 2 and 5)
chown –R oracle:oinstall /space
```

[OS.9] In the evaluated configuration, the software to be installed is made available through NFS. Issue the following commands as the `root` user:

```
/sbin/chkconfig –-level 3 portmap on
/sbin/chkconfig –-level 3 netfs on
/etc/init.d/portmap start
/etc/init.d/netfs start
mkdir –p /mnt/software
mount sagfs1t.saglab.uk.oracle.com:/vol/KITS \
/net/sagfs1t/vol/KITS
```

To permanently enable the NFS share, add the following line to the `/etc/fstab` file:

```
sagfs1t.saglab.uk.oracle.com:/vol/KITS /net/sagfs1t/vol/KITS \
nfs defaults 0 0
```

Annex D Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) Installation

This annex provides a step by step guide to installing Oracle SOA Suite 10*g* (10.1.3.1.0) in the evaluated configuration for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2), running on the Oracle Enterprise Linux Version 4 Update 5 operating system.

D.1 Prerequisites

As the `root` user add the following entries to the `/etc/sysctl.conf` file:

```
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
# semaphores: semmsl, semmns, semopm, semmni
kernel.sem = 256 32000 100 142
fs.file-max = 131072
net.ipv4.ip_local_port_range = 1024 65000
kernel.msgmni = 2878
kernel.msgmax = 8192
kernel.msgmnb = 65535
net.core.rmem_default = 262144
net.core.rmem_max = 262144
net.core.wmem_default = 262144
net.core.wmem_max = 262144
```

Use the following command to change the current values of the kernel parameters:

```
/sbin/sysctl –p
```

D.2 Input Parameters

The software installer will require the following input parameters for successful completion of the software installation. The values for these parameters should be gathered prior to starting the installation.

The following table should be completed with the insertion of the values to be used for the current installation into the ‘Installation Value’ column. The ‘Example Value’ column shows the values used in the example screenshots demonstrating the install process.

Pre-installation table matrix

Parameter Name	Installation Value	Example Value
Path		/space/oracle/product/10gAS/10g_J2EE
Inventory Path		/space/oracle/oraInventory
Instance Name		10gAS_J2EE
oc4jadmin Password		oracle1

D.3 Installation of Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0)

Login to the server machine as the oracle user and navigate to the directory where the issue media has been installed – in the Evaluated Configuration used to derive the screenshots given in this document, this was /net/sagfs1t/vol/KITS/Software/ApplicationServer/10.1.3.3-SOA/install

The following requirement must be performed prior to starting the Oracle Universal Installer. Enable 32-bit emulation mode by running the following command:

```
linux32 bash
```

As the `oracle` user set the `ORACLE_BASE` environment variable:

```
export ORACLE_BASE=/space/oracle
```

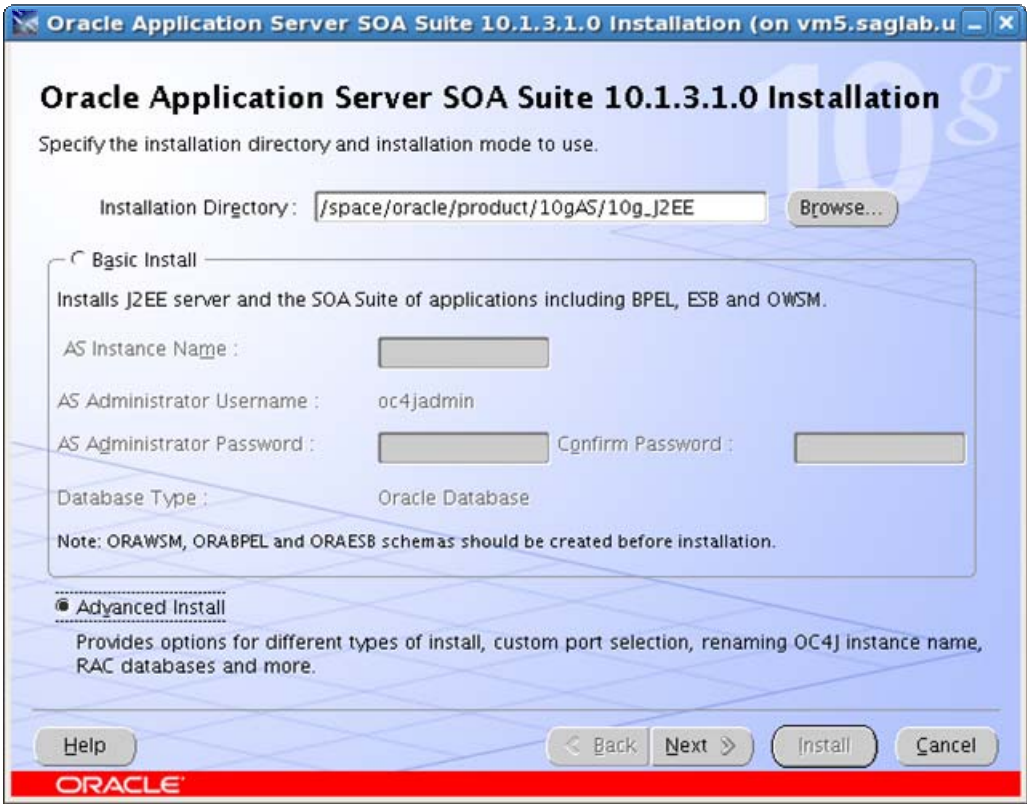
Start the Oracle Universal Installer as follows:

```
./runInstaller
```

The monitor pre-requisite check will fail as the `/usr/X11R6/bin/xdpyinfo` command is not available in the evaluated configuration of Oracle Enterprise Linux 4 Update 5. Ignore this error by entering **'Y'** when prompted to continue.

The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of Oracle SOA Suite 10*g* (10.1.3.1.0).

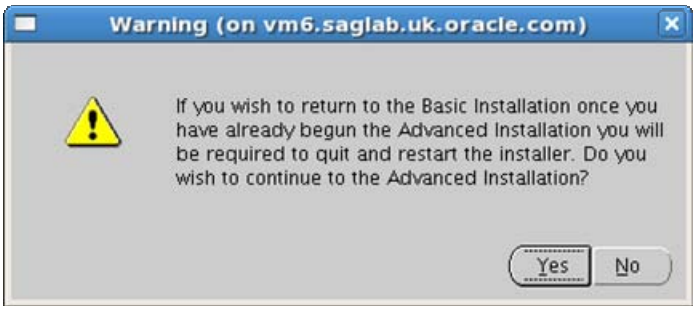
D.3.1 Installation



Enter the 'Installation Value' for the parameter **'Path'** specified in the pre-installation table matrix into the **'Installation Directory'** field.

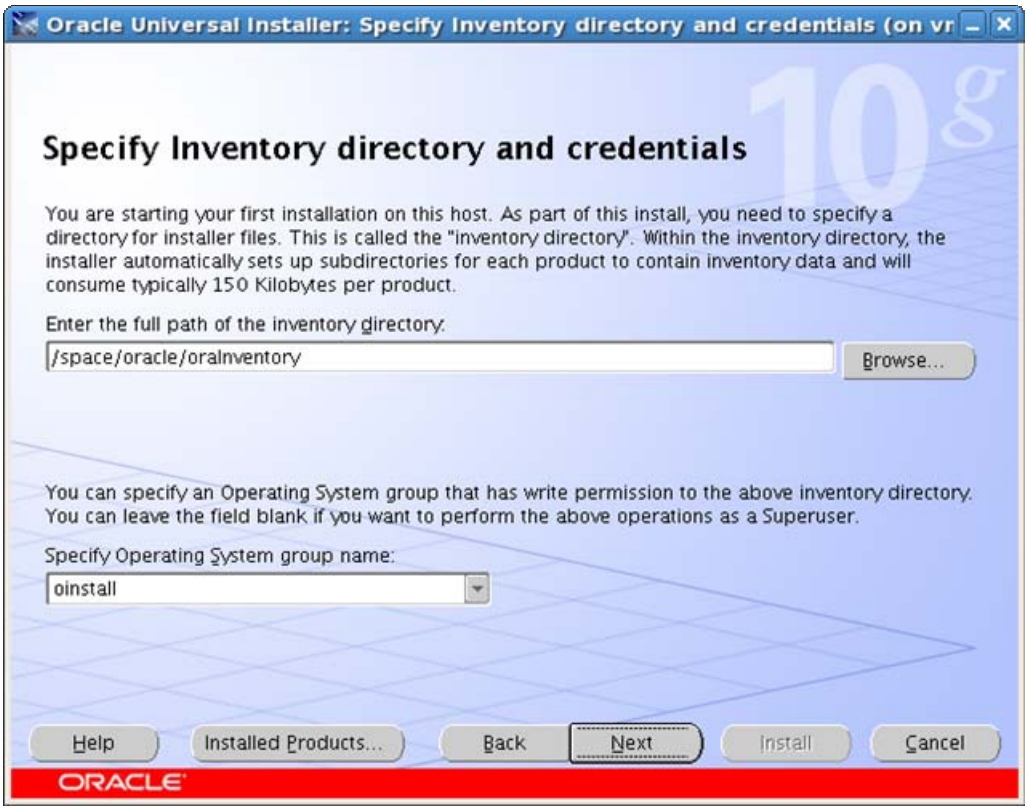
Click the **'Advanced Install'** radio button.

Click Next.



Click Yes.

D.3.2 Inventory

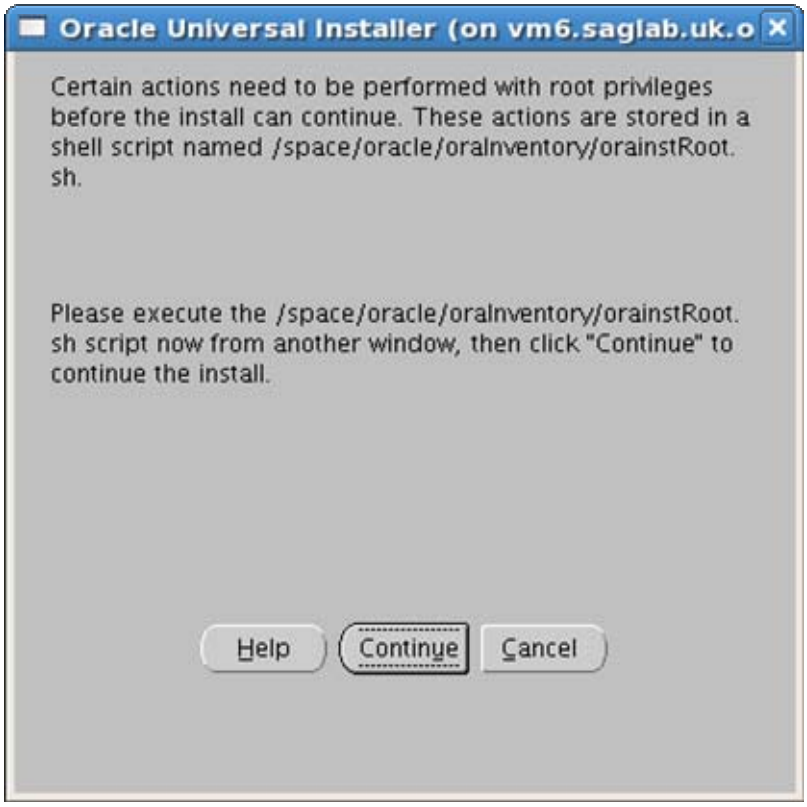


Enter the 'Installation Value' for the parameter **'Inventory Path'** specified in the pre-installation table matrix into the **'Inventory Directory'** field.

Accept the default setting of **'oinstall'** for the Operating System group name.

Click Next.

D.3.3 Configuration Script (1)

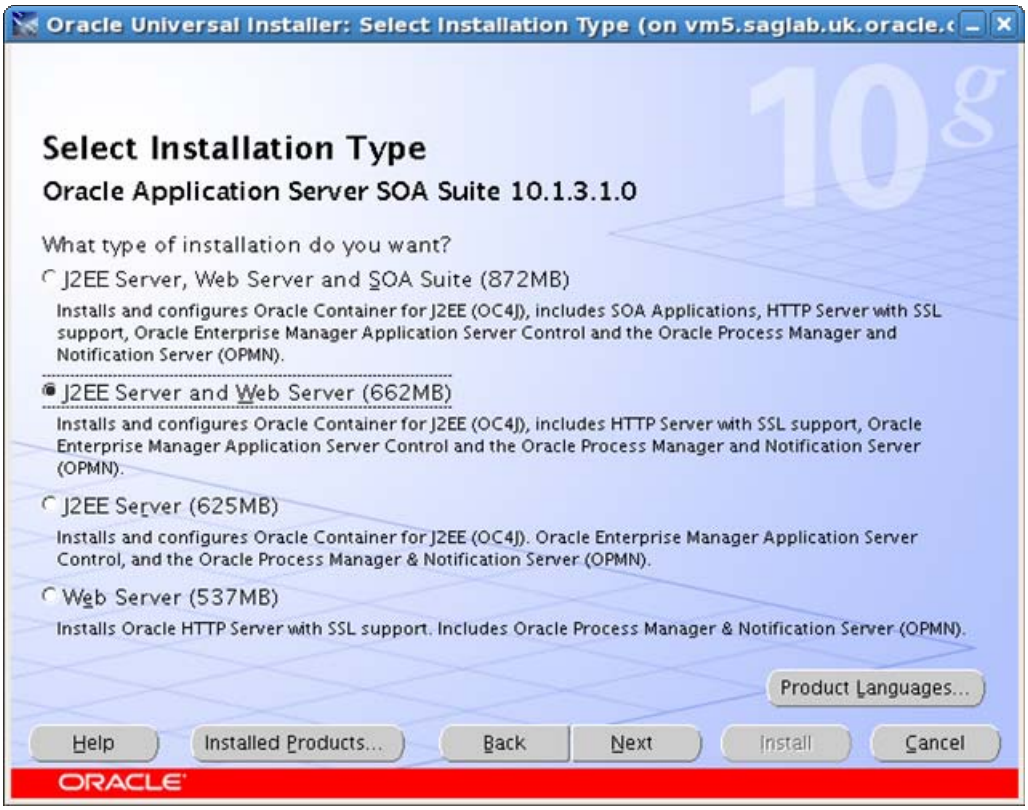


As the root user execute the script mentioned in the dialog. The script will output the following:

```
[root@vm3 ~]# /oracle/product/oraInventory/orainstRoot.sh
Creating the Oracle inventory pointer file (/etc/oraInst.loc)
Changing groupname of /oracle/product/oraInventory to oinstall.
[root@vm3 ~]#
```

When the script has completed return to the Oracle Universal Installer dialog window and click Continue.

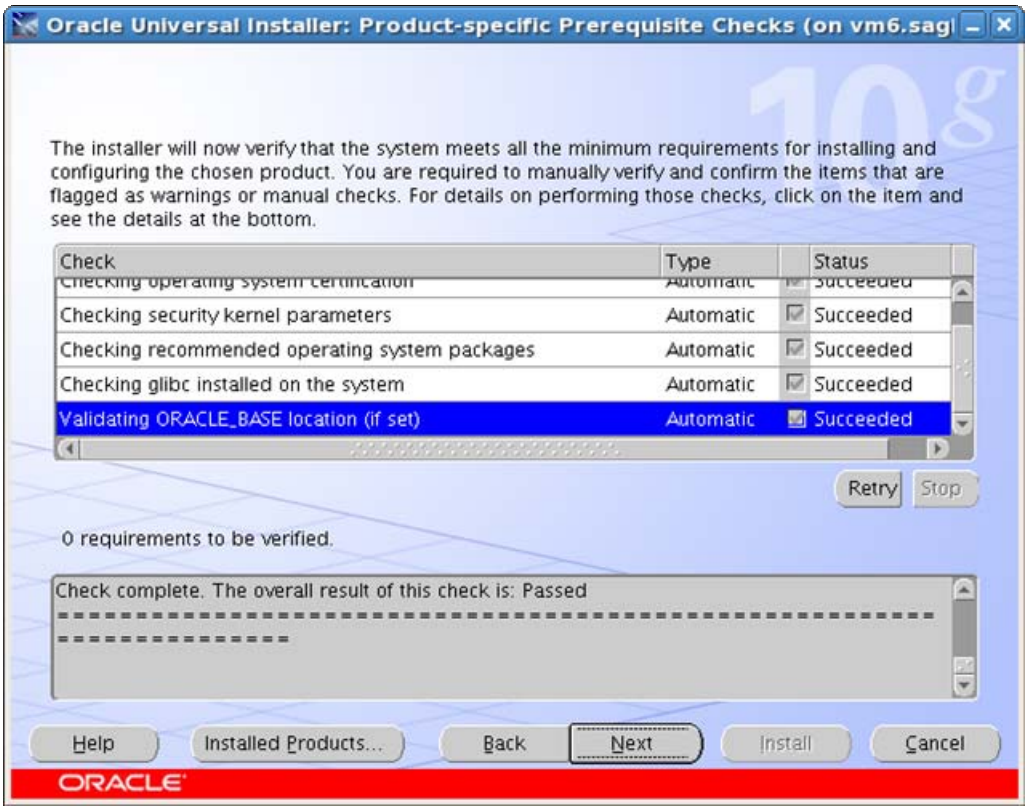
D.3.4 Installation Type



Click the **'J2EE Server and Web Server (662MB)'** radio button.

Click Next.

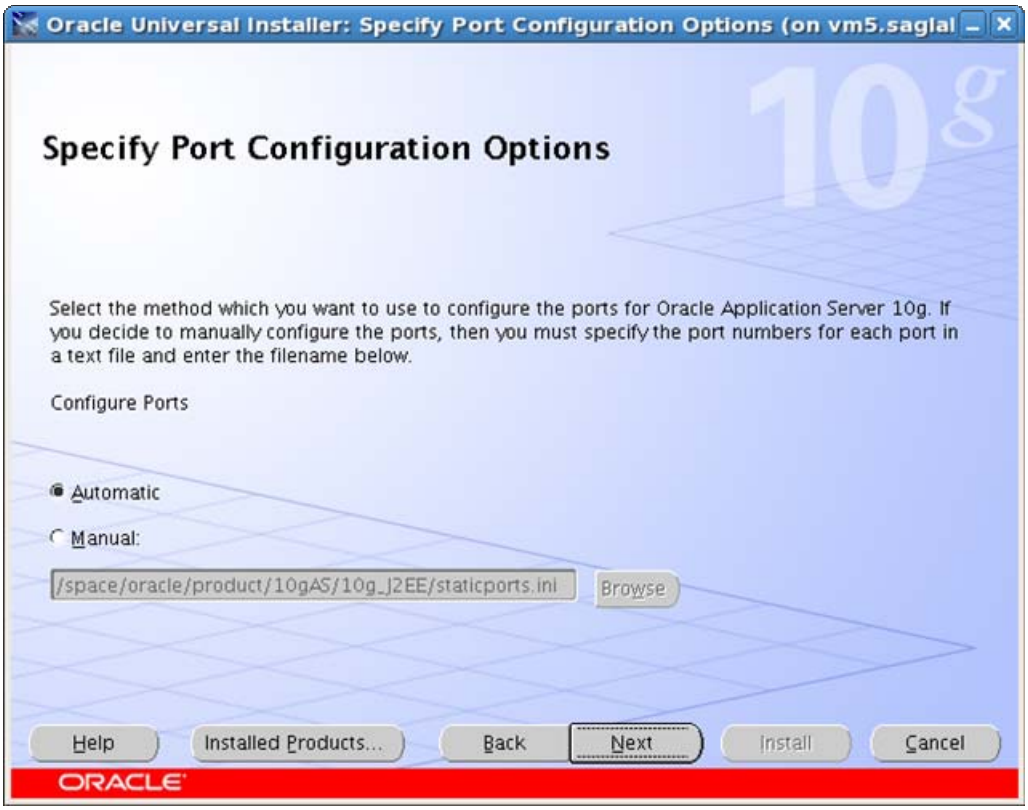
D.3.5 Prerequisite Checks



Ensure that all the product-specific prerequisite checks have a status of **'Succeeded'**.

Click Next.

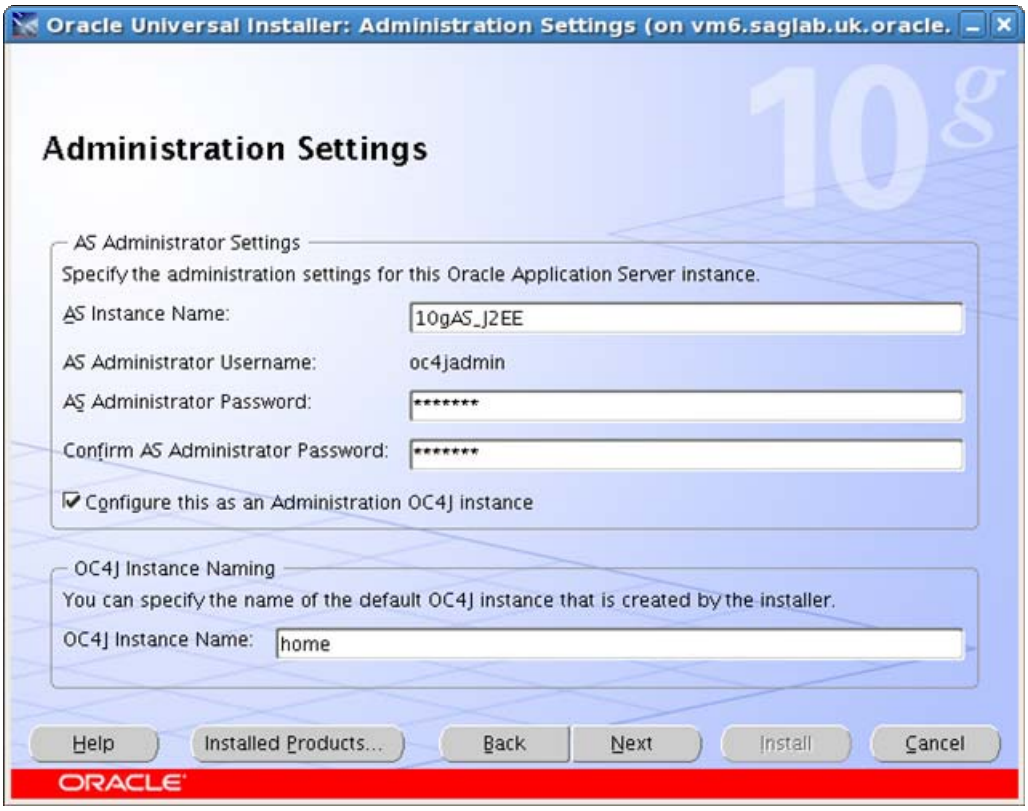
D.3.6 Port Configuration



Click the **'Automatic'** radio button.

Click Next.

D.3.7 Administration Settings



Enter the 'Installation Value' for the parameter **'Instance Name'** specified in the pre-installation table matrix into the **'AS Instance Name'** field.

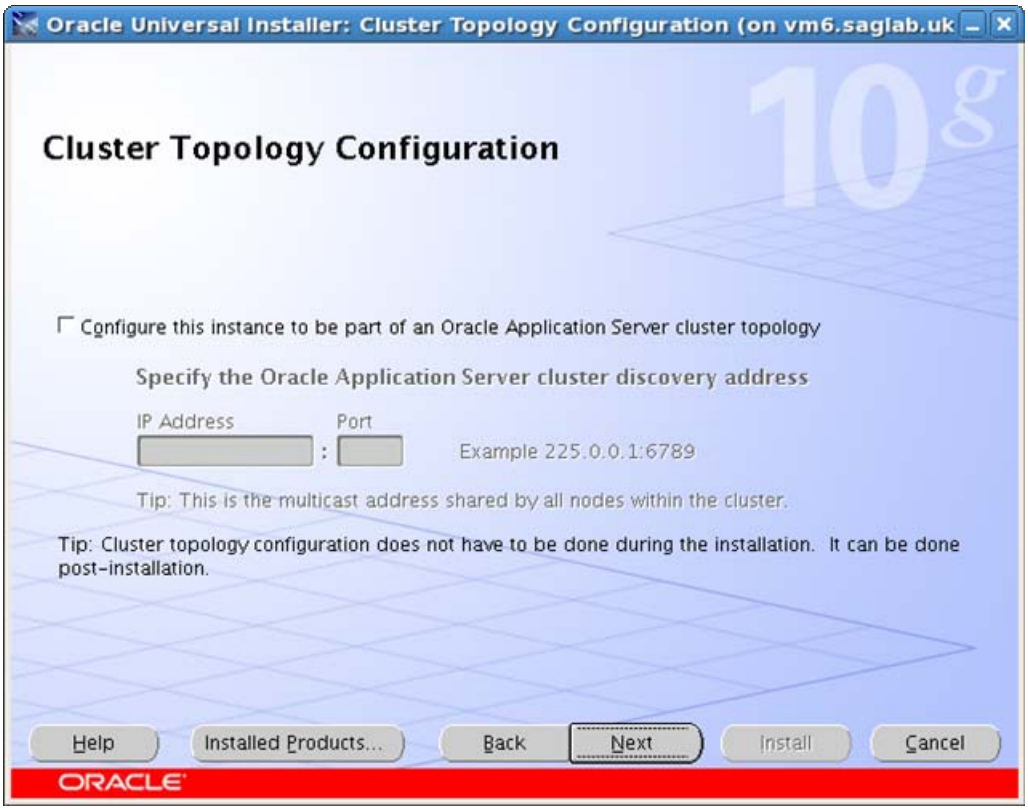
Enter the 'Installation Value' for the parameter **'oc4jadmin Password'** specified in the pre-installation table matrix into the **'AS Administrator Password'** and **'Confirm AS Administrator Password'** fields.

Tick the **'Configure this as an Administration OC4J instance'** check box.

Accept the default setting for **'OC4J Instance Name'**.

Click Next.

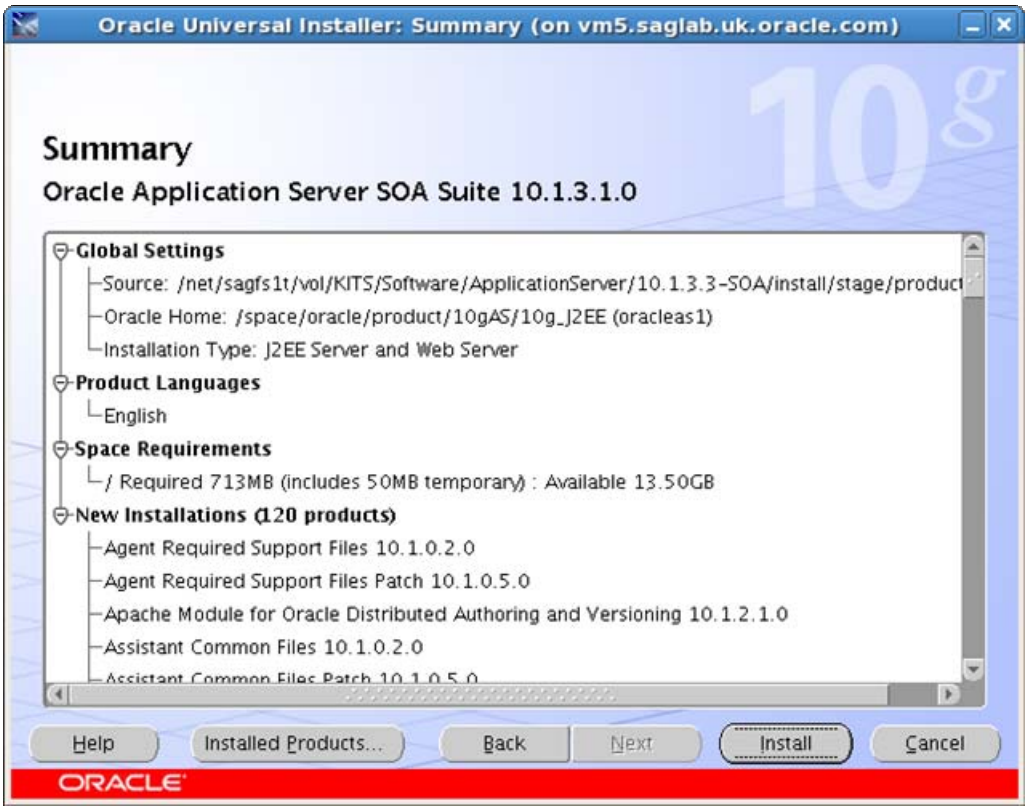
D.3.8 Cluster Topology



Accept the default settings.

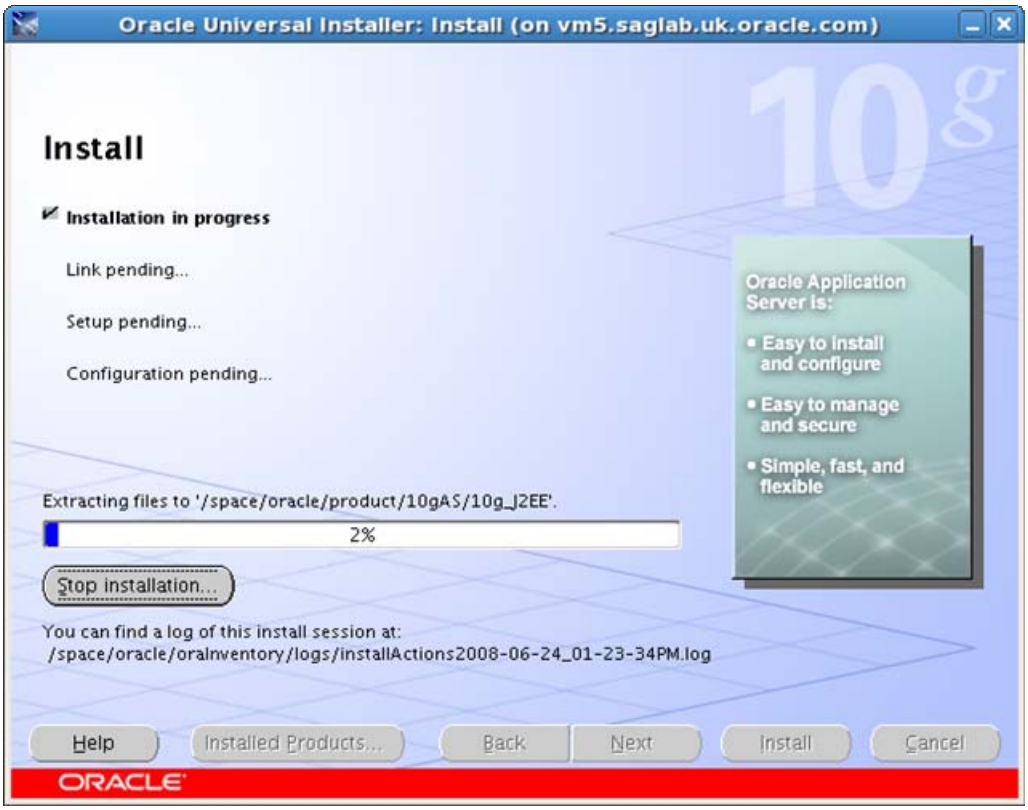
Click Next.

D.3.9 Summary

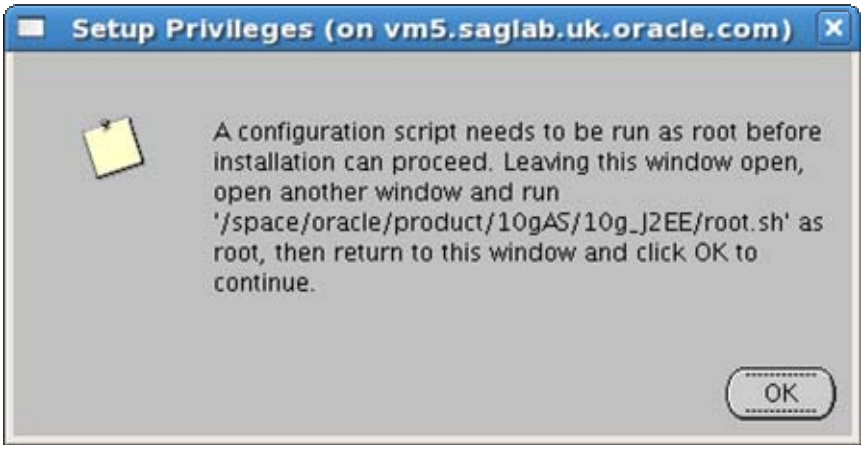


Click Install.

D.3.10 Install



D.3.11 Configuration Script (2)



As the `root` user execute the script mentioned in the dialog. The script will output the following:

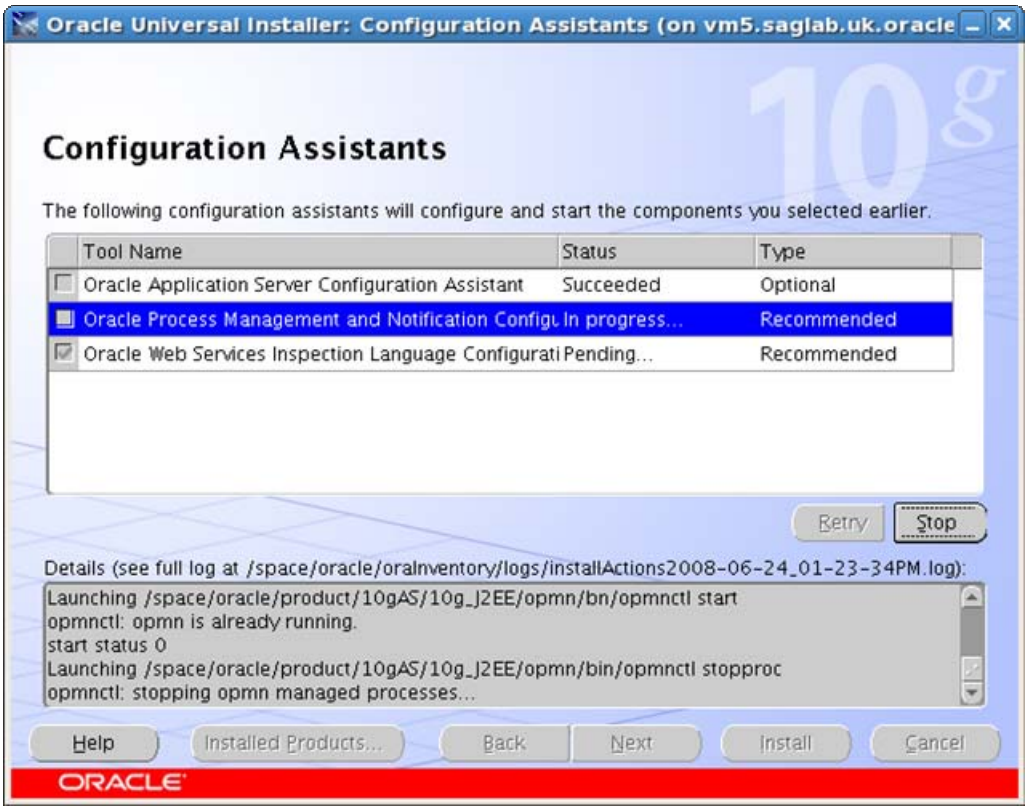
```
[root@vm3 ~]# /oracle/product/10gAS/10g_J2EE/root.sh
Running Oracle10 root.sh script...
\nThe following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /oracle/product/10gAS/10g_J2EE

Enter   the   full   pathname   of   the   local   bin   directory:
[/usr/local/bin]:
   Copying dbhome to /usr/local/bin ...
   Copying oraenv to /usr/local/bin ...
   Copying coraenv to /usr/local/bin ...

\nCreating /etc/oratab file...
Adding entry to /etc/oratab file...
Entries will be added to the /etc/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
[root@vm3 ~]#
```

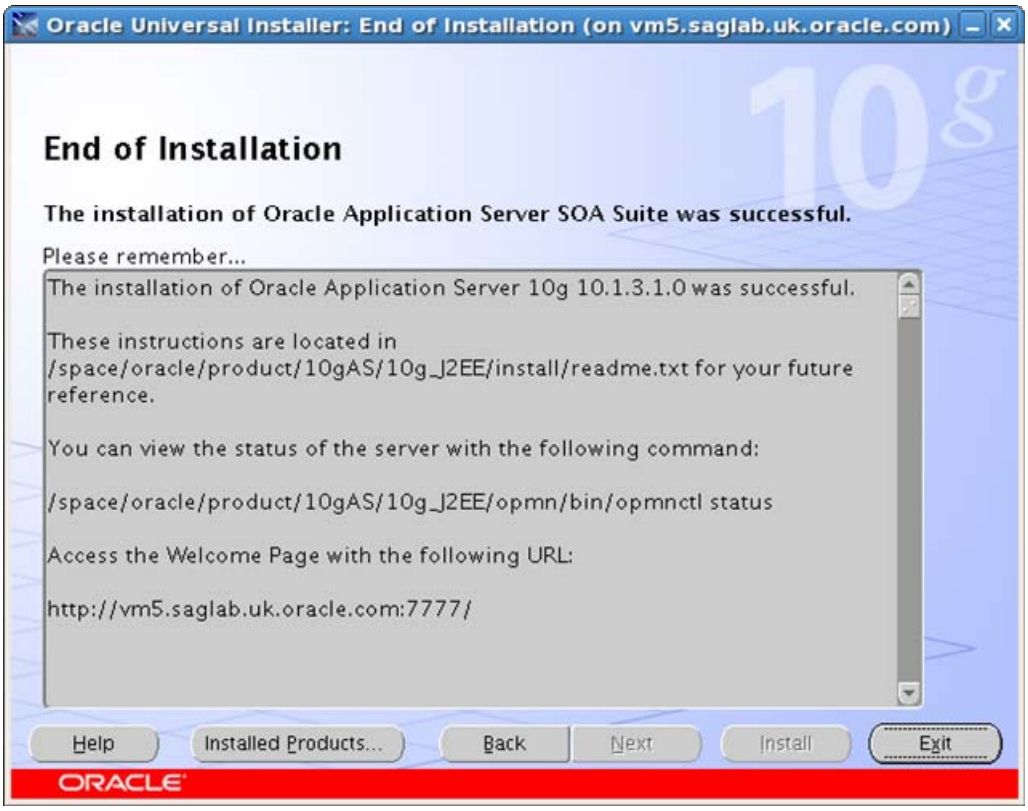
When the script has completed return to the **'Setup Privileges'** dialog box and click OK.

D.3.12 Configuration Assistants



The Oracle Universal Installer will run some configuration assistants.

D.3.13 End of Installation



Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) is now installed.

Click Exit.

Annex E Oracle Database 10g Client Release 2 (10.2.0.3.0) Installation

This annex provides a step by step guide to installing Oracle Database 10*g* Client Release 2 (10.2.0.3.0) in the evaluated configuration for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2), running on the Oracle Enterprise Linux Version 4 Update 5 operating system.

E.1 Prerequisites

Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) must be installed before proceeding with the Oracle Client installation. Annex D describes the steps needed to install Oracle SOA Suite.

E.2 Input Parameters

The Oracle Database 10*g* Client Release 2 (10.2.0.3.0) software installer will require the following input parameters for successful completion of the software installation. The values for these parameters should be gathered prior to starting the installation.

The following table should be completed with the insertion of the values to be used for the current installation into the 'Installation Value' column. The 'Example Value' column shows the values used in the example screenshots demonstrating the install process.

Pre-installation table matrix

Parameter Name	Installation Value	Example Value
Home		10g_10_2_0_CLIENT
Path		/space/oracle/product/10.2.0/client

E.3 Oracle Database 10*g* Client Release 2 (10.2.0.1.0) Installation

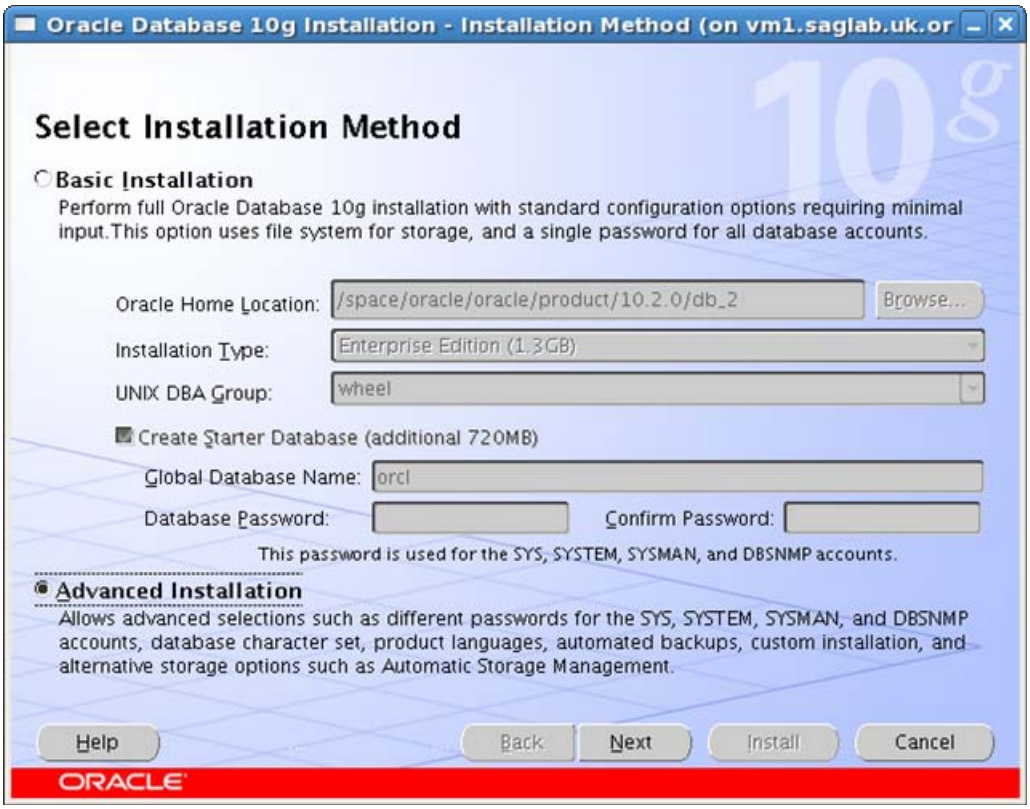
Login to the server machine as the `oracle` user and navigate to the directory where the issue media has been installed (in the Evaluated Configuration used to derive the screenshots given in this document, this was `/net/sagfs1t/vol/KITS/Software/Database/Linux/10.2.0.1/client`).

Start the Oracle Universal Installer as follows:

```
./runInstaller
```

The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of Oracle Database 10*g* Client Release 2 (10.2.0.1.0).

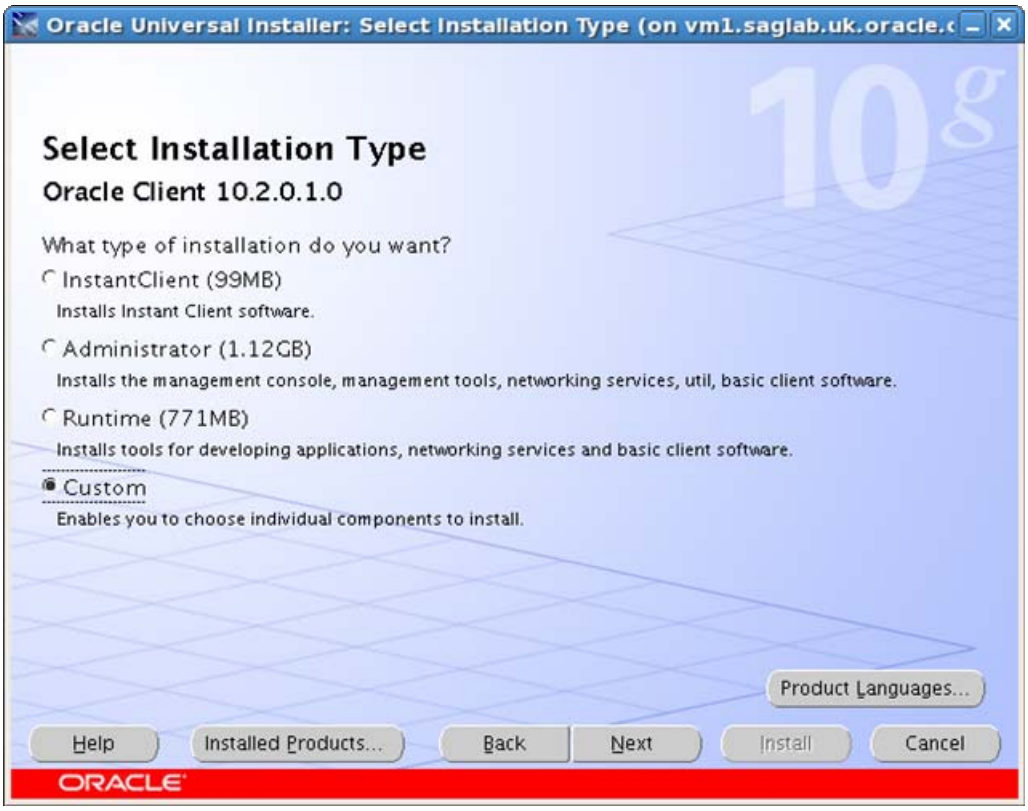
E.3.1 Installation Method



Click the **'Advanced Installation'** radio button.

Click Next.

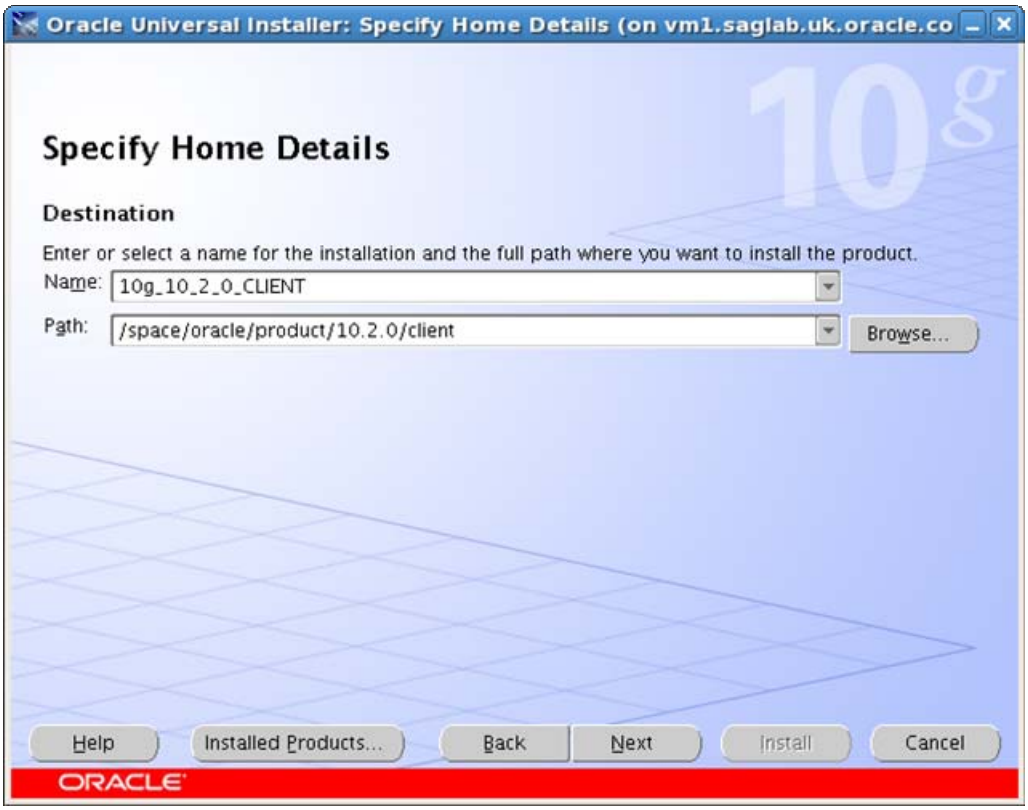
E.3.2 Installation Type



Click the **'Custom'** radio button.

Click Next.

E.3.3 Home Details

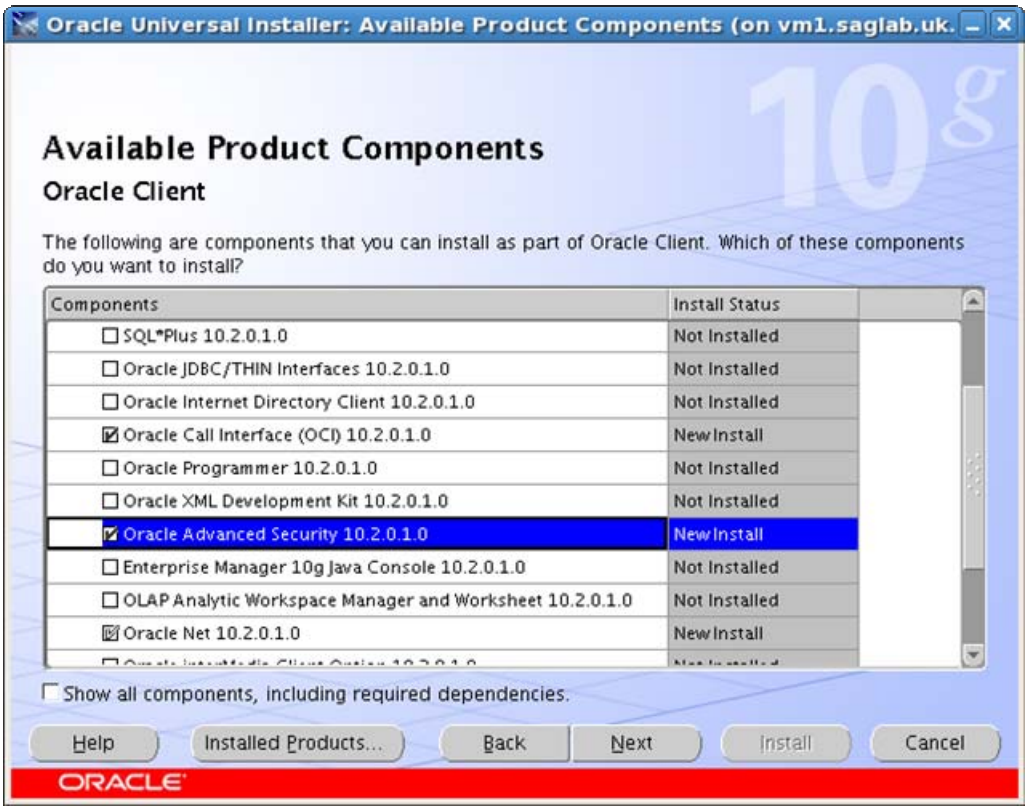


Enter the 'Installation Value' for the parameter **'Name'** specified in the pre-installation table matrix into the **'Name'** field.

Enter the 'Installation Value' for the parameter **'Path'** specified in the pre-installation table matrix into the **'Path'** field.

Click Next.

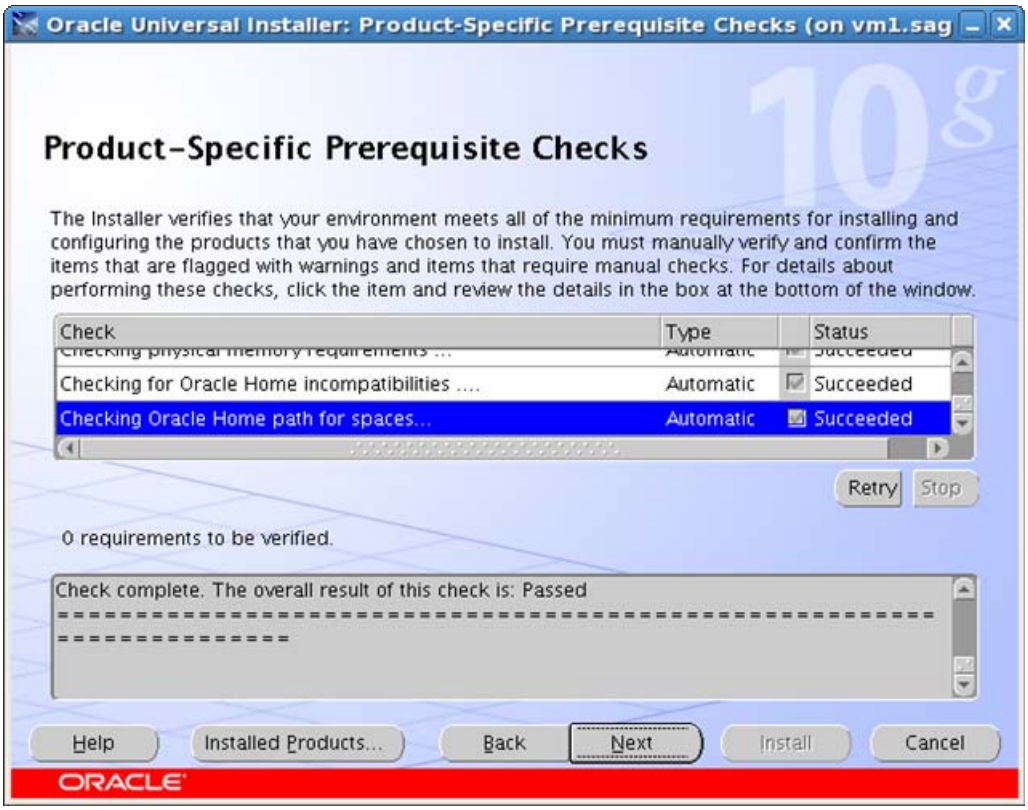
E.3.4 Product Components



Select the **'Oracle Call Interface (OCI) 10.2.0.1.0'** and **'Oracle Advanced Security 10.2.0.1.0'** components. The **'Oracle Net 10.2.0.1.0'** is a required component of Oracle Advanced Security and will also be selected.

Click Next.

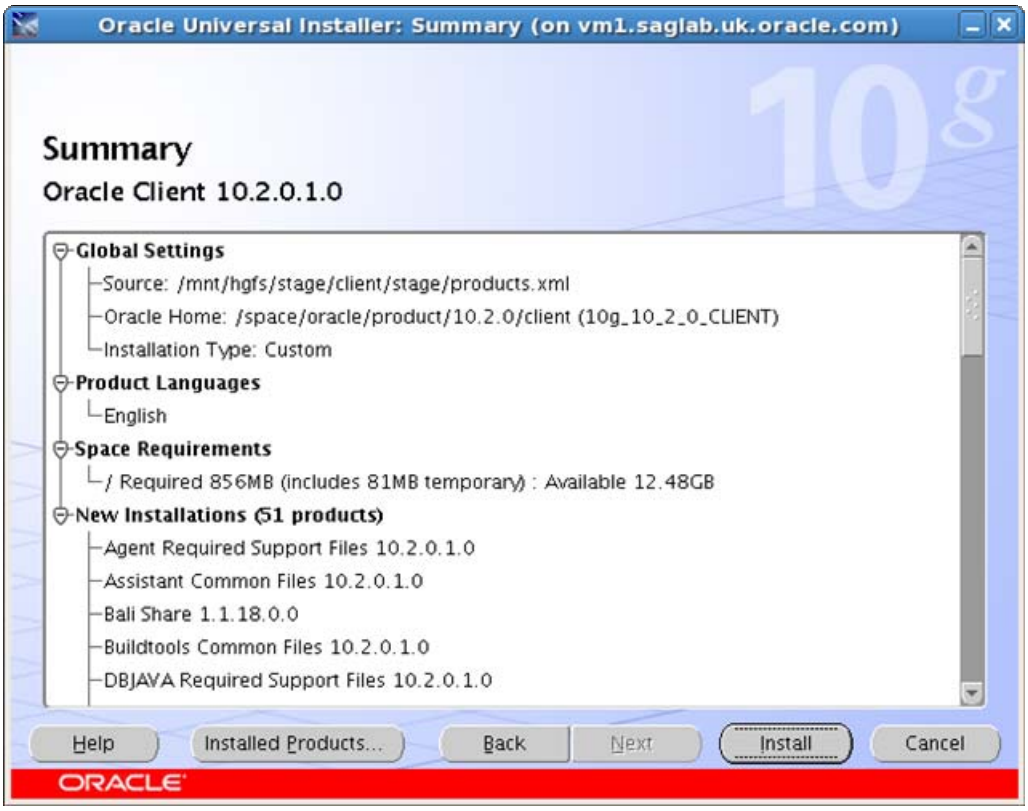
E.3.5 Prerequisite Checks



Make sure that there are **'0 requirements to be verified'**.

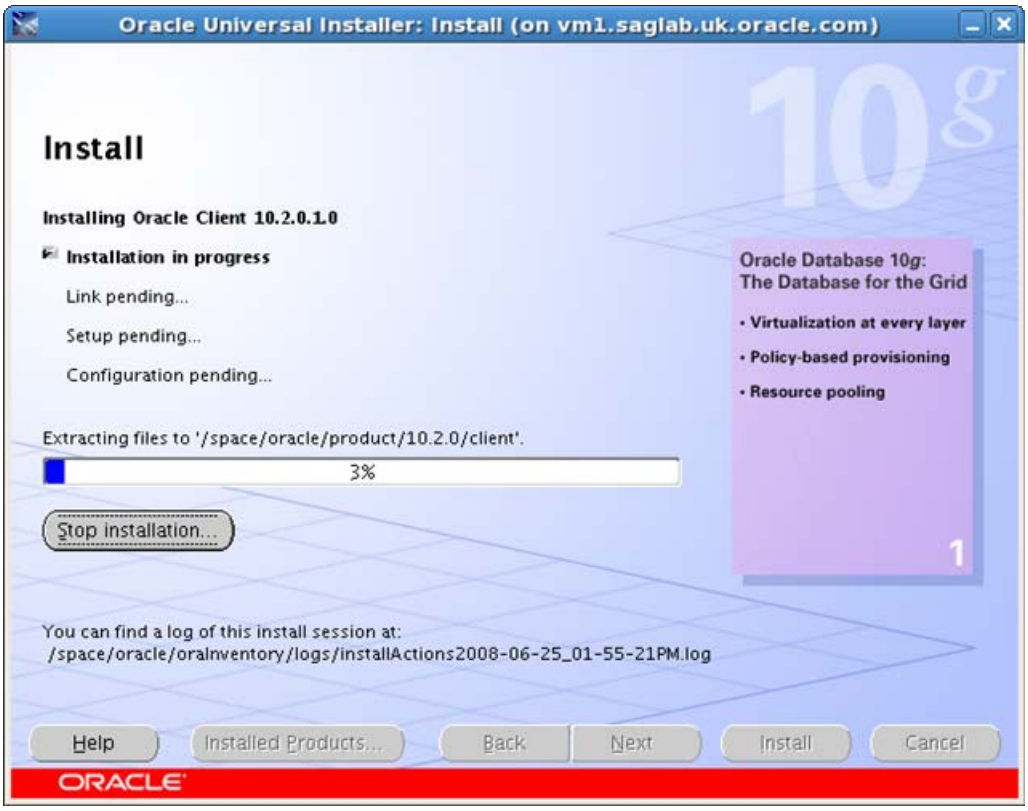
Click Next.

E.3.6 Summary

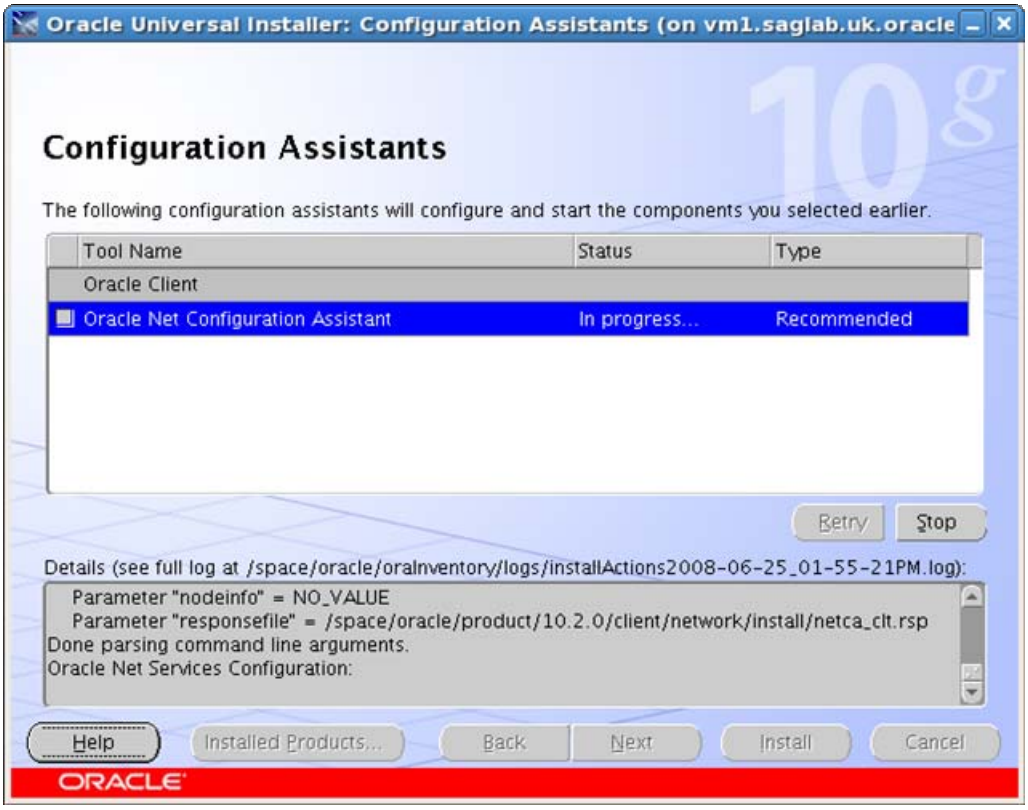


Click the **'Install'** radio button.

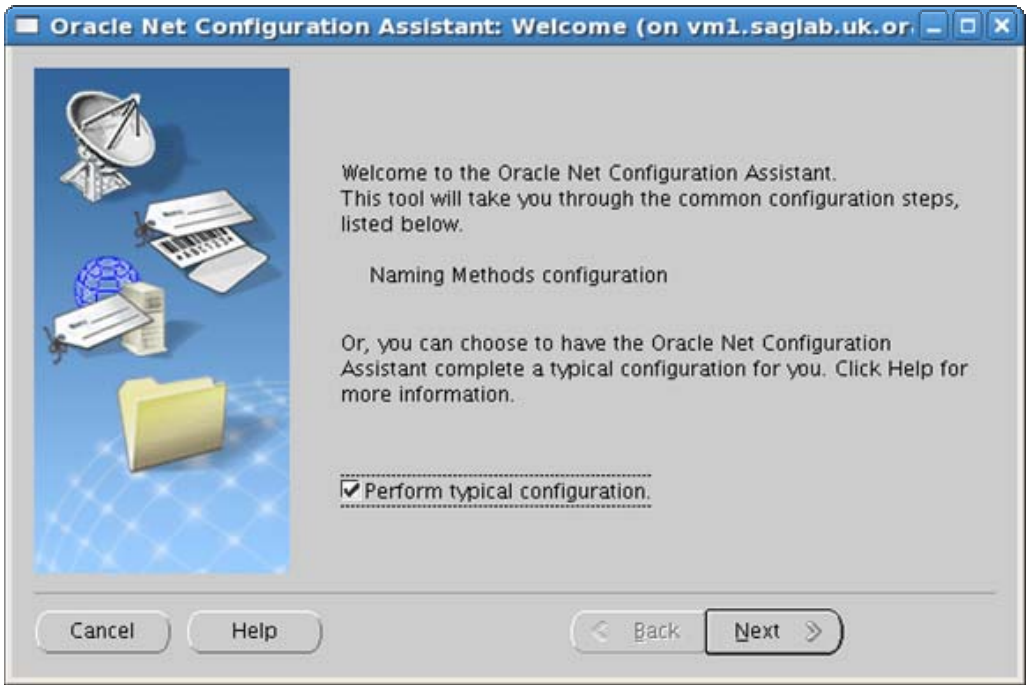
E.3.7 Install


Oracle Universal Installer: Install (on vm1.saglab.uk.oracle.com)
Install
Installing Oracle Client 10.2.0.1.0
Installation in progress
Link pending...
Setup pending...
Configuration pending...
Extracting files to '/space/oracle/product/10.2.0/client'.
3%
Stop installation...
Oracle Database 10g:
The Database for the Grid
• Virtualization at every layer
• Policy-based provisioning
• Resource pooling
You can find a log of this install session at:
/space/oracle/oraInventory/logs/installActions2008-06-25_01-55-21PM.log
Help
Installed Products...
Back
Next
Install
Cancel
ORACLE

E.3.8 Configuration Assistants



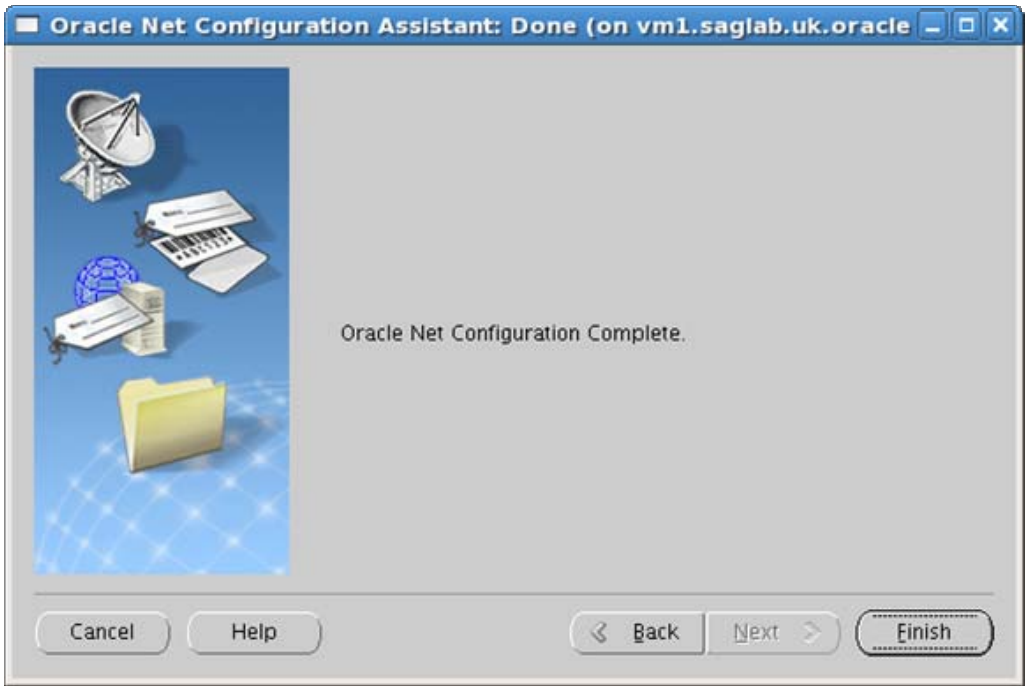
E.3.9 Net Configuration Assistants



Tick the **'Perform typical configuration'** check box.

Click Next.

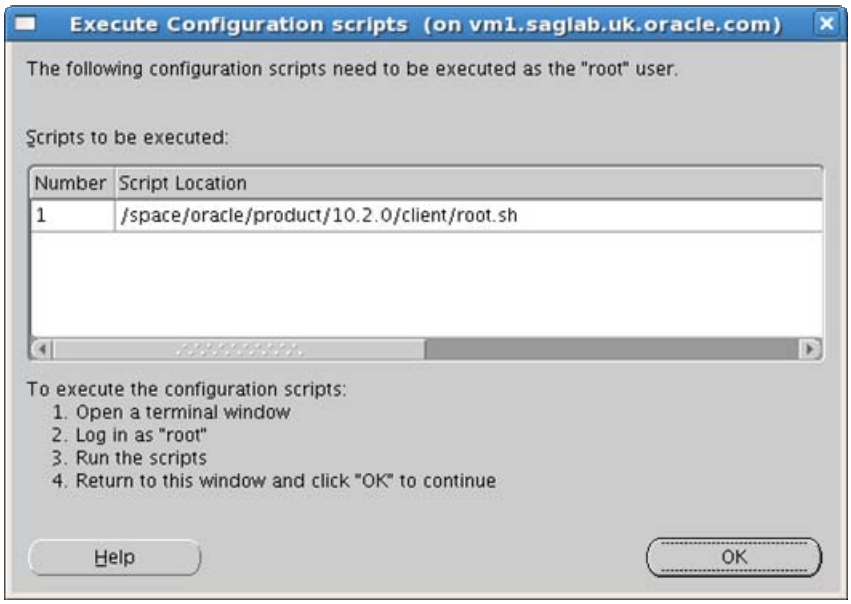
Click Next.



Click Finish.

E.3.10 Configuration Scripts

The OUI will request a configuration script to be executed as the `root` user:



As the `root` user run the `/space/oracle/product/10.2.0/client/root.sh` script. Do NOT overwrite existing files. The script will output the following:

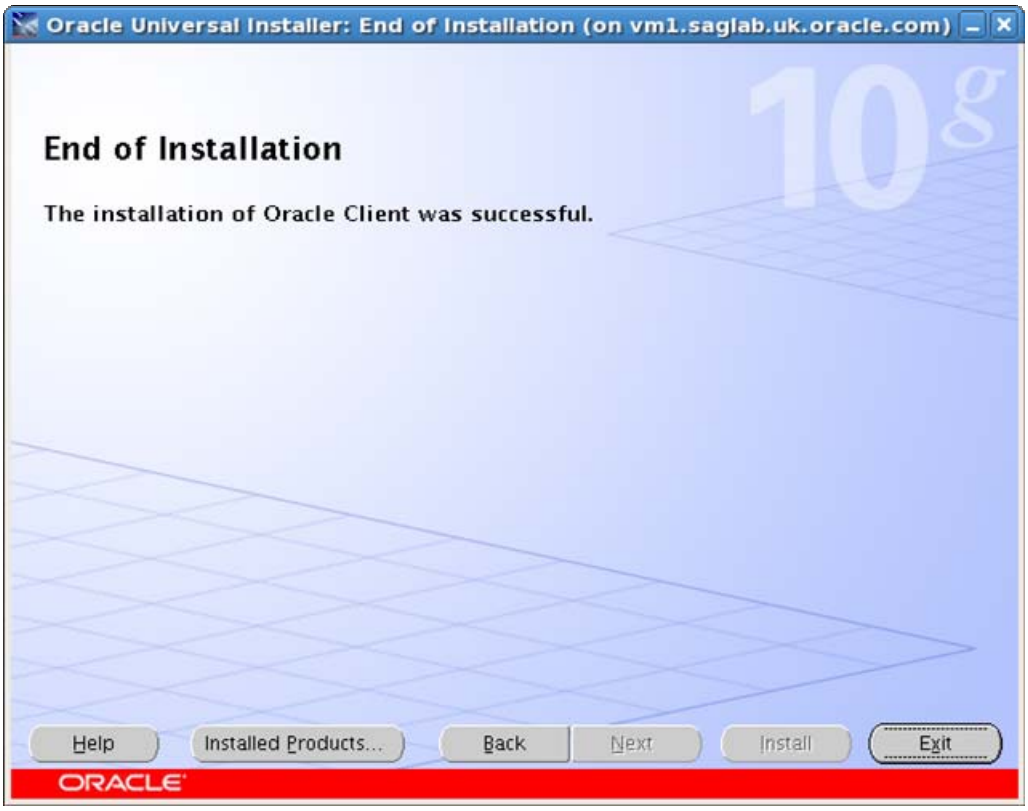
```
[root@vm1 oracle]# /space/oracle/product/10.2.0/client/root.sh
Running Oracle10 root.sh script...

The following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /space/oracle/product/10.2.0/client

Enter   the   full   pathname   of   the   local   bin   directory:
[/usr/local/bin]:
The file "dbhome" already exists in /usr/local/bin.  Overwrite
it? (y/n)
[n]:
The file "oraenv" already exists in /usr/local/bin.  Overwrite
it? (y/n)
[n]:
The file "coraenv" already exists in /usr/local/bin.  Overwrite
it? (y/n)
[n]:

Entries will be added to the /etc/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
[root@vm1 oracle]#
```

E.3.11 End of Installation



The installation of Oracle Database 10*g* Client Release 2 (10.2.0.1.0) is now complete.

E.4 Oracle Database 10*g* Client Release 2 (10.2.0.3.0) Installation

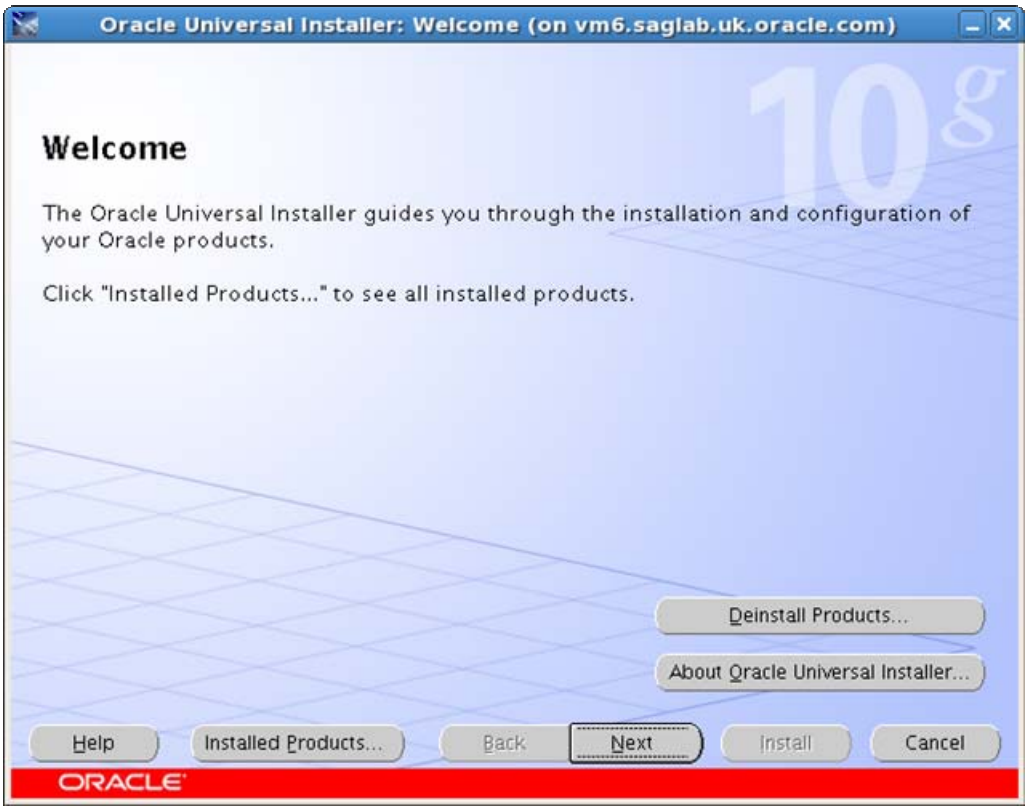
Login to the server machine as the `oracle` user and navigate to the directory where the issue media has been installed (in the Evaluated Configuration used to derive the screenshots given in this document, this was `/net/sagfs1t/vol/KITS/Software/Database/Linux/10.2.0.3/Linux/Disk1`

Start the Oracle Universal Installer as follows:

```
./runInstaller
```

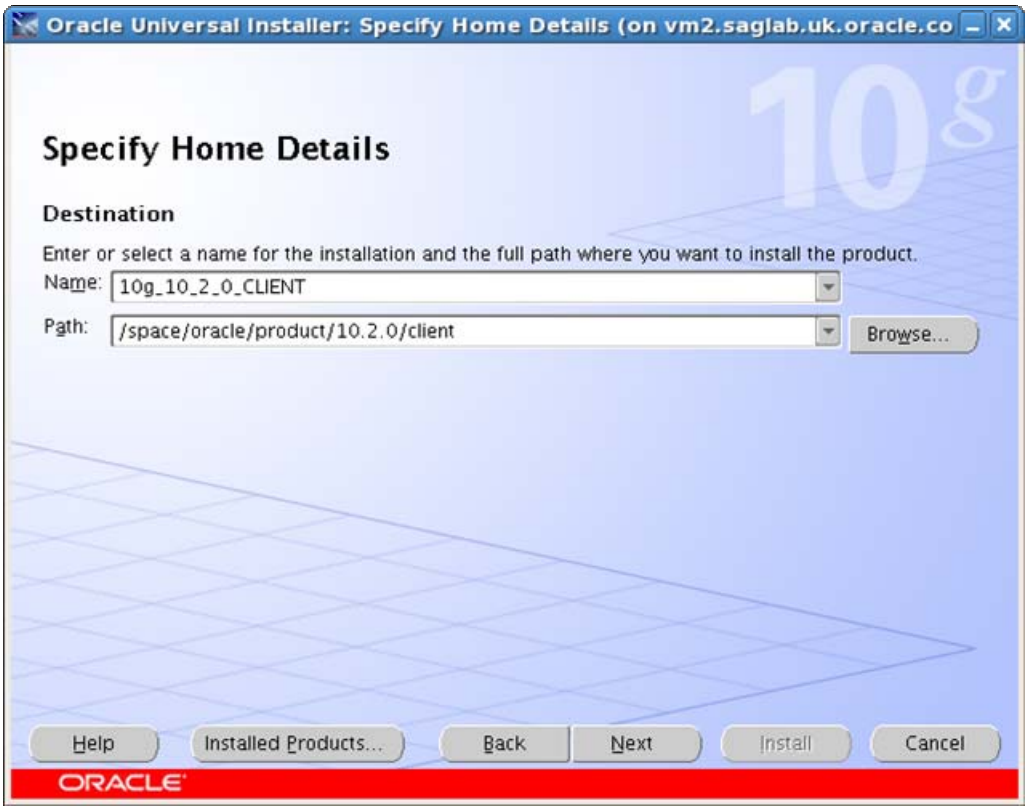
The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of Oracle Database 10*g* Client Release 2 (10.2.0.3.0).

E.4.1 Welcome Screen



Click Next.

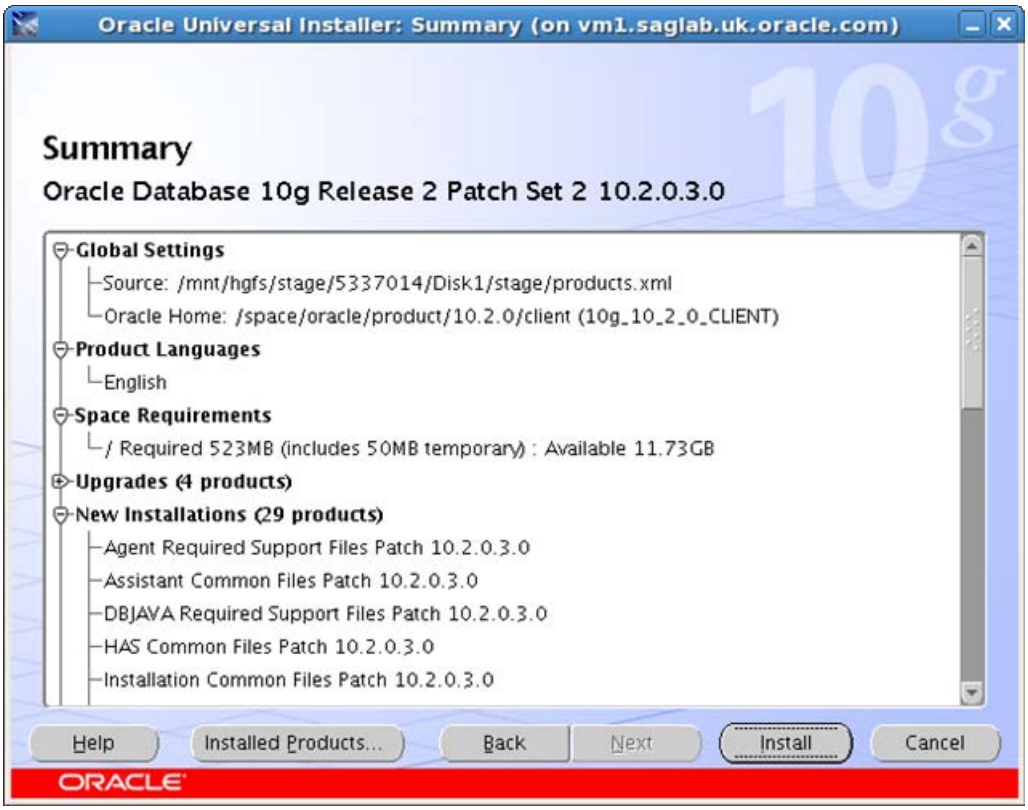
E.4.2 Home Details



Select the **'Name'** entered during the previous installation from the select list.

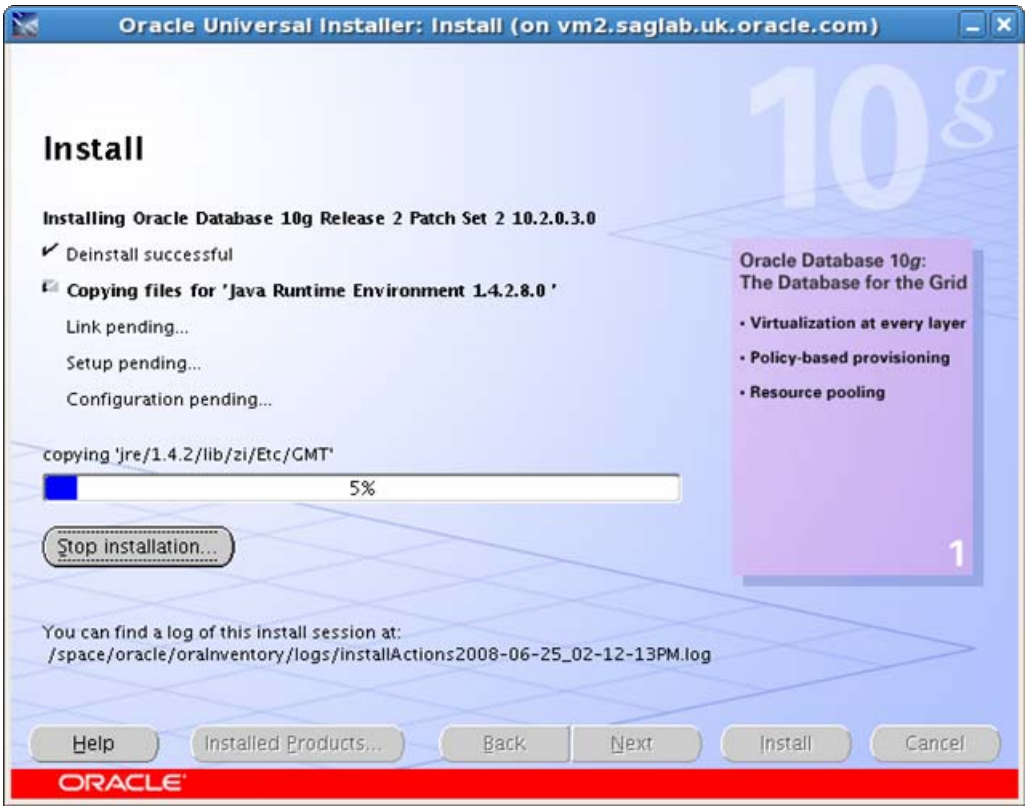
Click Next.

E.4.3 Summary

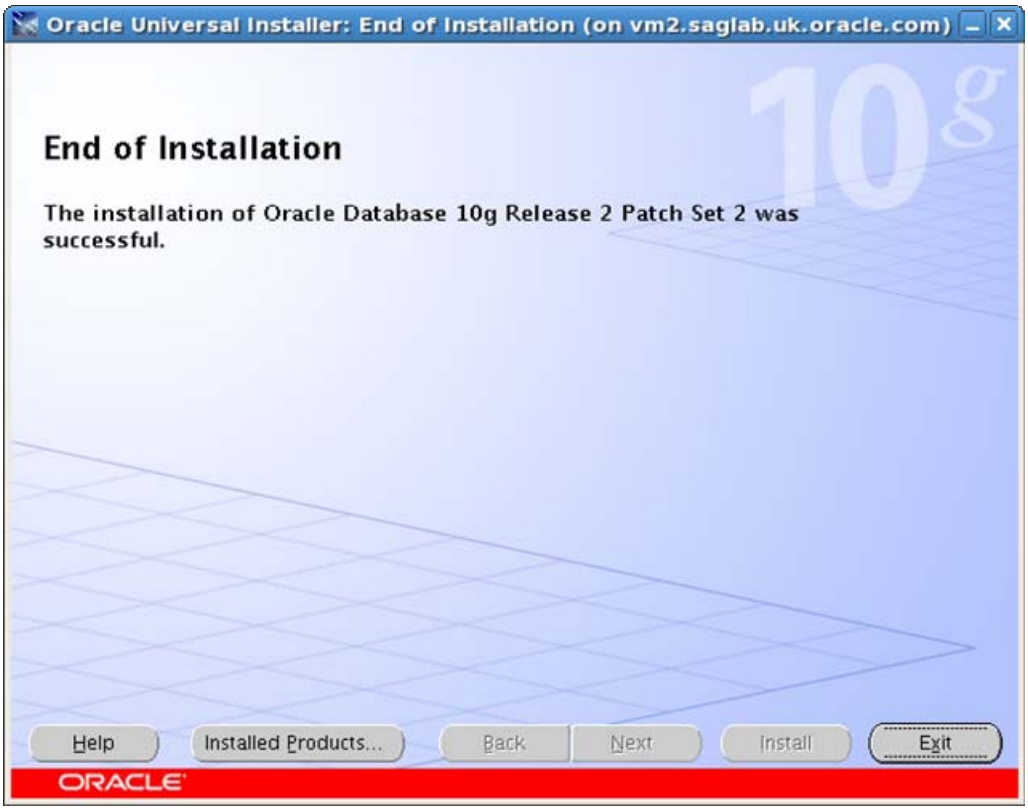


Click the **'Install'** button.

E.4.4 Install



E.4.5 End of Installation



The installation of Oracle Database 10*g* Client Release 2 (10.2.0.3.0) is now complete.

E.5 OPatch 10.2.0.4.3

OPatch is delivered through patch `6880880`. Issue the following commands:

```
export ORACLE_HOME=/space/oracle/product/10.2.0/client
export PATH=$ORACLE_HOME/OPatch:$PATH
cd $ORACLE_HOME
mv OPatch OPatch.102030
```

Extract the patch `p6880880_102000_Linux-x86-64.zip` to the client `ORACLE_HOME`:

```
unzip <path-to>/p6880880_102000_Linux-x86-64.zip
```

Verify that OPatch has been updated by issuing the command:

```
opatch version
```

The result should be:

```
Invoking OPatch 10.2.0.4.3

OPatch Version: 10.2.0.4.3

OPatch succeeded.
```

E.6 Patch 5240469

Patch 5240469 is required to correct a problem that will occur during the application of CPU April 2007[2]. It should be applied prior to the application of CPU April 2007. Change directory to the location of the extracted patch and apply it using OPatch by issuing the following command:

```
opatch apply
```

[2] Refer to MetaLink note 417319.1 for further information.

At the **'Is the local system ready for patching? [y/n]'** prompt enter: **'Y'**.

Oracle Configuration Manager (OCM) is bundled with OPatch and must be configured during the OPatch session:

At the **'stop displaying the license agreement'** prompt enter: **'q'**.

At the **'License Agreement'** prompt enter: **'Y'**.

At the **'Proxy specification'** prompt enter: **'NONE'**.

OCM will be installed and configured and patch `5240469` will be installed.

Successful patch application will be indicated by:

```
The local system has been patched and can be restarted.

OPatch succeeded.
```

E.7 Critical Patch Update April 2007

Change directory to the location of the extracted patch and issue:

```
opatch apply
```

At the **'Is the local system ready for patching? [y/n]'** prompt enter: **'Y'**.

Successful patch application will be indicated by:

```
Return Code = 0

The local system has been patched and can be restarted.

OPatch succeeded.
```

Annex F Oracle Database 10*g* Release 2 (10.2.0.3.0) Installation

[ECGDB] describes the steps required to install Oracle Database 10*g* Release 2 (10.2.0.3.0) in the evaluated configuration for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2), running on Oracle Enterprise Linux 4 Update 5 operating system.

This annex and [ECGDB] should be followed to install Oracle Database 10*g* Release 2 (10.2.0.3.0) on machine 3 in the following manner:

The operating system shall be installed according to annex C and replaces **[OS.1]** in [ECGDB, 3] when installing the operating system for Oracle Database 10*g* Release 2 (10.2.0.3.0). Although Oracle Enterprise Linux 4 Update 5 is not listed in [ECGDB, 3] it has met Common Criteria security requirements for assurance level EAL 4.

Perform the additional tasks from [ECGDB, 5.2.1.1].

Install Oracle Database 10*g* Release 2 (10.2.0.1.0) Enterprise Edition according to [ECGGB, 5.2.3].

Install Oracle Database 10*g* Release 2 (10.2.0.3.0) Enterprise Edition according to [ECGGB, 5.3].

Install OPatch according to Annex F.5.

Install patch 5240469 according to Annex F.6.

Install Critical Patch Update April 2007 according to [ECGDB, 5.4].

Setup the evaluated configuration of Oracle Database 10g Release 2 (10.2.0.3.0) according to [ECGDB, 5.5].

Annex G Oracle Internet Directory 10*g* (10.1.4.0.1) Installation

[ECGOID] describes the steps required to install Oracle Internet Directory 10*g* (10.1.4.0.1) in the evaluated configuration for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2), running on a Oracle Enterprise Linux 4 Update 5 operating system.

This annex and [ECGOID] should be followed to install Oracle Internet Directory 10*g* (10.1.4.0.1) on machine 4 with the following modifications:

The operating system shall be installed according to annex C and replaces **[DI.PRE-1]** in [ECGOID, 3] when installing the operating system for Oracle Internet Directory 10*g* (10.1.4.0.1).

[OS.2] – [OS.4] in annex C must be performed.

[DI.PRE-2] in [ECGOID, 3] must be performed. Use the following command to change the current values of the kernel parameters:

```
/sbin/sysctl –p
```

[OS.6] – [OS.8] in annex C replaces **[DI.PRE-3]** in [ECGOID, 3] when creating the operating system group and user required for the installation.

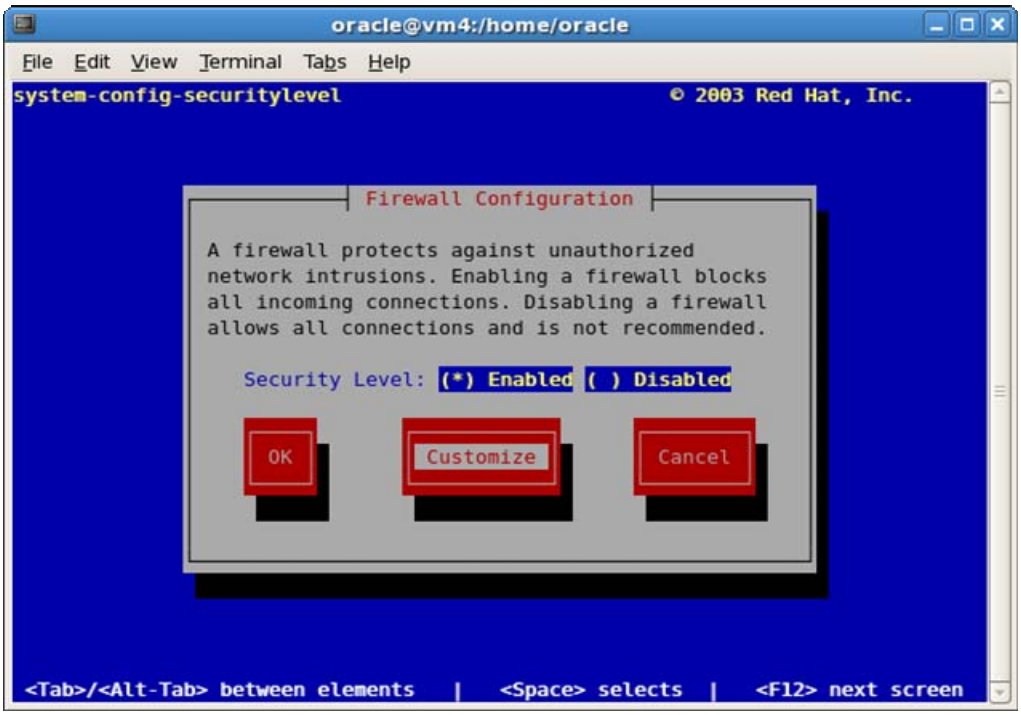
[DI.PRE-4] must be performed.

The following requirement replaces **[DI.PRE-5]** in [ECGOID, 3] when configuring the firewall on the server machine:

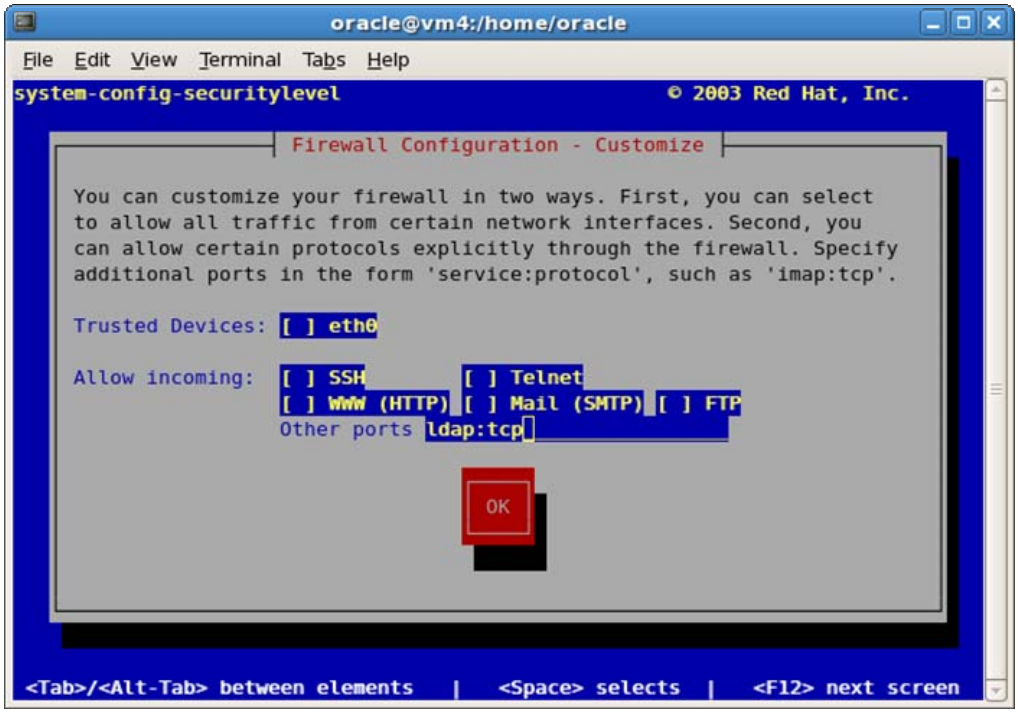
[DI.PRE-5x] As the `root` user, issue the following command to setup the firewall:

```
/usr/bin/system-config-securitylevel-tui
```

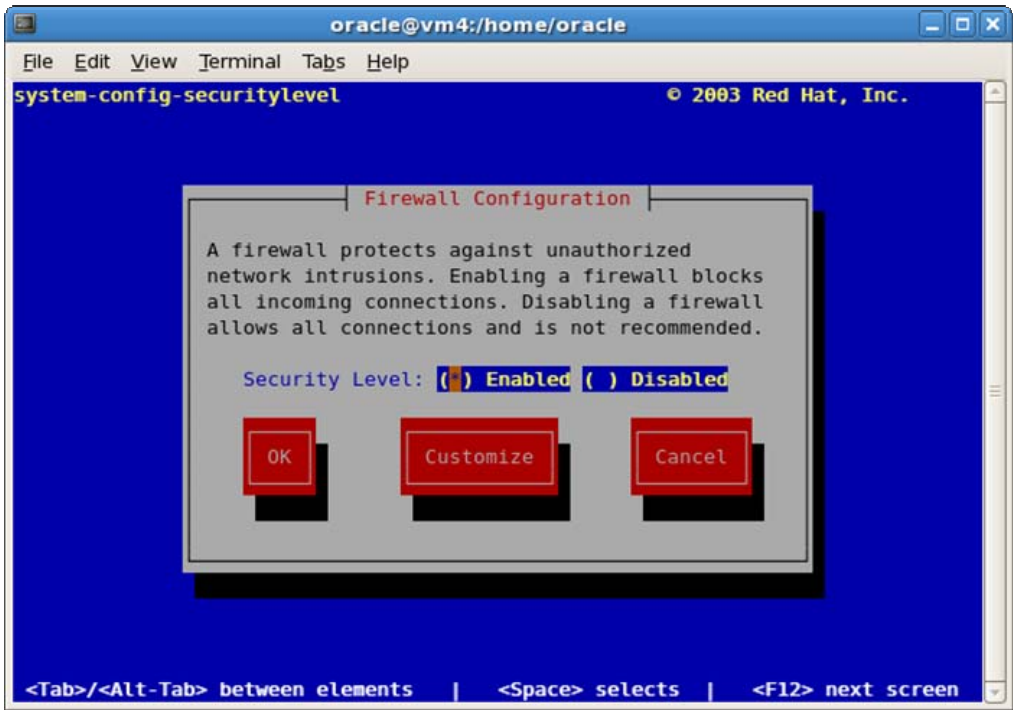
The command will open the Firewall Configuration application:



Enable the firewall by clicking the space bar. Tab to “Customize” and click Enter.



Tab to “Other ports” and enter “ldap:tcp”. Tab to “OK” and click Enter.



Tab to "OK" and click Enter.

Restart the firewall using the following command:

```
/sbin/service iptables restart
```

The following requirement must be performed prior to starting the Oracle Universal Installer in [ECGOIDIG, 2]:

Enable 32-bit emulation mode by running the following command:

```
linux32 bash
```

Start the Universal Installer according to [ECGOIDIG, 2]. The monitor pre-requisite check will fail as the `/usr/X11R6/bin/xdpyinfo` command is not available in the evaluated configuration of Oracle Enterprise Linux 4 Update 5. Ignore this error by entering **'Y'** when prompted to continue.

Setup the evaluated configuration of Oracle Internet Directory 10*g* (10.1.4.0.1) according to [ECGOID, 4].

The following requirement supplements **[DI.POST-4]** in [ECGOID, 3] when setting the password policy for OID:

[DI.POST-4x]The directory administrator must modify the password policy for each user that can access OID using the following LDIF file:

```
dn: cn=ECDPwdPolicy,cn=pwdPolicies,cn=Common,cn=Products,cn=OracleContext
changetype: modify
replace: pwdLockOut
pwdLockOut: 1

dn: cn=ECDPwdPolicy,cn=pwdPolicies,cn=Common,cn=Products,cn=OracleContext
changetype: modify
replace: pwdCheckSyntax
pwdCheckSyntax: 1
```

Annex H Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2) Installation

[ECGHTTP] describes the steps required to install Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2) in the evaluated configuration for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2), running on a Oracle Enterprise Linux 4 Update 5 operating system.

This annex and [ECGHTTP] should be followed to install Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2) on machine 5 with the following modifications:

The operating system shall be installed according to annex C and replaces **[HS.SS-1]** in [ECGHTTP, 3] when installing the operating system for Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2).

The following requirement replaces **[HS.PRE-1]** in [ECGHTTP, 4]. As the `root` user modify the following entries in the `/etc/sysctl.conf` file:

```
kernel.shmmax = 4294967295
fs.file-max = 206173
```

Use the following command to change the current values of the kernel parameters:

```
/sbin/sysctl –p
```

The following requirement must be performed prior to starting the Oracle Universal Installer in [ECGHTTP, 5]:

Enable 32-bit emulation mode by running the following command:

```
linux32 bash
```

As the `oracle` user set the `ORACLE_BASE` environment variable to specify the Oracle base directory:

```
export ORACLE_BASE=/space/oracle
```

Start the Universal Installer according to [ECGHTTP, 5]. The monitor pre-requisite check will fail as the `/usr/X11R6/bin/xdpyinfo` command is not available in the evaluated configuration of Oracle Enterprise Linux 4 Update 5. Ignore this error by entering **'Y'** when prompted to continue.

Setup the evaluated configuration of Oracle HTTP Server 10g Release 2 (10.1.2) according to [ECGHTTP, 4.2].

The following requirement replaces **[HS.POST-3]** in [ECGHTTP, 4.2]:

When setting the read access on web resources the following directive must be used:

```
<Directory />
   <LimitExcept POST GET>
      Deny from all
   </LimitExcept>
</Directory>
```

In place of:

```
<Directory />
   <LimitExcept GET>
      Deny from all
   </LimitExcept>
</Directory>
```

Annex I Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Installation

This chapter provides a step by step guide to installing Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406, running on an Oracle Enterprise Linux 4 Update 5 operating system.

I.1 Prerequisites

Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) installed according to Annex D.

Oracle Client 10g Release 2 (10.2.0.3.0) installed according to Annex F.

I.2 Input Parameters

The software installer will require the following input parameters for successful completion of the software installation. The values for these parameters should be gathered prior to starting the installation.

The following table should be completed with the insertion of the values to be used for the current installation into the 'Installation Value' column. The 'Example Value' column shows the values used in the example screenshots demonstrating the install process.

Pre-installation table matrix

Parameter Name	Installation Value	Example Value
BI Home		/space/oracle/product/OBIEE
BI Data Home		/space/oracle/oradata/OBIEE
AS Home		/space/oracle/product/10gAS/10g_J2EE
oc4jadmin Password		oracle1

I.3 Installation of Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406

Login to the server machine as the `oracle` user and navigate to the directory where the issue media has been installed (in the Evaluated Configuration used to derive the screenshots given in this document, this was /net/sagfs1t/vol/KITS/Software/BusinessIntelligence/10.1.3.3.2/Linux/RH_Linux/Server/Oracle_Business_Intelligence

Issue the following command to verify the machine is configured correctly:

```
$ ./UnixChk.sh /space/oracle/product/OBIEE
```

The script should return the following result:

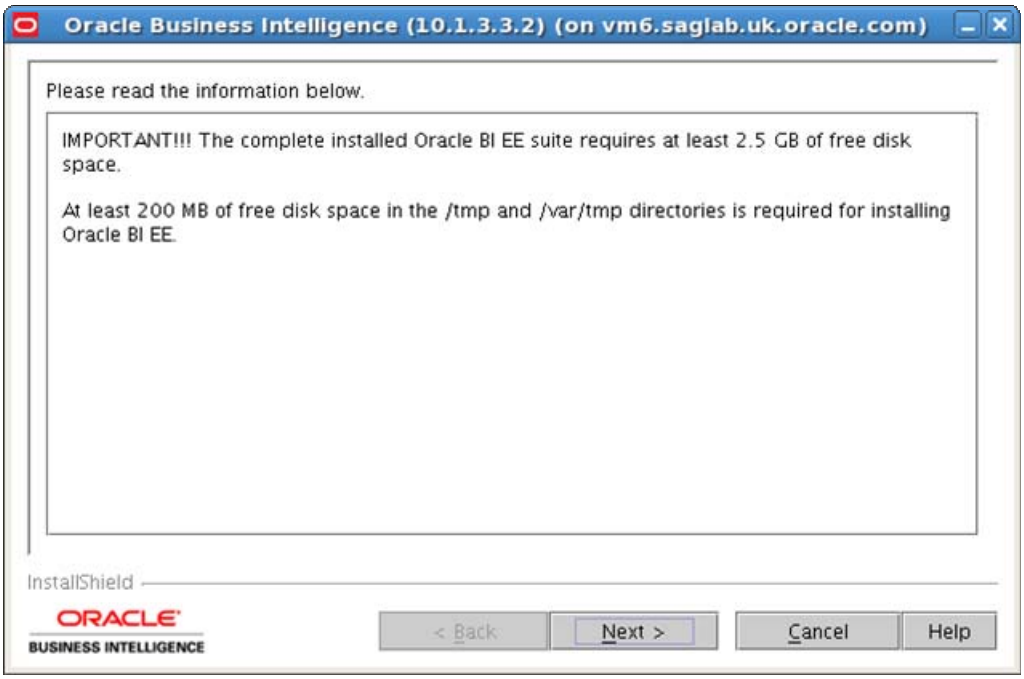
```
SUCCESS!! – This machine is configured for Oracle BI EE
10.1.3.3.2
```

If the pre-installation step is successful start the Oracle Business Intelligence (10.1.3.3.2) with Quick Fix 090406 Installer as follows:

```
$ ./setup.sh
```

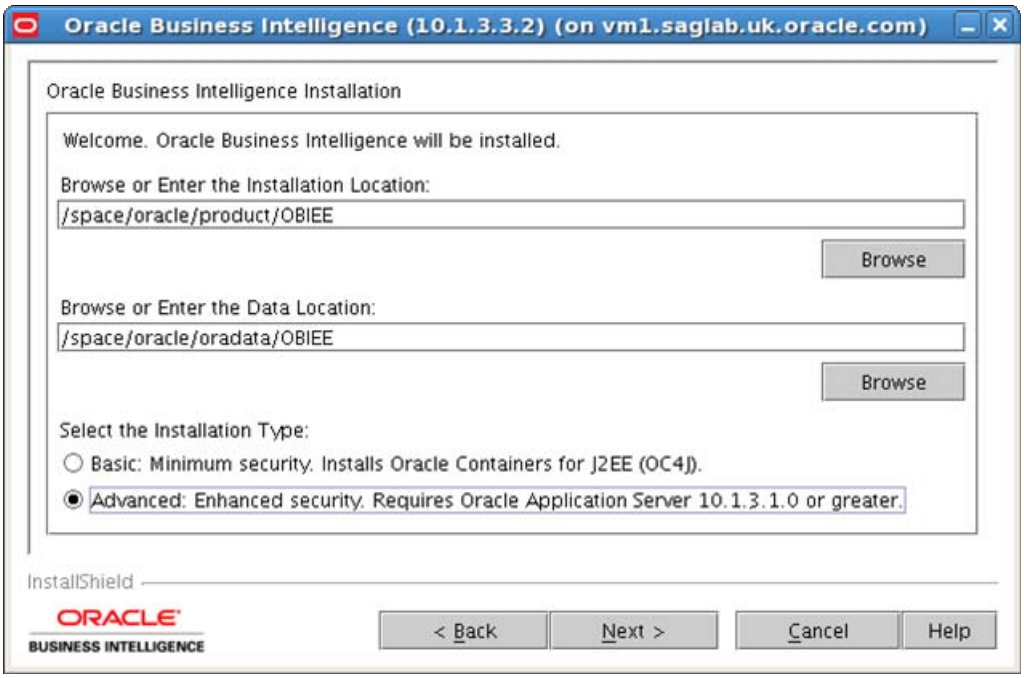
The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406.

I.3.1 Information



Click Next.

I.3.2 Installation Location



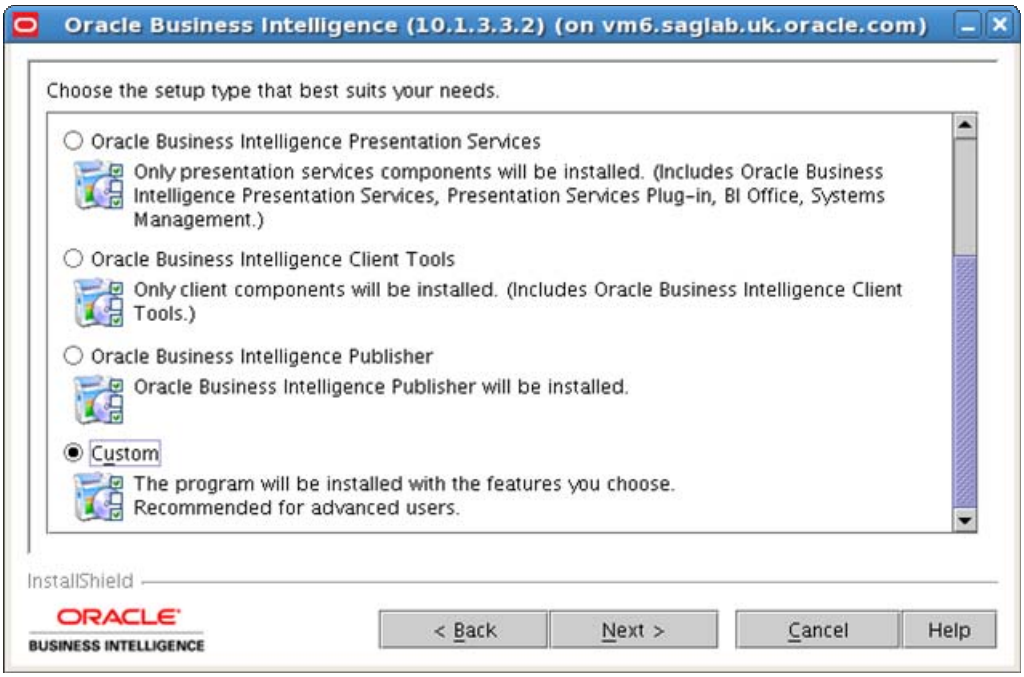
Enter the 'Installation Value' for the parameter **'BI Home'** specified in the pre-installation table matrix into the **'Installation Location'** field.

Enter the 'Installation Value' for the parameter **'BI Data Home'** specified in the pre-installation table matrix into the **'Data Location'** field.

Click the **'Advanced: Enhanced security. Requires Oracle Application Server 10.1.3.1.0 or greater'** radio button.

Click Next.

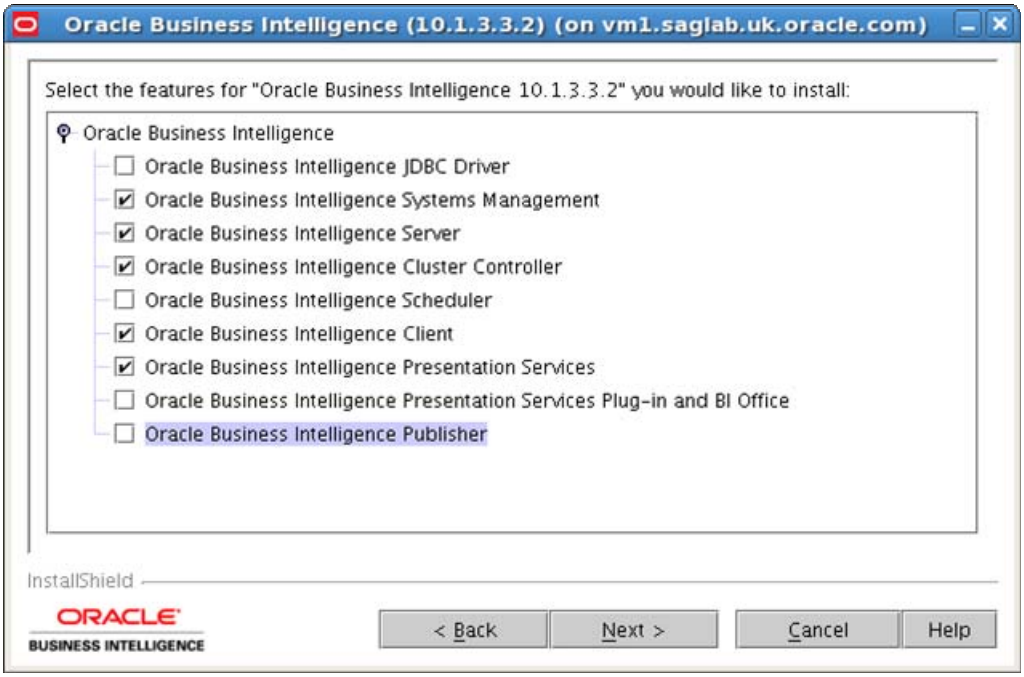
I.3.3 Product Components



Scroll down the page on the menu to the bottom. Click the **'Custom'** radio button.

Click Next.

I.3.4 Product Features

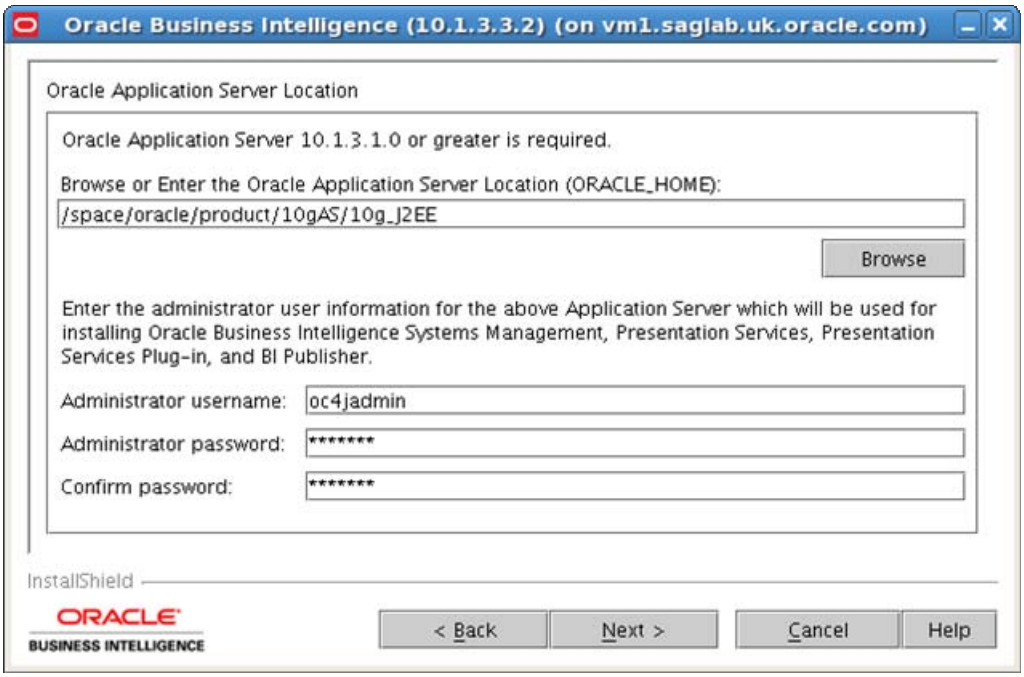


Deselect the following features:

- Oracle Business Intelligence JDBC Driver
- Oracle Business Intelligence Scheduler
- Oracle Business Intelligence Presentation Services Plug-in and BI Office
- Oracle Business Intelligence Publisher

Click Next.

I.3.5 Application Server Location



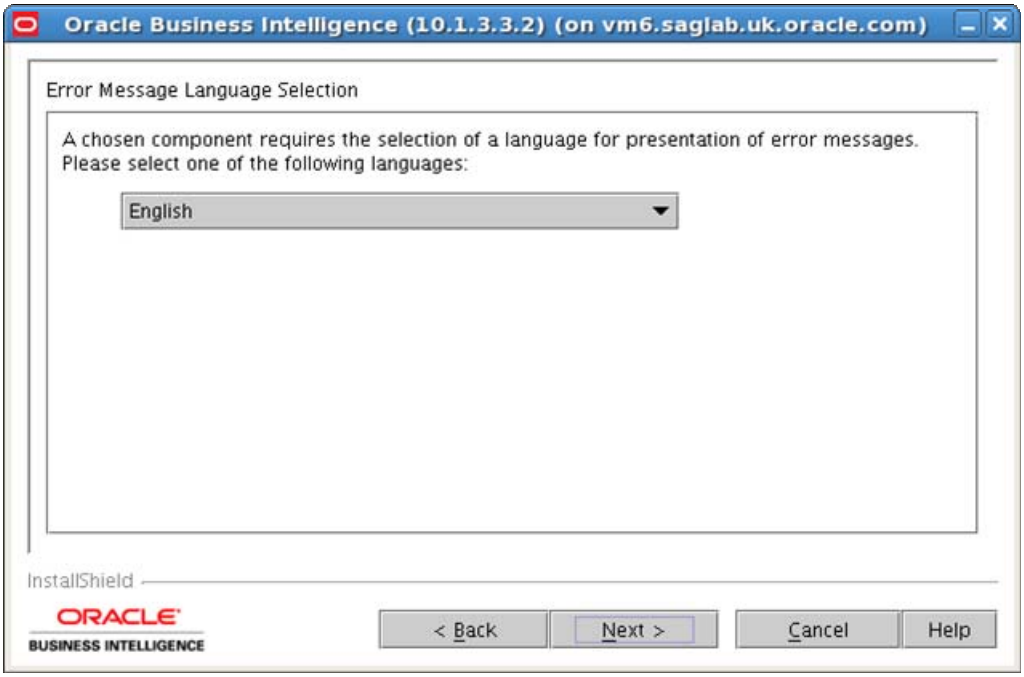
Enter the 'Installation Value' for the parameter **'AS Home'** specified in the pre-installation table matrix into the **'Oracle Application Server Location'** field.

Accept the default **'Administrator username'** of **'oc4jadmin'**.

Enter the 'Installation Value' for the parameter **'oc4jadmin Password'** specified in the pre-installation table matrix into the **'Administrator password'** and **'Confirm password'** fields.

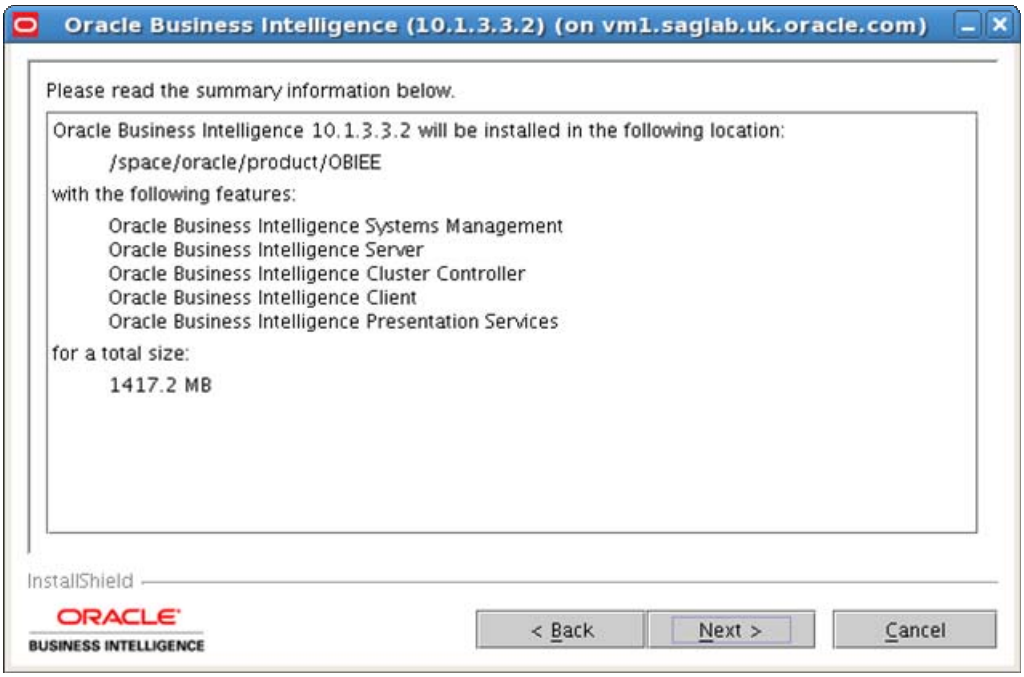
Click Next.

I.3.6 Error Message Language Selection



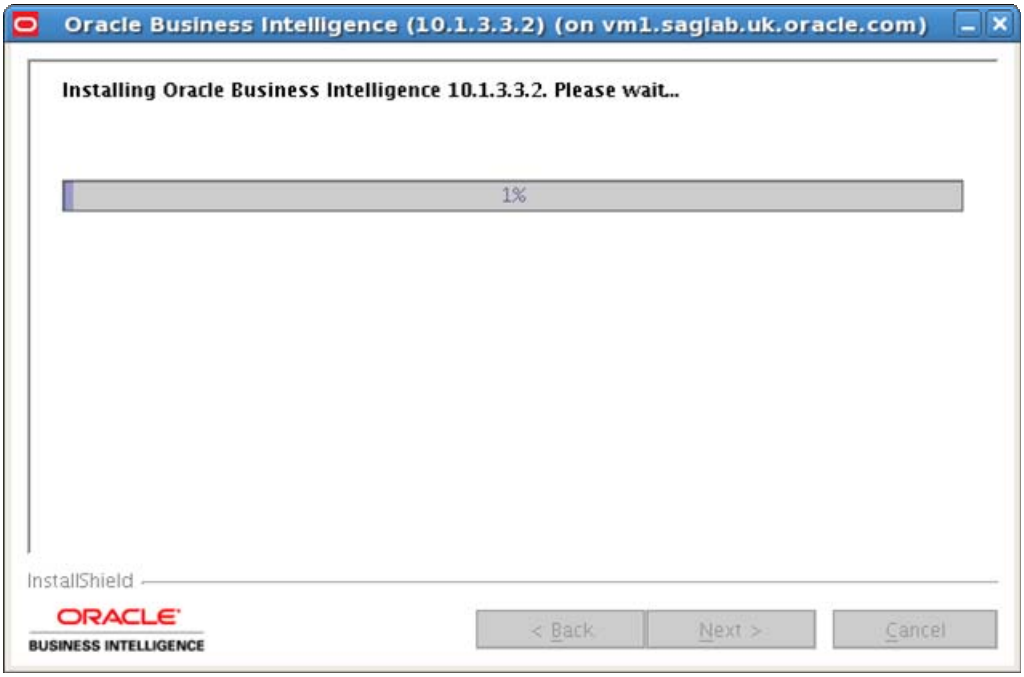
Click Next.

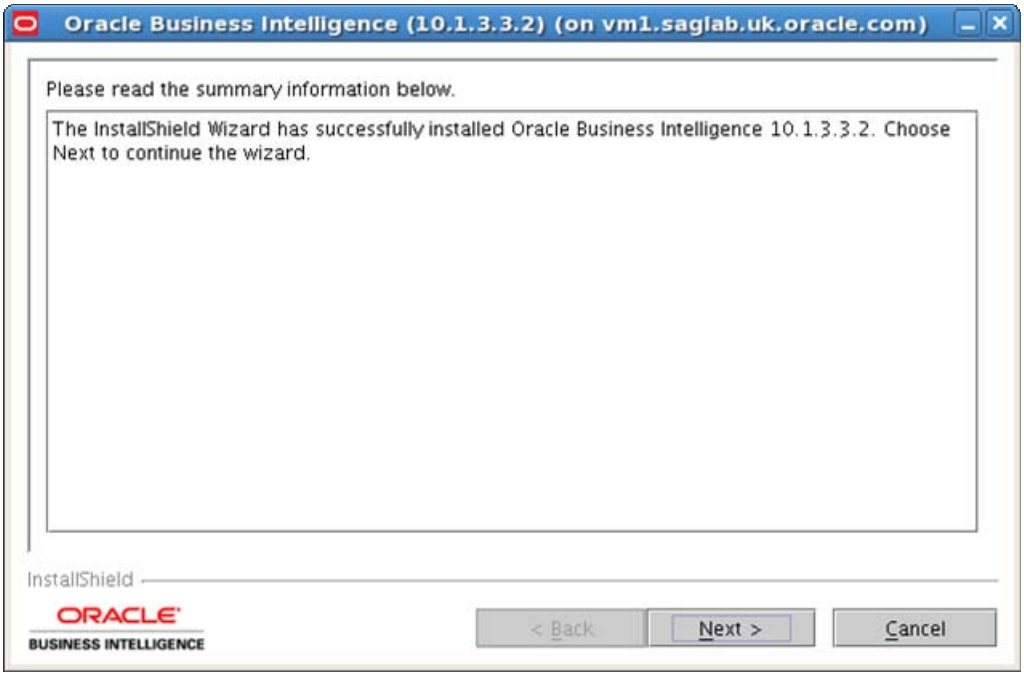
I.3.7 Summary



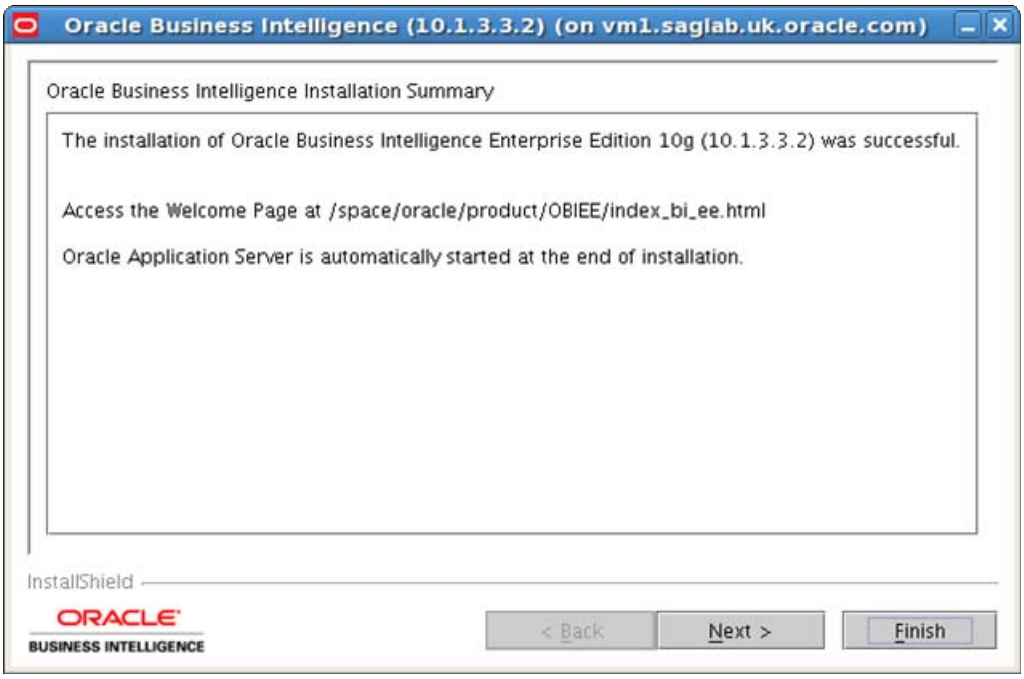
Click Next.

I.3.8 Installation





Click Next.



Click Finish.

The installation of Oracle Business Intelligence Enterprise Edition 10g (10.1.3.3.2) with Quick Fix 090406 is complete.

Annex J Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Presentation Services Plug-In Installation

This annex provides a step by step guide to installing the Presentation Services Plug-In in the evaluated configuration for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406, running on the Oracle Enterprise Linux Version 4 Update 5 operating system.

J.1 Prerequisites

Oracle SOA Suite 10*g* Release 3 (10.1.3.1.0) installed according to Annex D.

J.2 Input Parameters

The Presentation Services Plug-In software installer will require the following input parameters for successful completion of the software installation. The values for these parameters should be gathered prior to starting the installation.

The following table should be completed with the insertion of the values to be used for the current installation into the 'Installation Value' column. The 'Example Value' column shows the values used in the example screenshots demonstrating the install process.

Pre-installation table matrix

Parameter Name	Installation Value	Example Value
BI Home		/space/oracle/product/OBIEE
BI Data Home		/space/oracle/oradata/OBIEE
AS Home		/space/oracle/product/10gAS/10g_J2EE
Primary Host		obiee1.saglab.uk.oracle.com

J.3 Installation of Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406 Presentation Services Plug-In

Login to the server machine as the `oracle` user and navigate to the directory where the issue media has been installed (in the Evaluated Configuration used to derive the screenshots given in this document, this was /net/sagfs1t/vol/KITS/Software/BusinessIntelligence/10.1.3.3.2/Linux/RH_Linux/Server/Oracle_Business_Intelligence

Issue the following command to verify the machine is configured correctly:

```
$ ./UnixChk.sh /space/oracle/product/OBIEE
```

The script should return the following result:

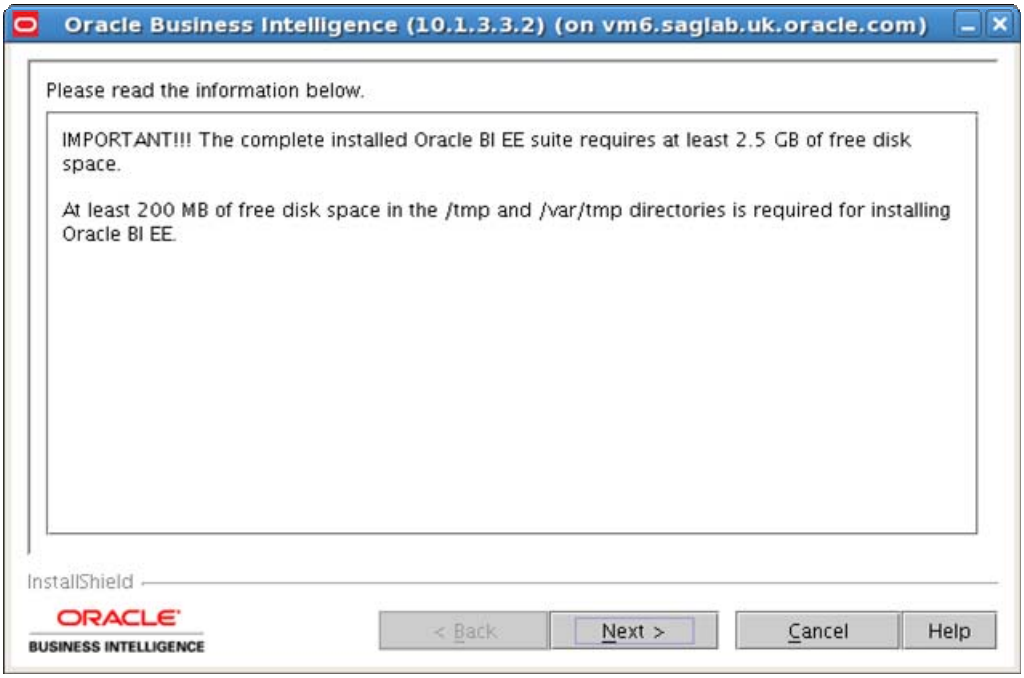
```
SUCCESS!! – This machine is configured for Oracle BI EE
10.1.3.3.2
```

If the pre-installation step is successful start the Oracle Business Intelligence (10.1.3.3.2) with Quick Fix 090406 Installer as follows:

```
$ ./setup.sh
```

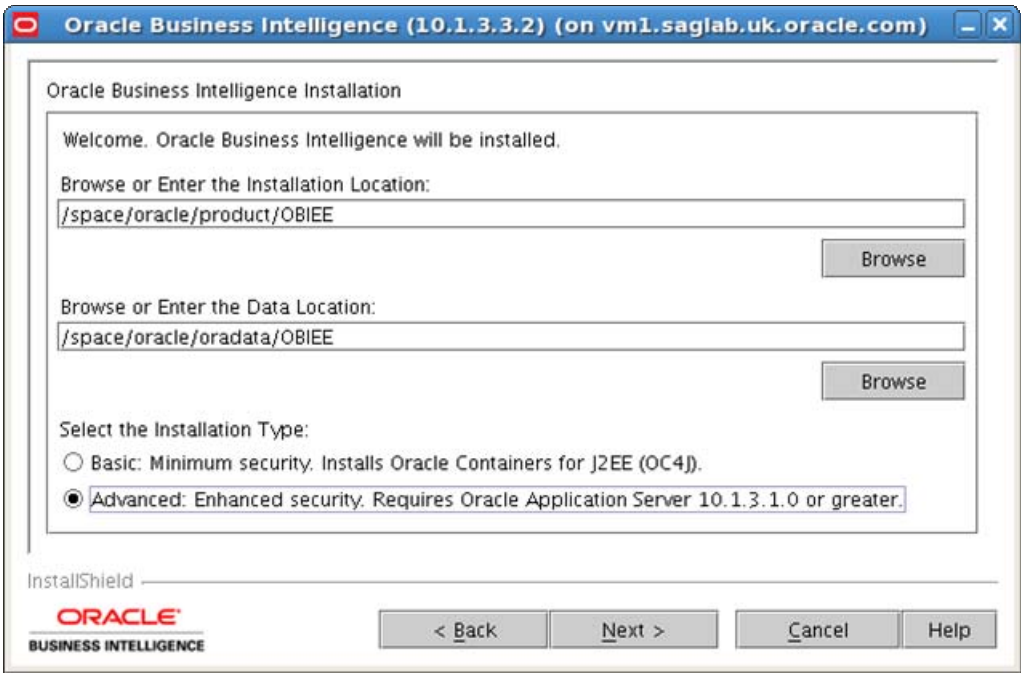
The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406.

J.3.1 Information



Click Next.

J.3.2 Installation Location



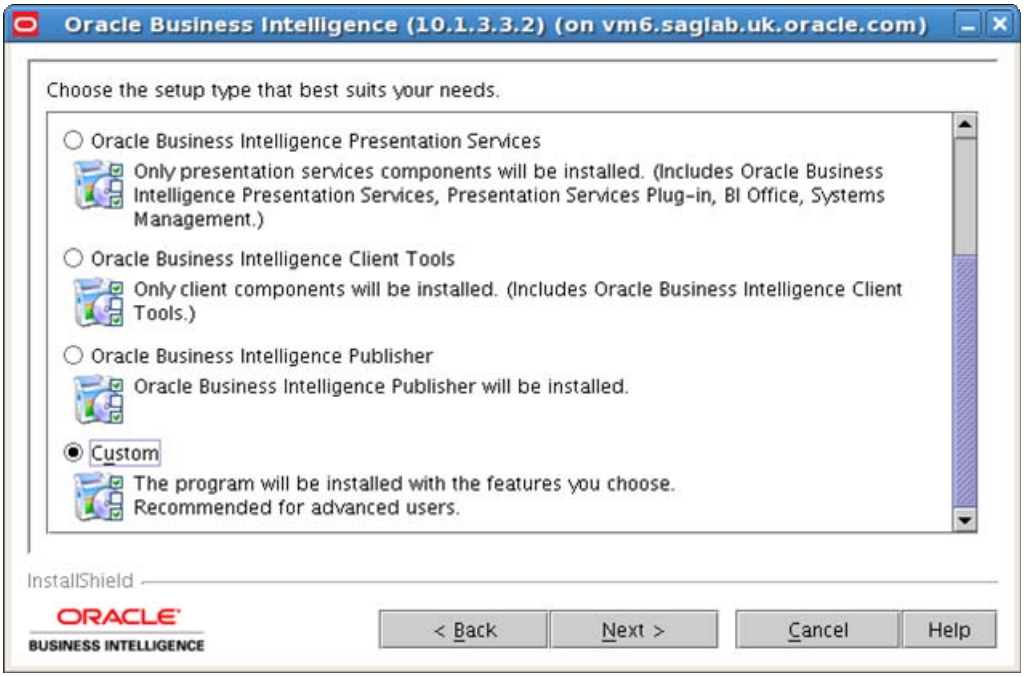
Enter the 'Installation Value' for the parameter **'BI Home'** specified in the pre-installation table matrix into the **'Installation Location'** field.

Enter the 'Installation Value' for the parameter **'BI Data Home'** specified in the pre-installation table matrix into the **'Data Location'** field.

Click the **'Advanced: Enhanced security. Requires Oracle Application Server 10.1.3.1.0 or greater'** radio button.

Click Next.

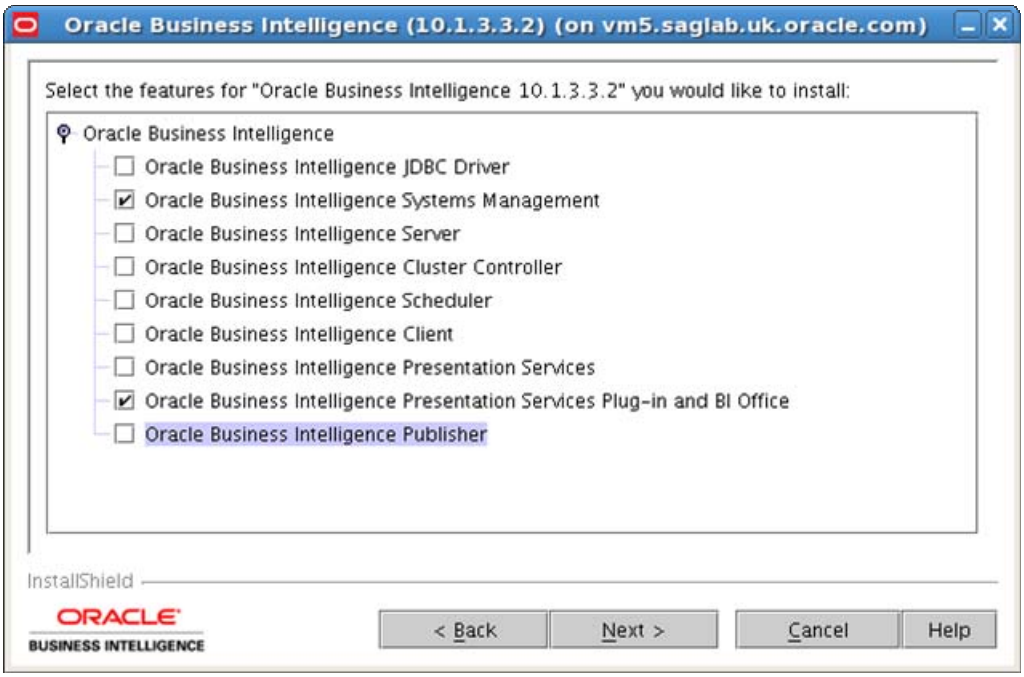
J.3.3 Product Components



Scroll down the menu until you reach the bottom. Click the **'Custom'** radio button.

Click Next.

J.3.4 Product Features

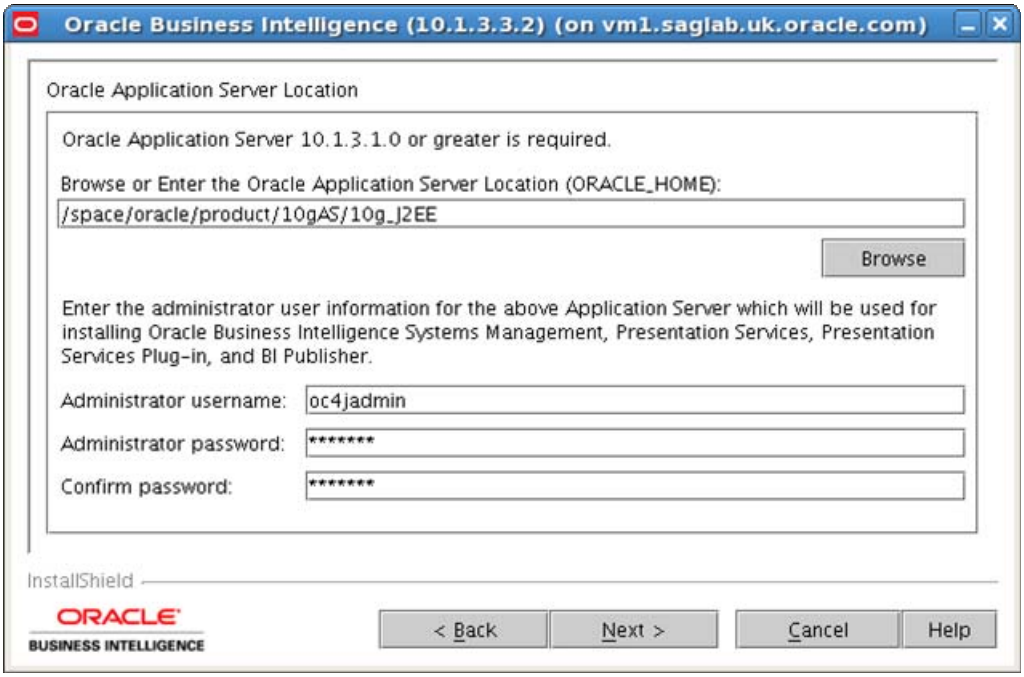


Deselect the following features:

- Oracle Business Intelligence JDBC Driver
- Oracle Business Intelligence Server
- Oracle Business Intelligence Cluster Controller
- Oracle Business Intelligence Scheduler
- Oracle Business Intelligence Client
- Oracle Business Intelligence Presentation Services
- Oracle Business Intelligence Publisher

Click Next.

J.3.5 Oracle Application Server Location



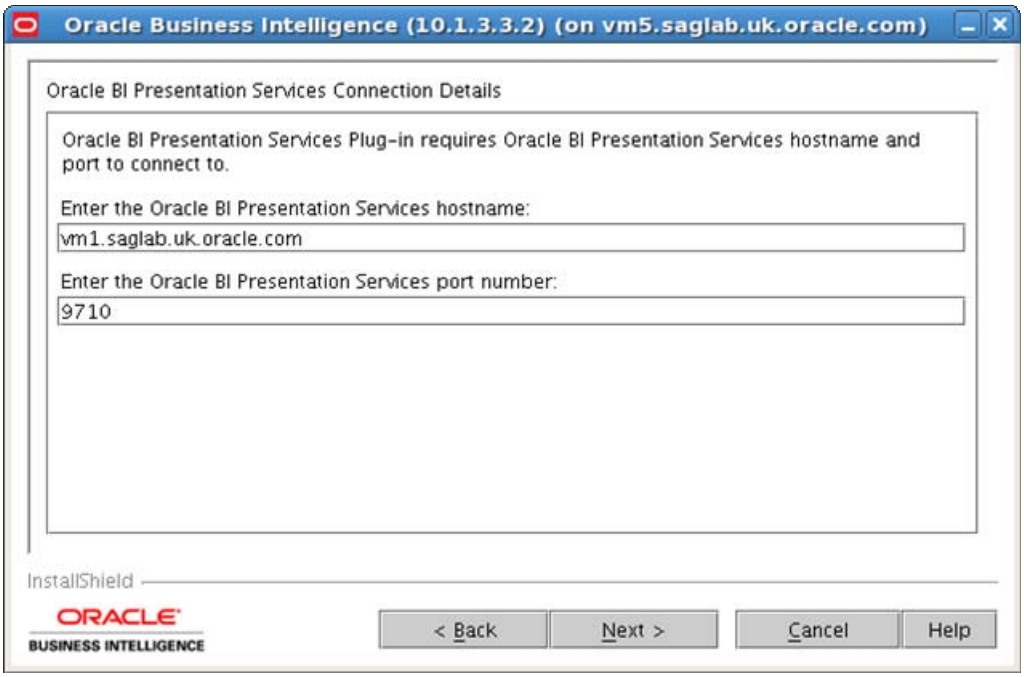
Enter the 'Installation Value' for the parameter **'AS Home'** specified in the pre-installation table matrix into the **'Oracle Application Server Location'** field.

Accept the default **'Administrator username'** of **'oc4jadmin'**.

Enter the 'Installation Value' for the parameter **'oc4jadmin Password'** specified in the pre-installation table matrix into the **'Administrator password'** and **'Confirm password'** fields.

Click Next.

J.3.6 Presentation Services Connection Details

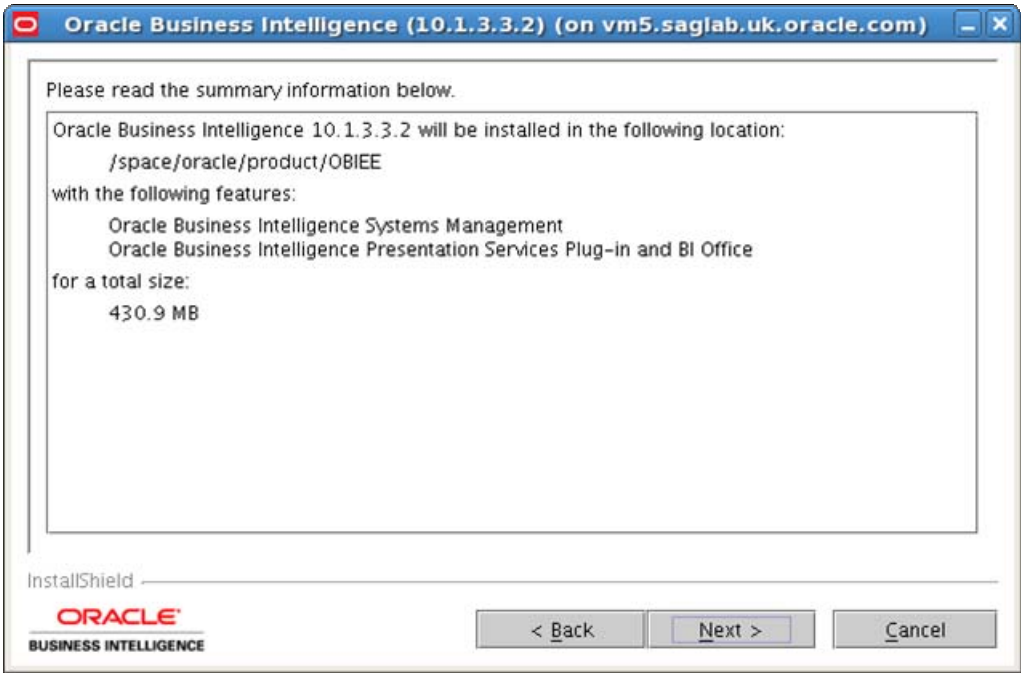


Enter the 'Installation Value' for the parameter **'Primary Host'** specified in the pre-installation table matrix into the **'Hostname'** field.

Accept the default Oracle BI Presentation Services port number.

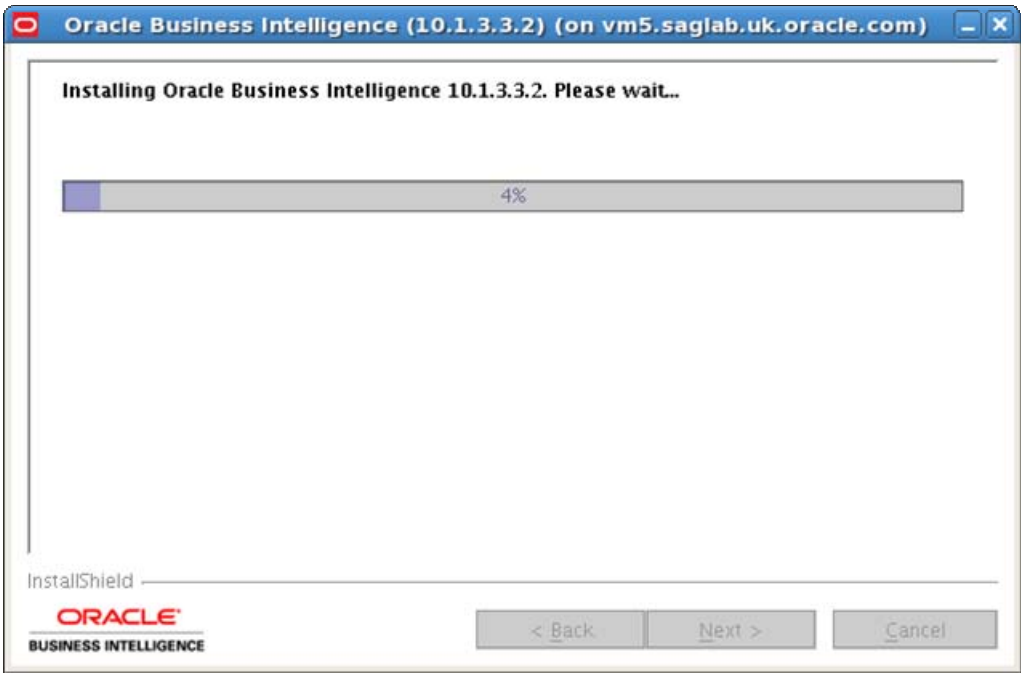
Click Next.

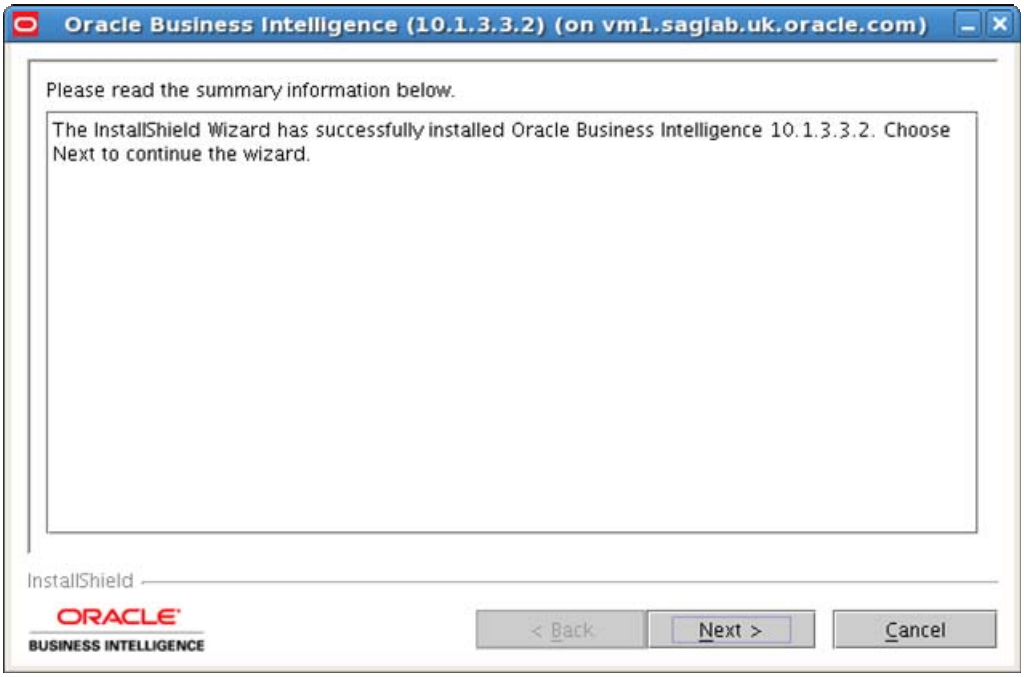
J.3.7 Summary



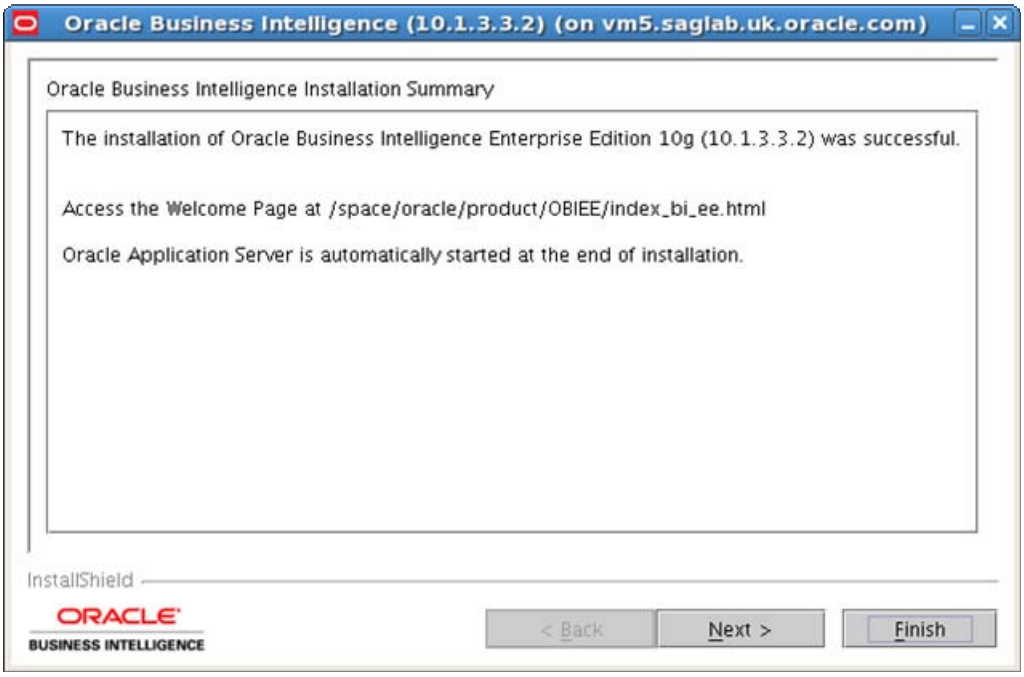
Click Next.

J.3.8 Installation





Click Next.



Click Finish.

The installation of Oracle Business Intelligence Presentation Services Plug-In 10g (10.1.3.3.2) with Quick Fix 090406 is complete.

Annex K J2SE Development Kit 5.0 Update 16

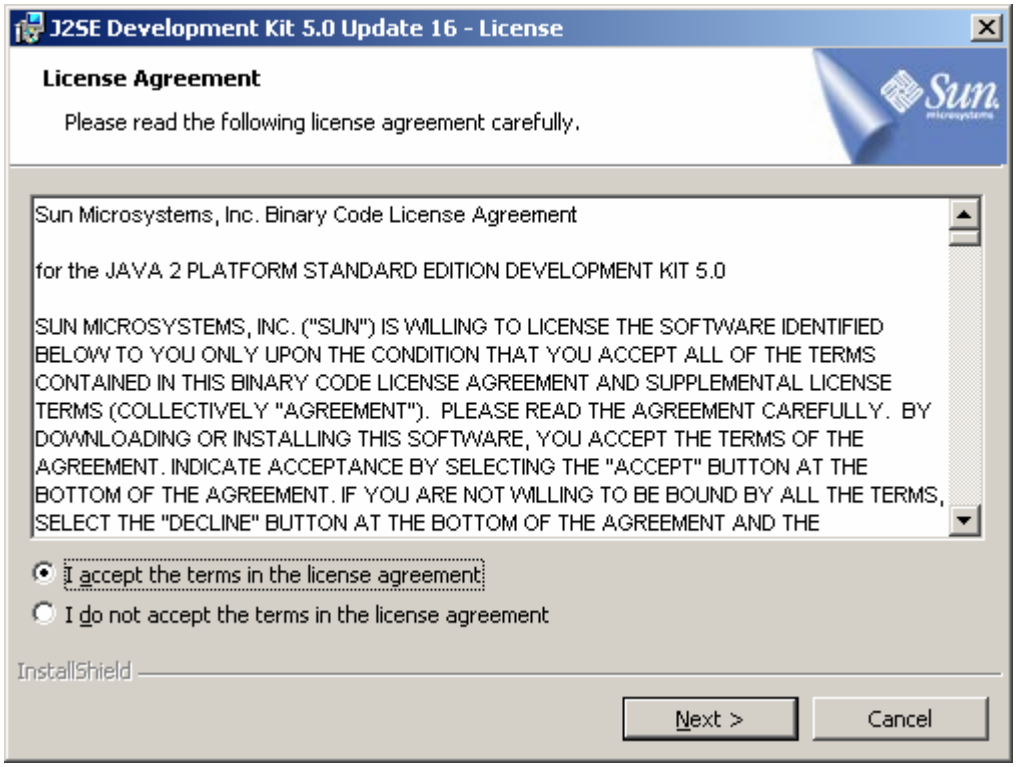
K.1 Prerequisites

None.

K.2 Installation of JDK 5 Update 16

Double-click on the jdk-1_5_0_16-windows-i586-p.exe file.

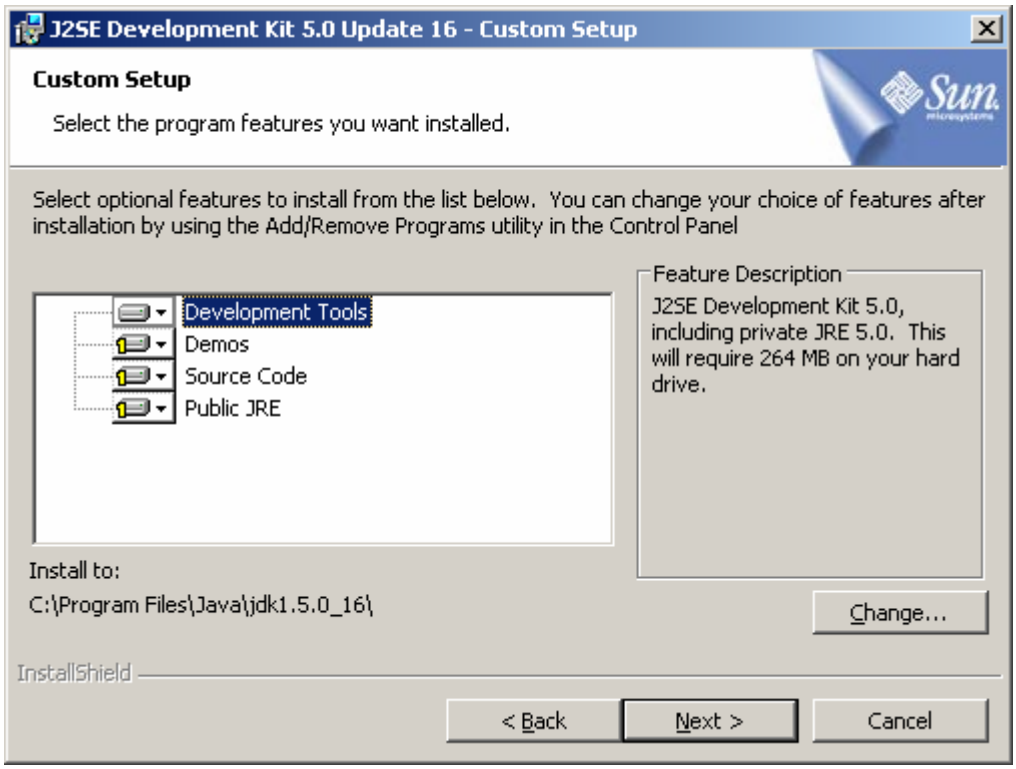
K.2.1 License Agreement



Click the **'I accept the terms in the license agreement'** radio button.

Click Next.

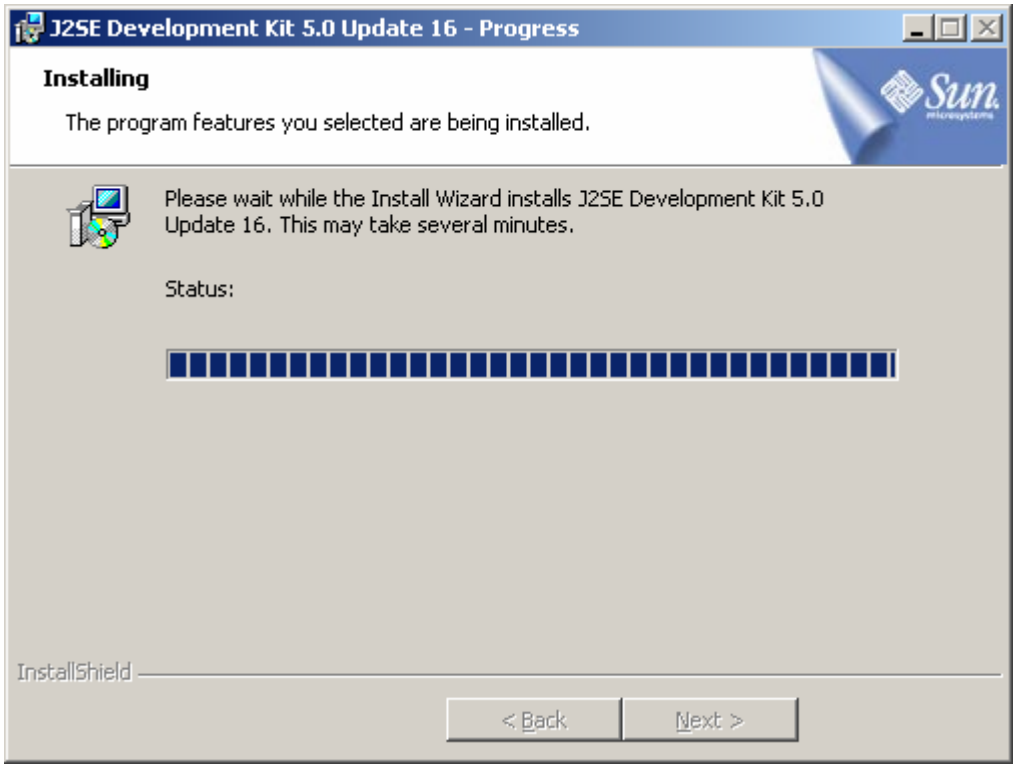
K.2.2 Custom Setup



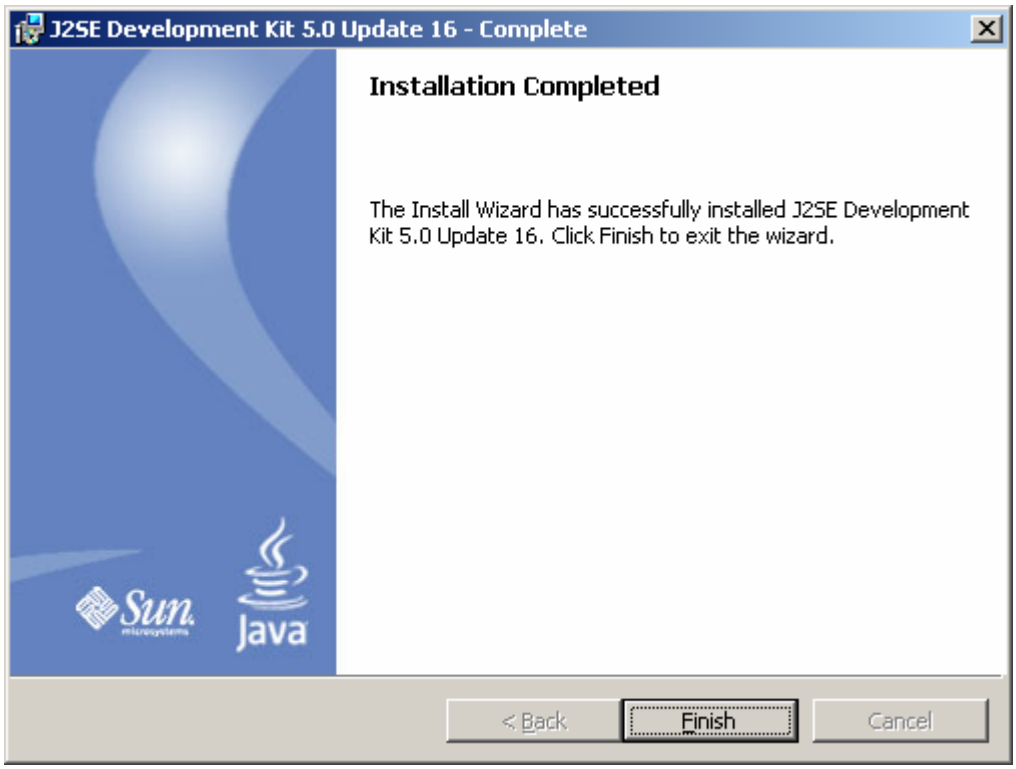
Make sure only **'Development Tools'** are installed.

Click Next.

K.2.3 Progress



K.2.4 Installation Complete



Click Finish.

The installation of J2SE Development Kit 5.0 Update 16 is now complete.

Annex L Oracle Database 10*g* Client Release 2 (10.2.0.3.0) Installation

This annex provides a step by step guide to installing Oracle Database 10*g* Client Release 2 (10.2.0.3.0), running on a Microsoft Windows XP operating system.

L.1 Prerequisites

None.

L.2 Input Parameters

The software installer will require the following input parameters for successful completion of the software installation. The values for these parameters should be gathered prior to starting the installation.

The following table should be completed with the insertion of the values to be used for the current installation into the 'Installation Value' column. The 'Example Value' column shows the values used in the example screenshots demonstrating the install process.

Pre-installation table matrix

Parameter Name	Installation Value	Example Value
Home		10g_10_2_0_CLIENT
Path		C:\oracle\product\10.2.0\client

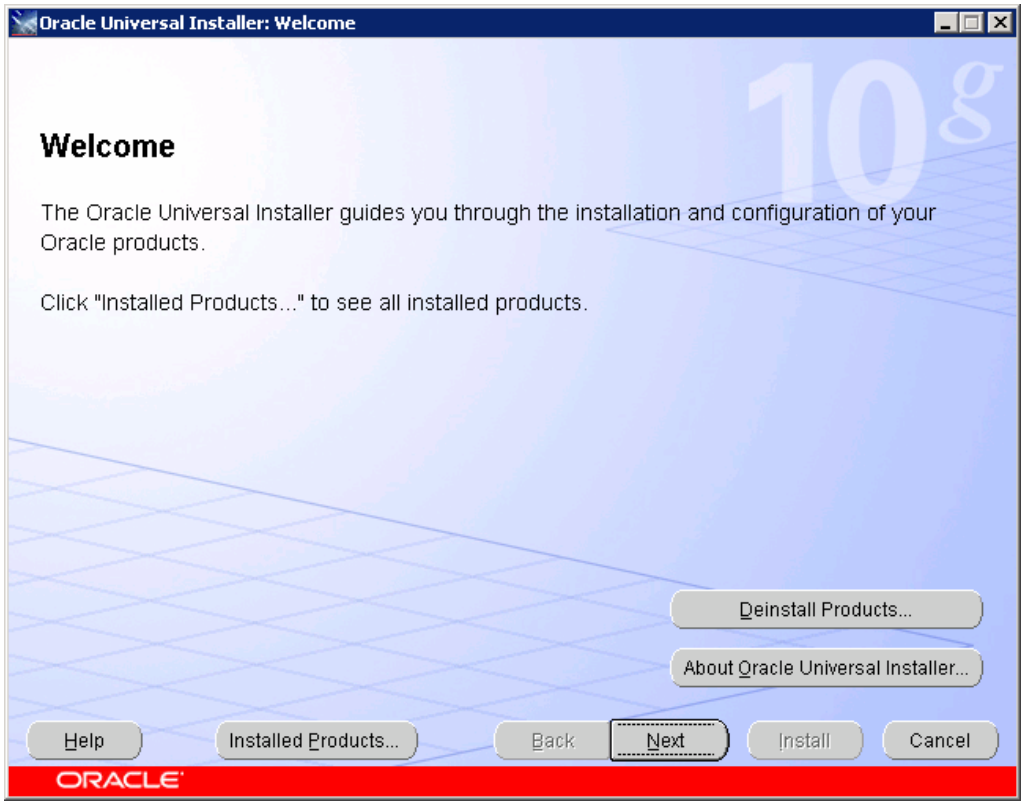
L.3 Oracle Database 10g Client Release 2 (10.2.0.1.0) Installation

Login to the server machine as the oracle user and navigate to the directory where the issue media has been installed (in the Evaluated Configuration used to derive the screenshots given in this document, this was `C:\stage\client`.

Start the Oracle Universal Installer by double-clicking setup.exe.

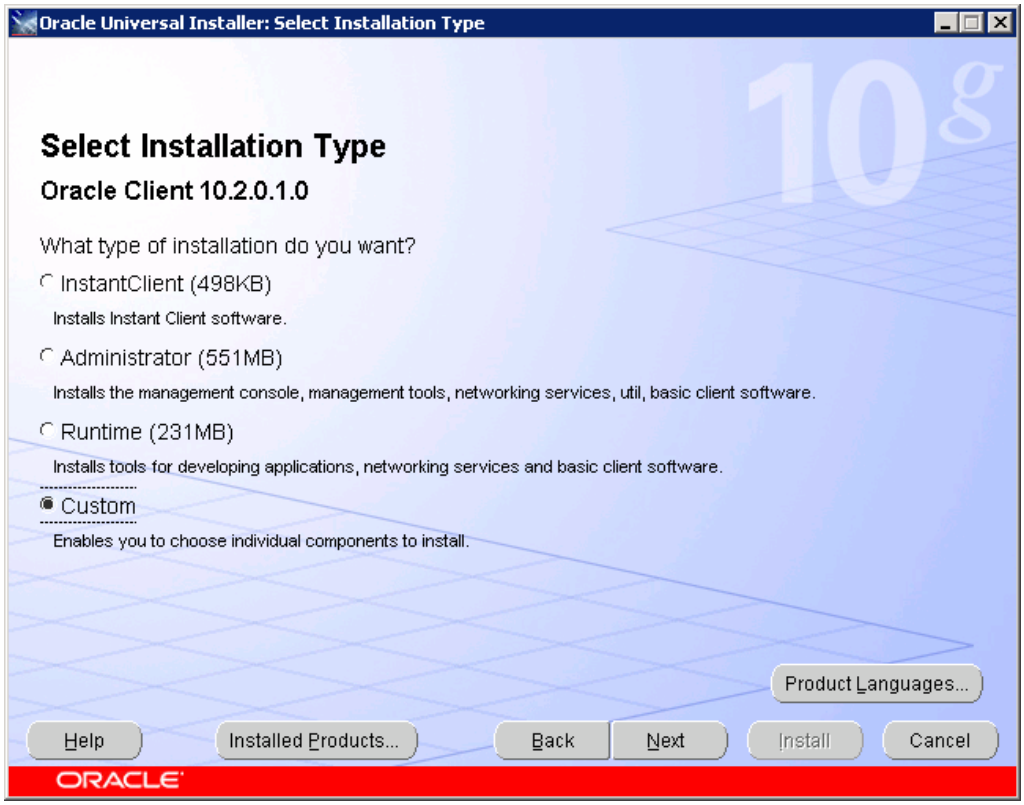
The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of Oracle Database 10*g* Client Release 2 (10.2.0.1.0).

L.3.1 Welcome Screen



Click Next.

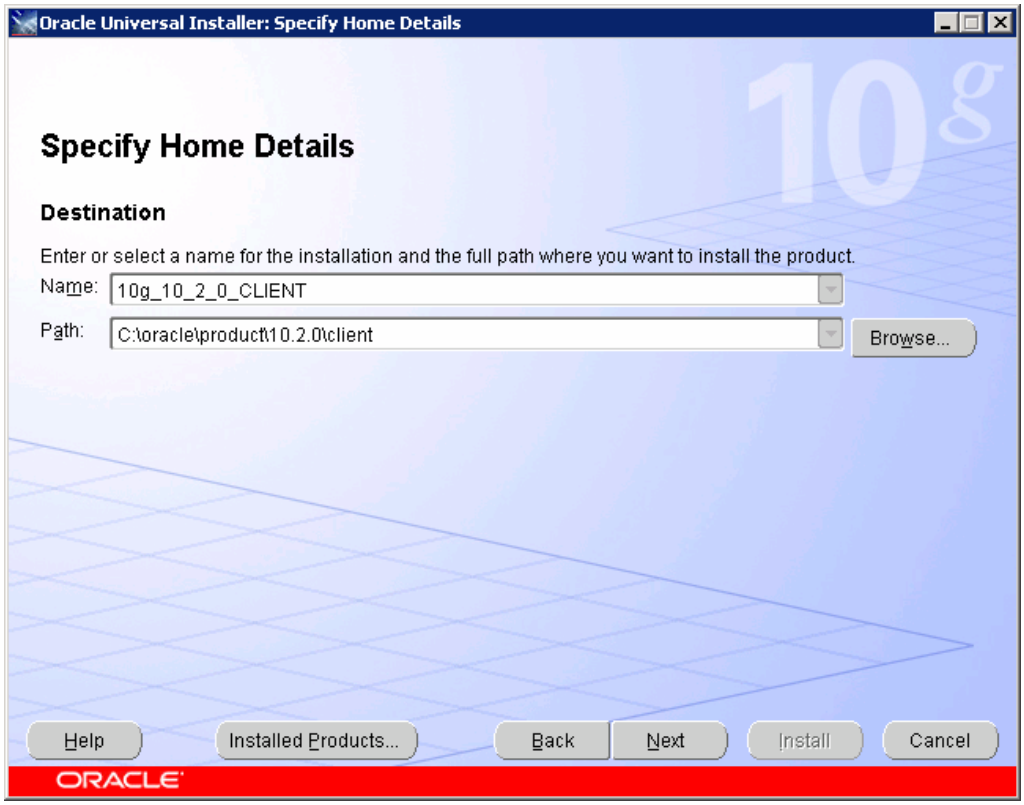
L.3.2 Installation Type



Click the **'Custom'** radio button.

Click Next.

L.3.3 Home Details

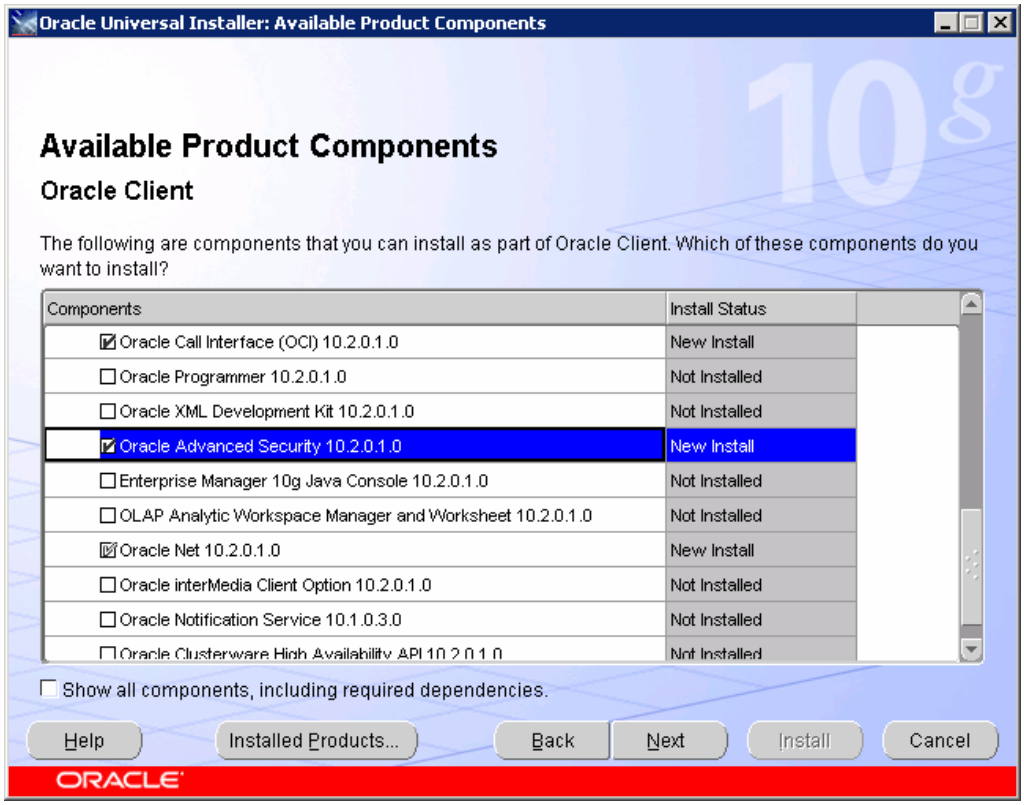


Enter the 'Installation Value' for the parameter **'Name'** specified in the pre-installation table matrix into the **'Name'** field.

Enter the 'Installation Value' for the parameter **'Path'** specified in the pre-installation table matrix into the **'Path'** field.

Click Next.

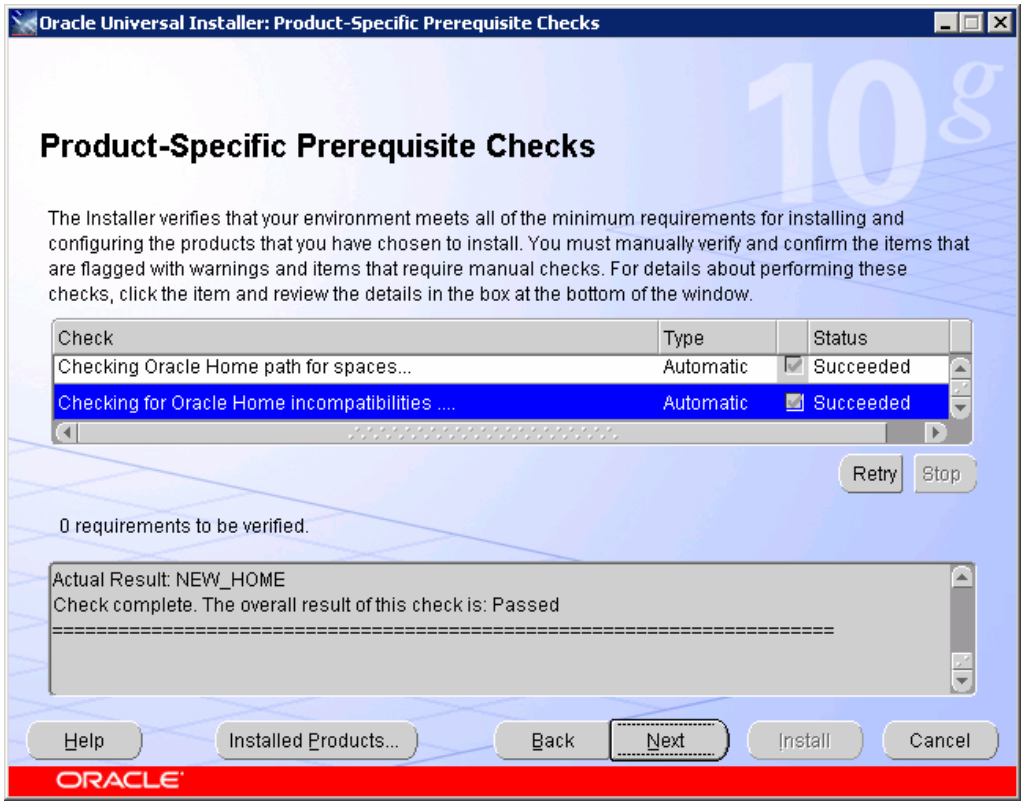
L.3.4 Product Components



Select the **'Oracle Call Interface (OCI) 10.2.0.1.0'** and **'Oracle Advanced Security 10.2.0.1.0'** components. The **'Oracle Net 10.2.0.1.0'** is a required component of Oracle Advanced Security and will also be selected.

Click Next.

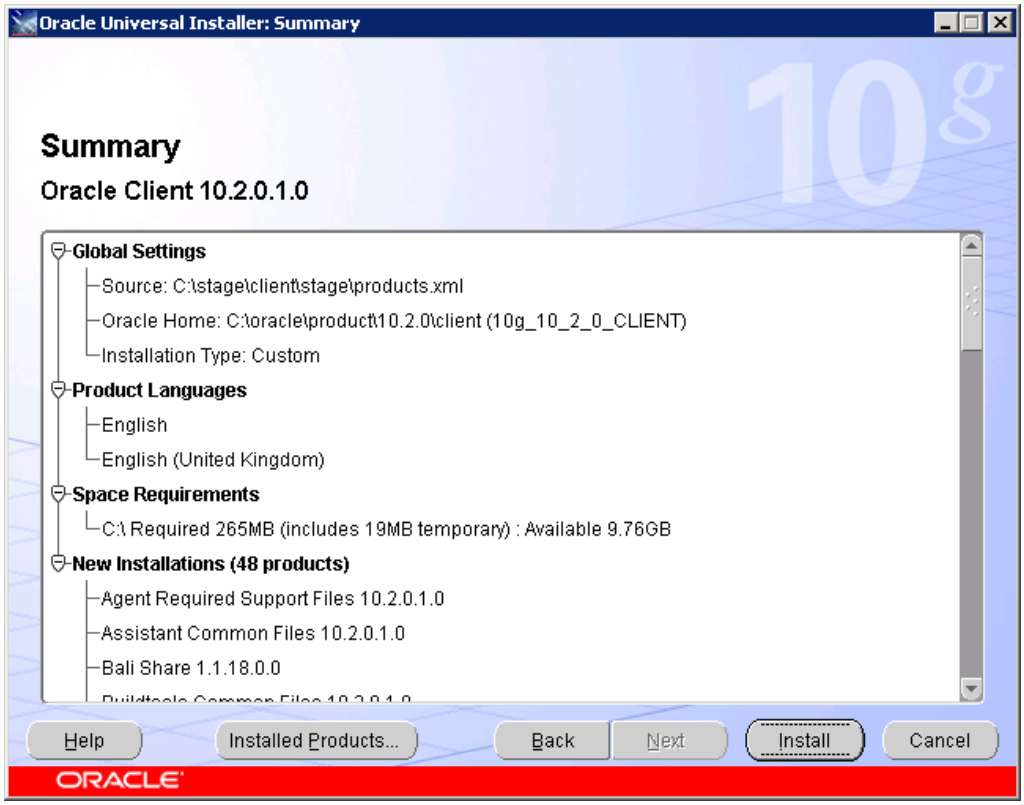
L.3.5 Product Components



Make sure that there are **‘0 requirements to be verified’**.

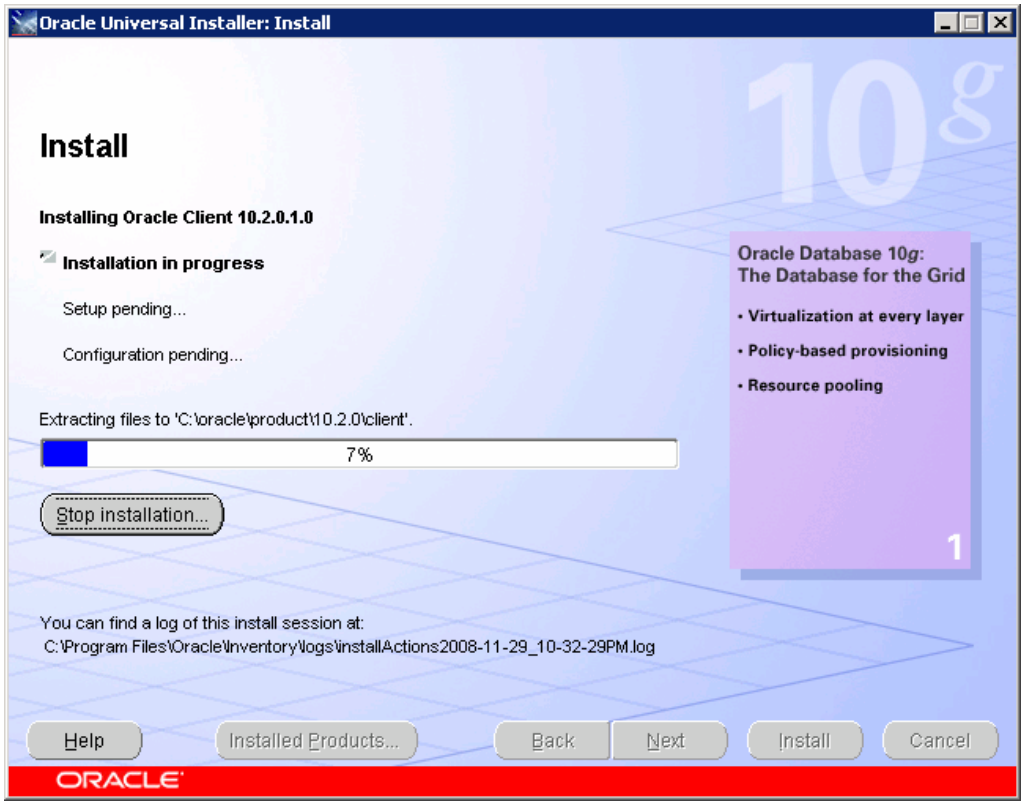
Click Next.

L.3.6 Product Components

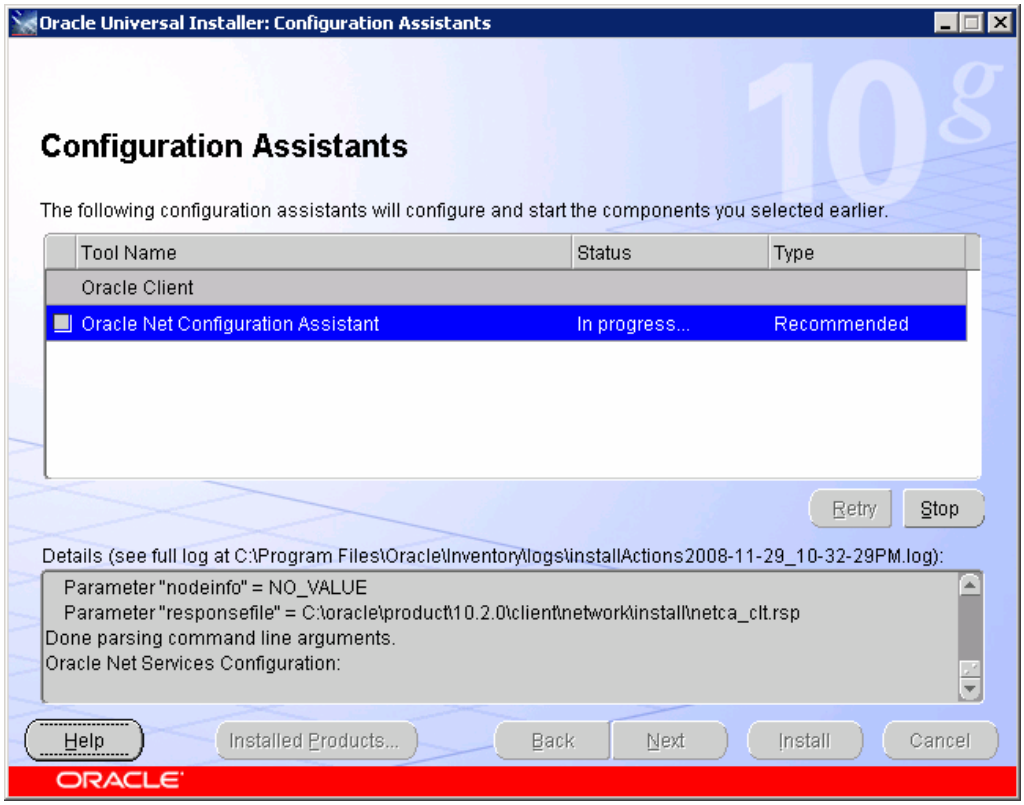


Click the **'Install'** radio button.

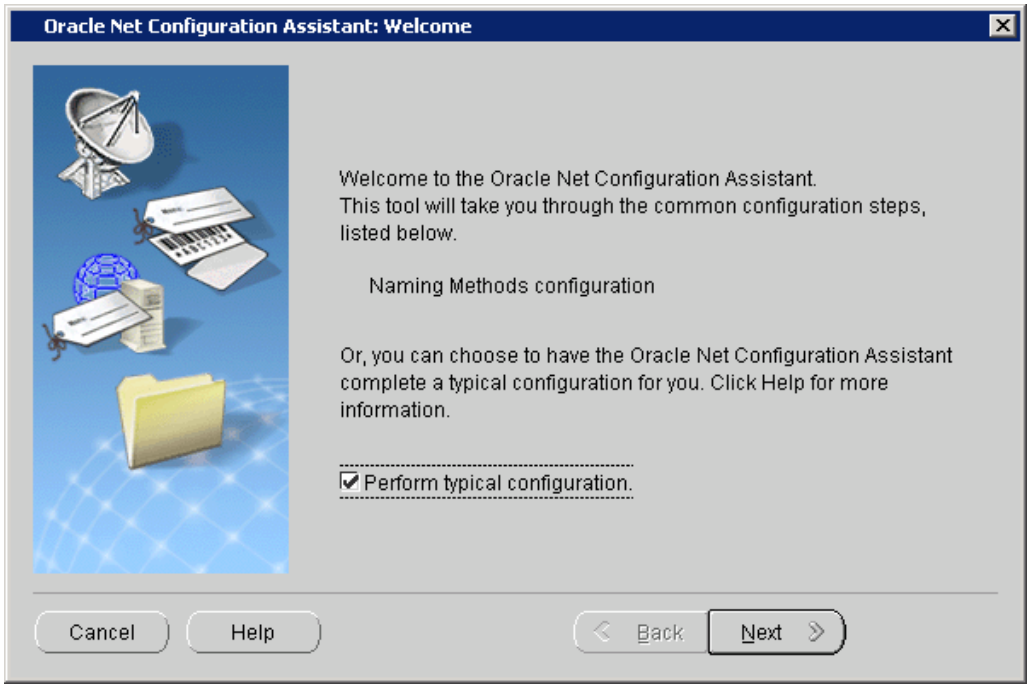
L.3.7 Install



L.3.8 Configuration Assistants

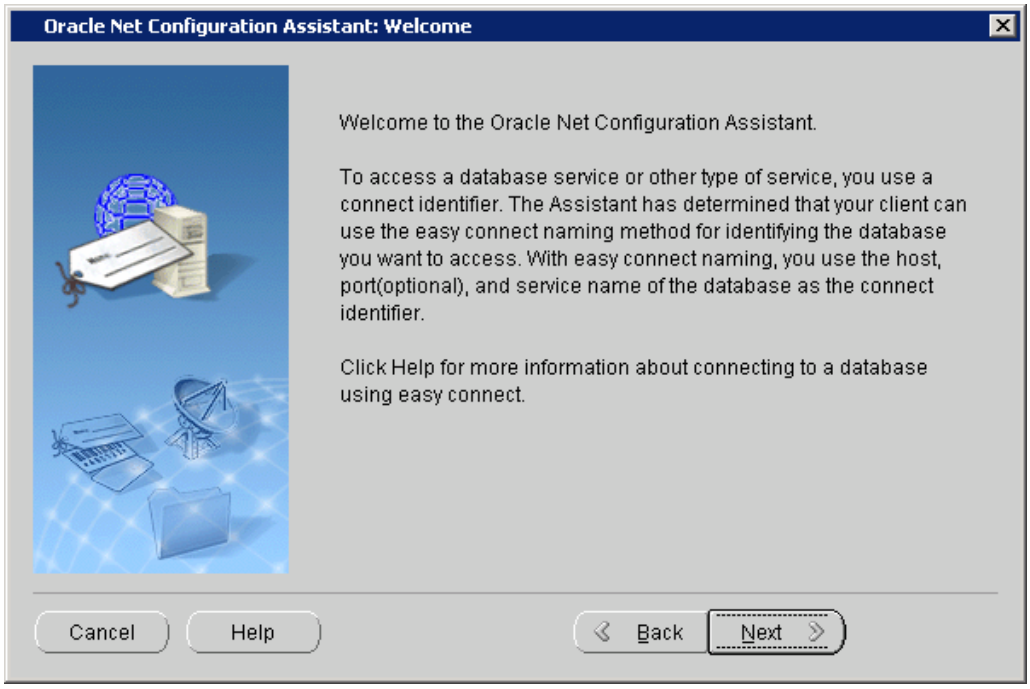


L.3.9 Net Configuration Assistants

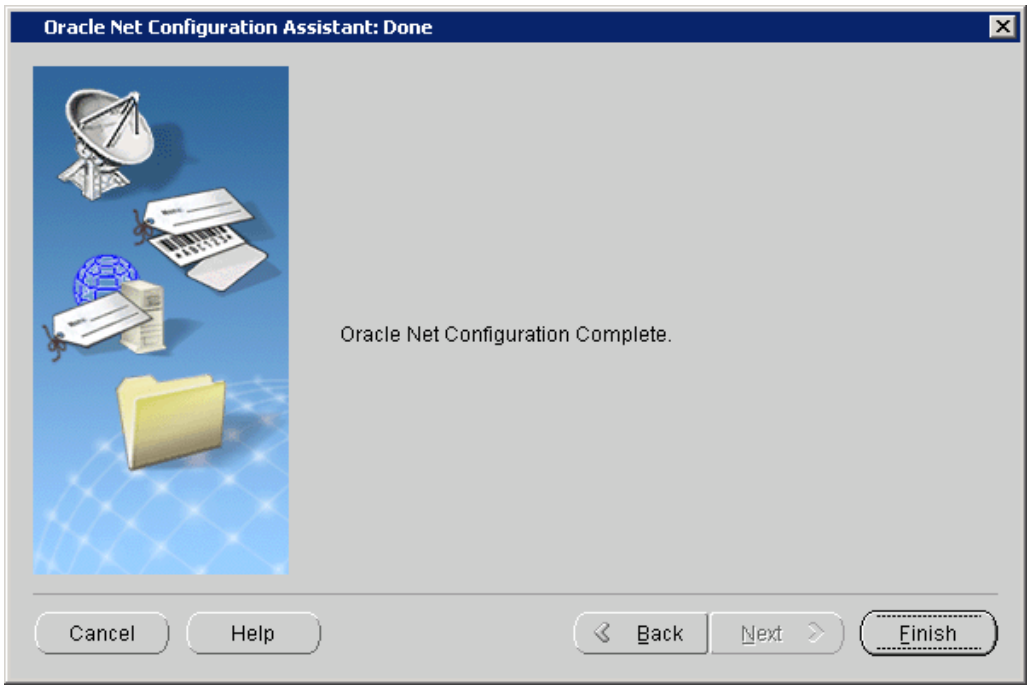


Tick the **'Perform typical configuration'** check box.

Click Next.

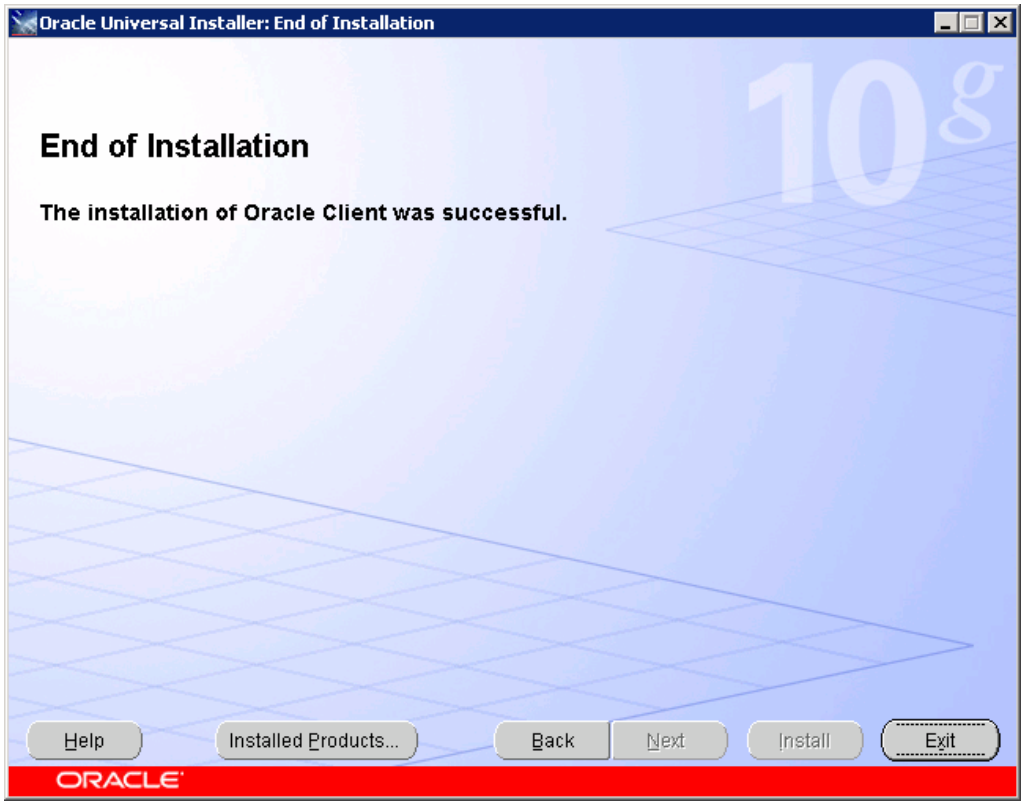


Click Next.



Click Finish.

L.3.10 End of Installation



The installation of Oracle Database 10*g* Client Release 2 (10.2.0.1.0) is now complete.

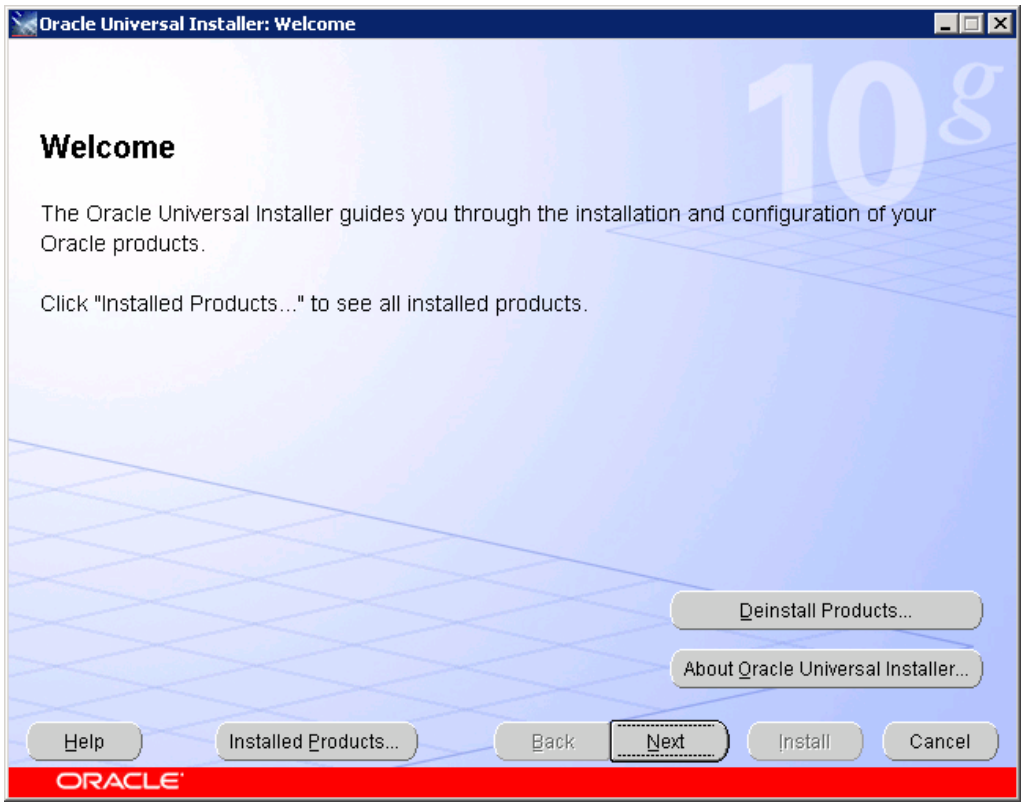
L.4 Oracle Database 10*g* Client Release 2 (10.2.0.3.0) Installation

Login to the server machine as the `oracle` user and navigate to the directory where the issue media has been installed (in the Evaluated Configuration used to derive the screenshots given in this document, this was `C:\stage\database_10203\Disk1`.

Start the Oracle Universal Installer by double-clicking setup.exe.

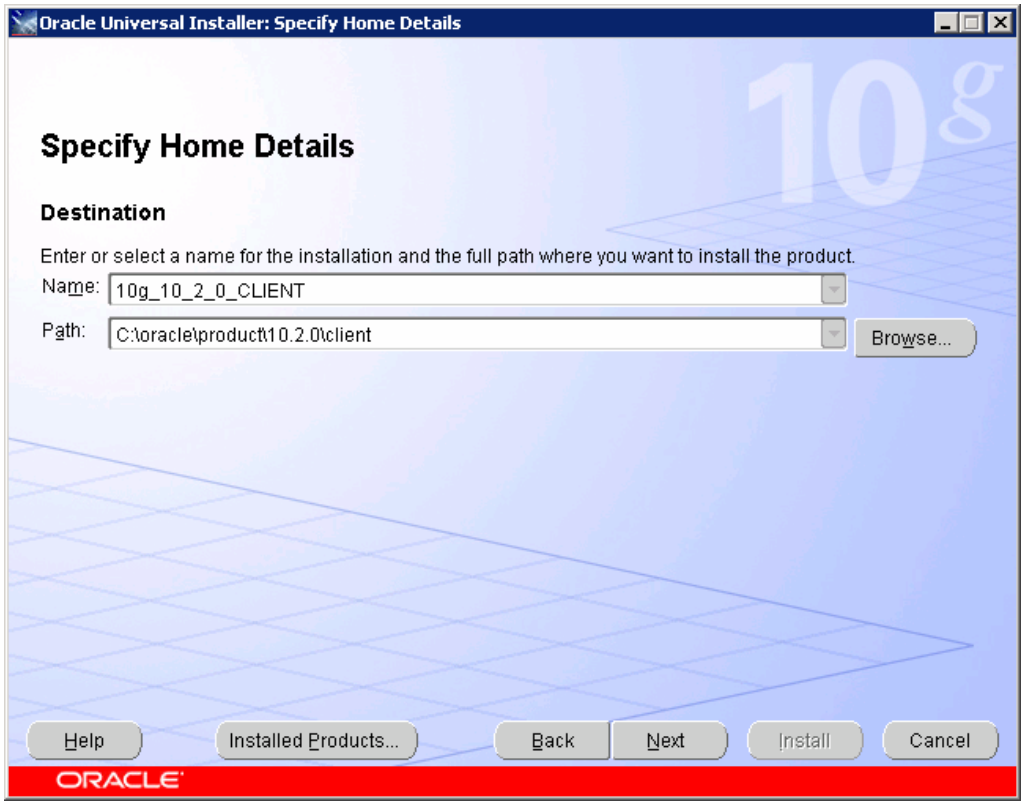
The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of Oracle Database 10*g* Client Release 2 (10.2.0.3.0).

L.4.1 Welcome Screen



Click Next.

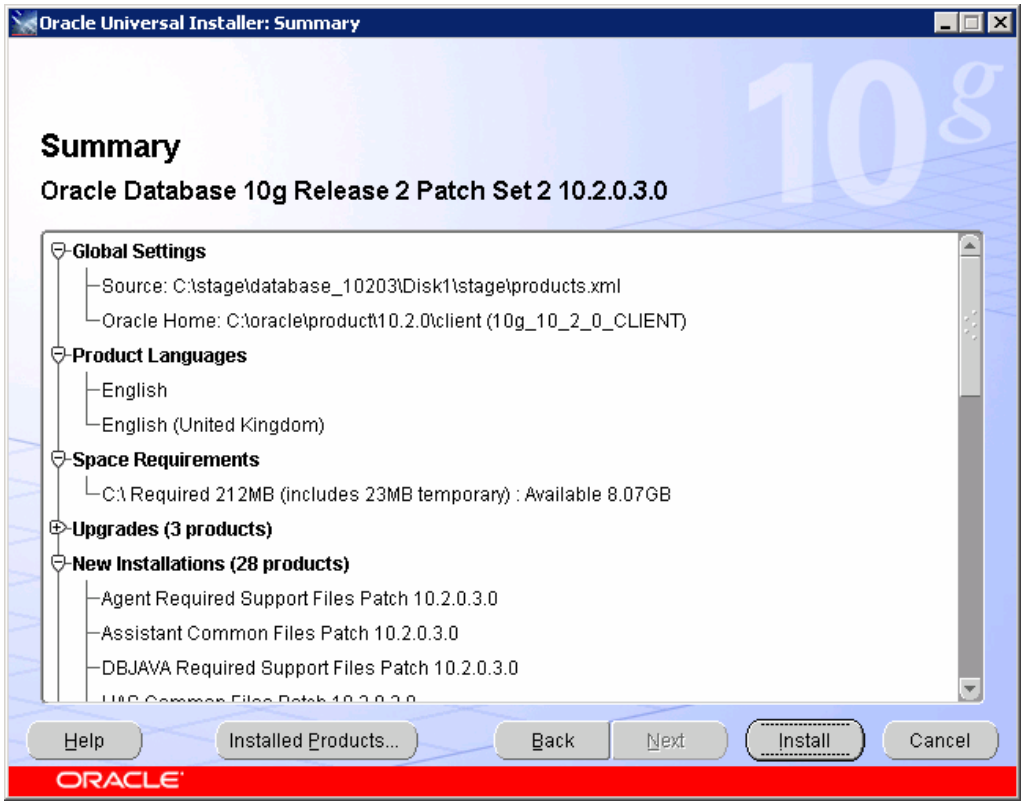
L.4.2 Home Details



Select the **'Name'** entered during the previous installation from the select list.

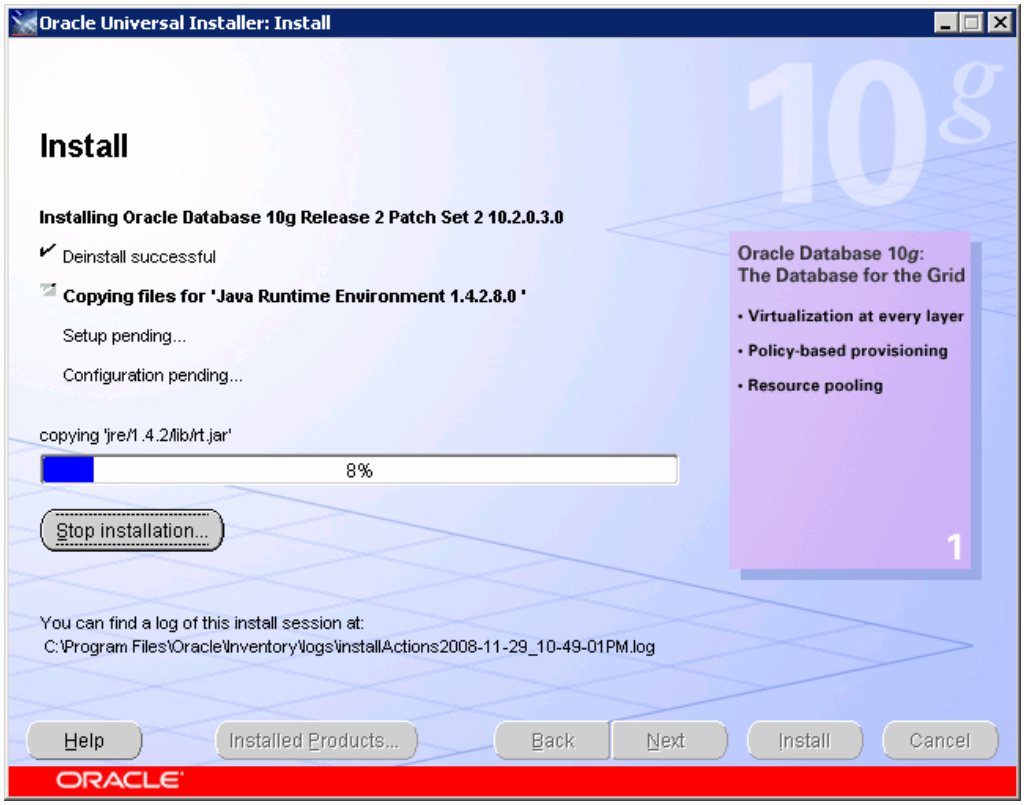
Click Next.

L.4.3 Summary



Click the **'Install'** button.

L.4.4 Install



L.4.5 End of Installation

The installation of Oracle Database 10*g* Client Release 2 (10.2.0.3.0) is now complete.

L.5 OPatch 10.2.0.4.3

OPatch is delivered through patch `6880880`. Issue the following commands:

```
set ORACLE_HOME=C:\oracle\product\10.2.0\client
set PATH=%ORACLE_HOME%\OPatch;%PATH%
cd %ORACLE_HOME%
move OPatch OPatch.102030
```

Extract the patch `p6880880_102000_WINNT.zip` to the client `ORACLE_HOME`:

```
unzip <path-to>/p6880880_102000_WINNT.zip
```

Verify that OPatch has been updated by issuing the command:

```
opatch version
```

The result should be:

```
Invoking OPatch 10.2.0.4.3

OPatch Version: 10.2.0.4.3

OPatch succeeded.
```

L.6 Critical Patch Update April 2007

Change directory to the location of the extracted patch and issue:

```
opatch apply
```

At the **'Is the local system ready for patching? [y/n]'** prompt enter: **'Y'**.

Oracle Configuration Manager (OCM) is bundled with OPatch and must be configured during the OPatch session:

At the **'stop displaying the license agreement'** prompt enter: **'q'**.

At the **'License Agreement'** prompt enter: **'Y'**.

At the **'Proxy specification'** prompt enter: **'NONE'**.

OCM will be installed and configured and then the critical patch for April 2007 will be installed.

Successful patch application will be indicated by:

```
Return Code = 0

The local system has been patched and can be restarted.

OPatch succeeded.
```

Annex M Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) Client Tools Installation

This annex provides a step by step guide to installing Oracle Business Intelligence Enterprise Edition 10g (10.1.3.3.2) Client Tools, running on a Microsoft Windows XP operating system.

M.1 Prerequisites

J2SE Development Kit 5.0 Update 16 installed according to Annex K.

Oracle Database 10*g* Client Release 2 (10.2.0.3.0) according to Annex L.

M.2 Input Parameters

The software installer will require the following input parameters for successful completion of the software installation. The values for these parameters should be gathered prior to starting the installation.

The following table should be completed with the insertion of the values to be used for the current installation into the 'Installation Value' column. The 'Example Value' column shows the values used in the example screenshots demonstrating the install process.

Pre-installation table matrix

Parameter Name	Installation Value	Example Value
BI Home		C:\oracle\product\OBIEE
BI Data Home		C:\oracle\oradata\OBIEE
JDK Home		C:\Program Files\Java\jdk1.5.0_16

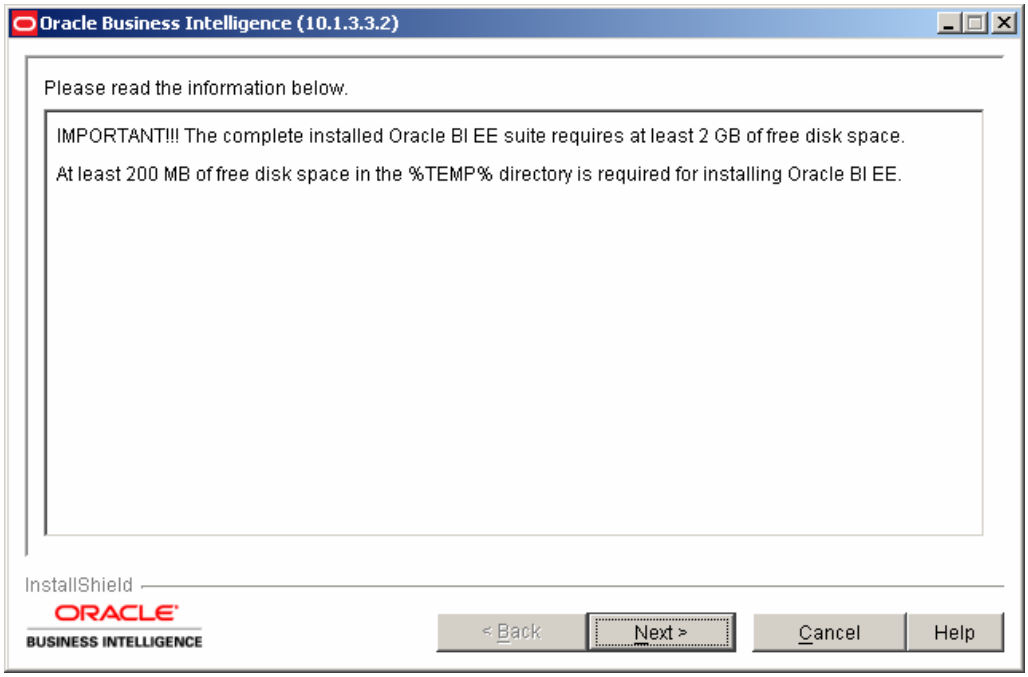
M.3 Installation of Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) Client Tools

Login to the server machine as the oracle user and navigate to the directory where the issue media has been installed (in the Evaluated Configuration used to derive the screenshots given in this document, this was <CD Drive>\Server\Oracle_Business_Intelligence

Navigate to the directory above and double-click on setup.exe. This will start the Oracle Business Intelligence (10.1.3.3.2) Installer.

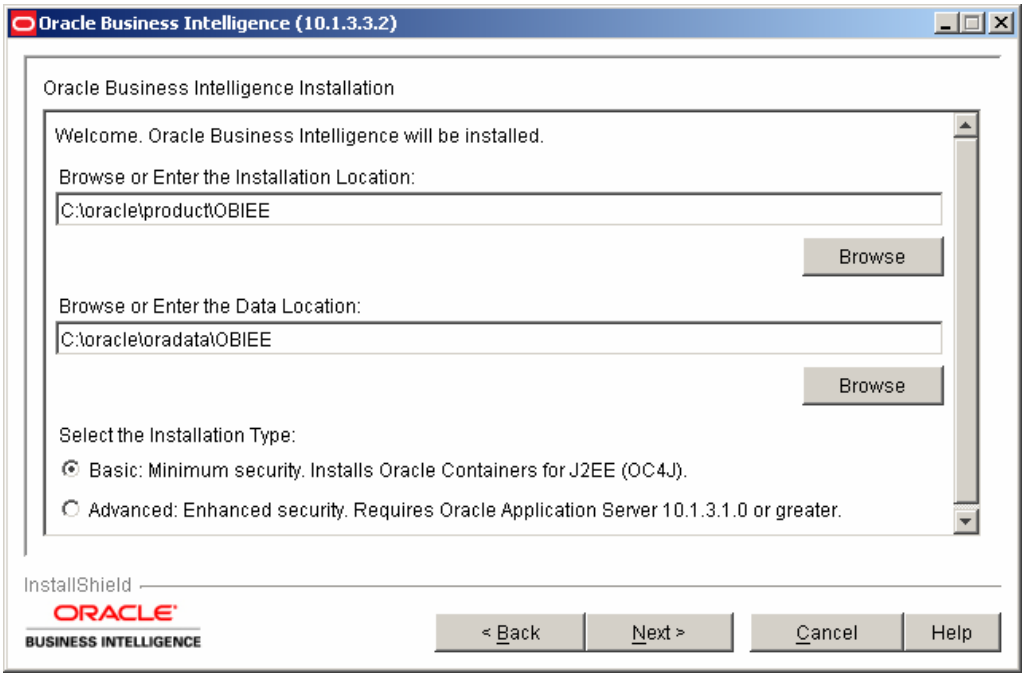
The information to be supplied by the administrator for each step is indicated on the pages below underneath the relevant screenshot. These screenshots illustrate the screens that were displayed during the installation of the Client Tools.

M.3.1 Information



Click Next.

M.3.2 Installation Location



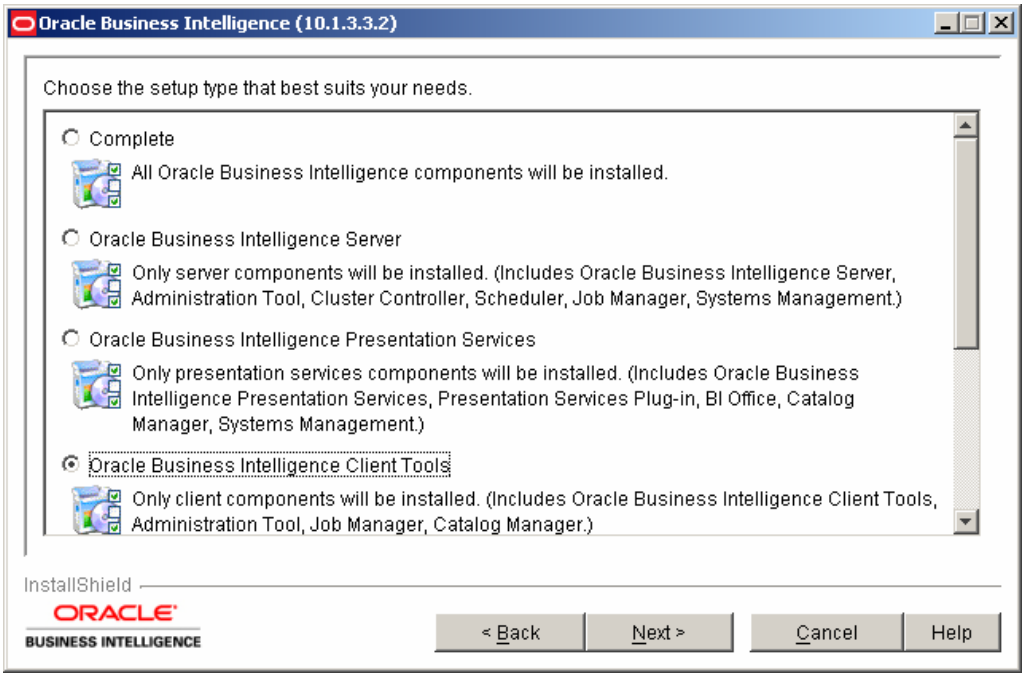
Enter the 'Installation Value' for the parameter **'BI Home'** specified in the pre-installation table matrix into the **'Installation Location'** field.

Enter the 'Installation Value' for the parameter **'BI Data Home'** specified in the pre-installation table matrix into the **'Data Location'** field.

Click the **'Basic: Minimum security. Installs Oracle Containers for J2EE (OC4J)'** radio button.

Click Next.

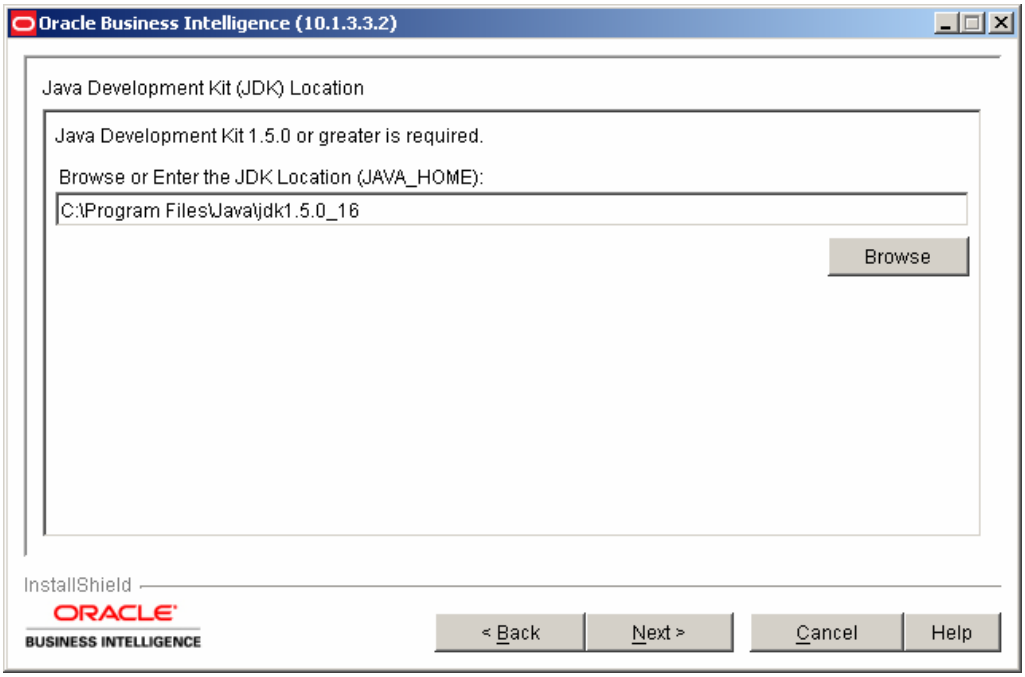
M.3.3 Product Components



Click the **'Oracle Business Intelligence Client Tools'** radio button.

Click Next.

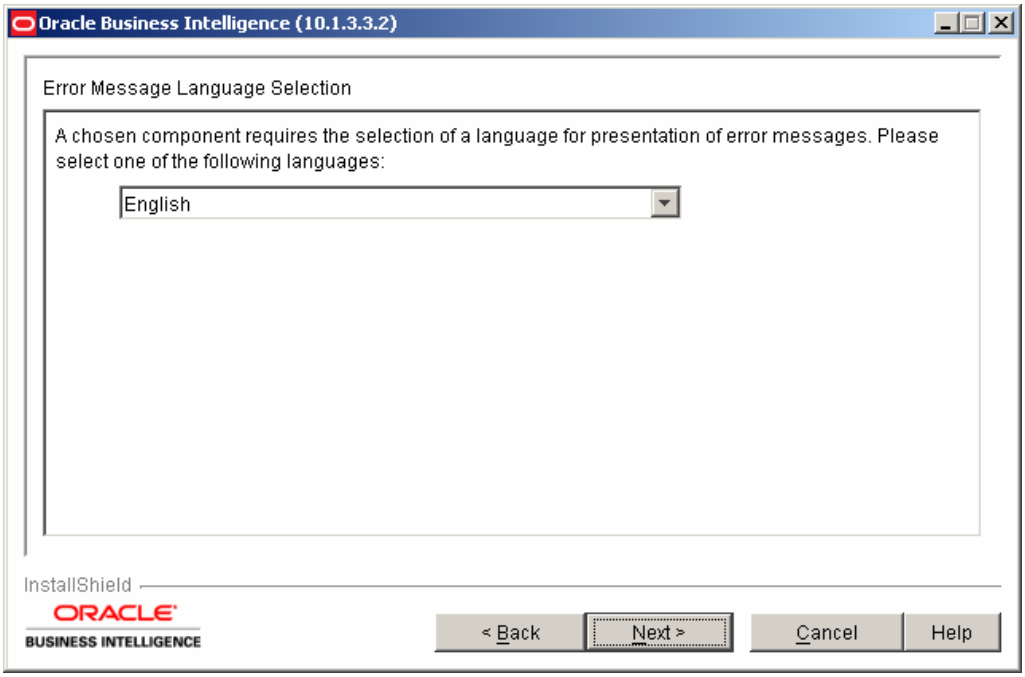
M.3.4 Java Development Kit (JDK) Location



Enter the 'Installation Value' for the parameter **'JDK Home'** specified in the pre-installation table matrix into the **'JDK Location'** field.

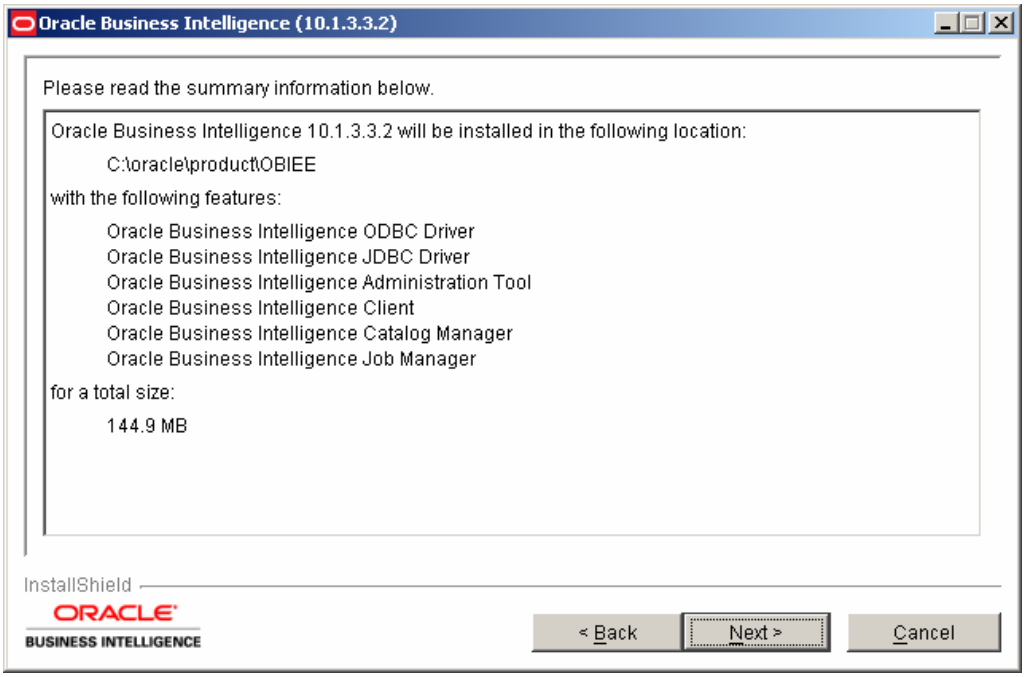
Click Next.

M.3.5 Error Message Language Selection



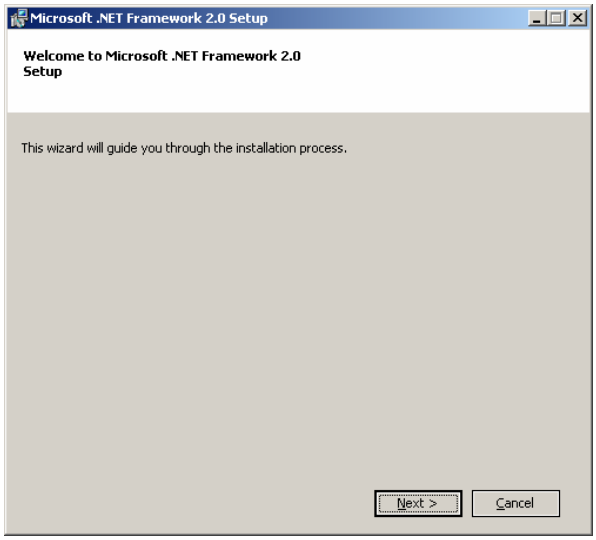
Click Next.

M.3.6 Summary

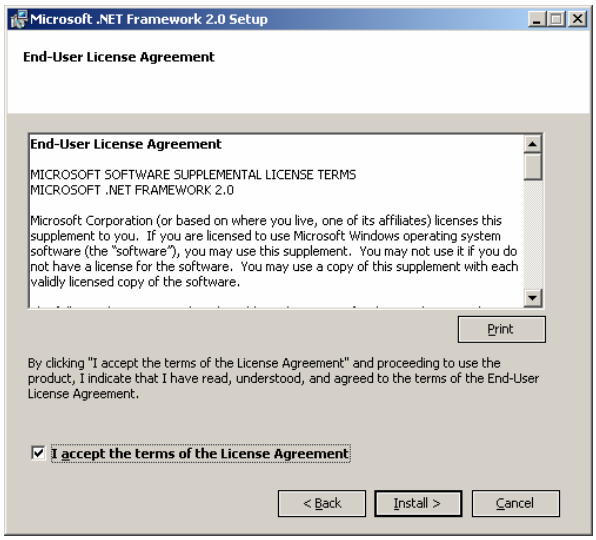


Click Next.

M.3.7 Microsoft .NET Framework and Visual C++ Redistributable

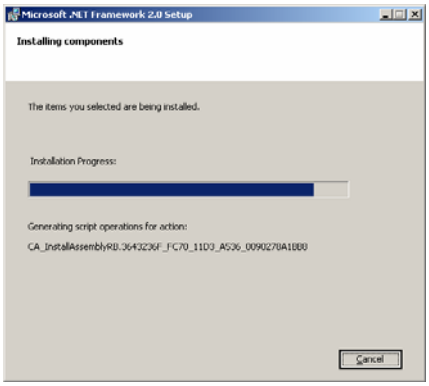


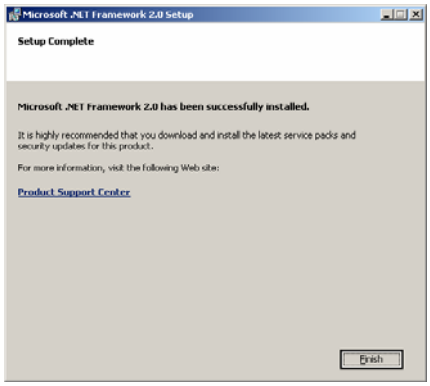
Click Next.



Tick the **'I accept the terms of the License Agreement'** check box.

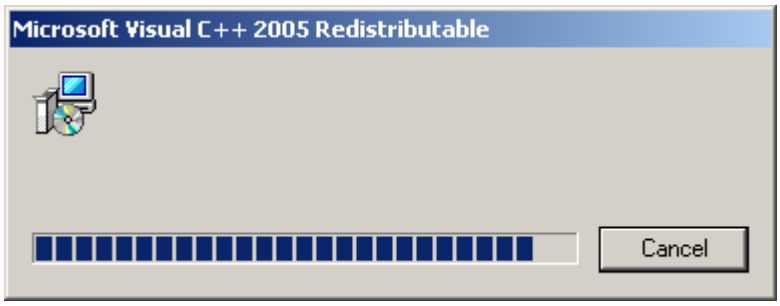
Click Install.





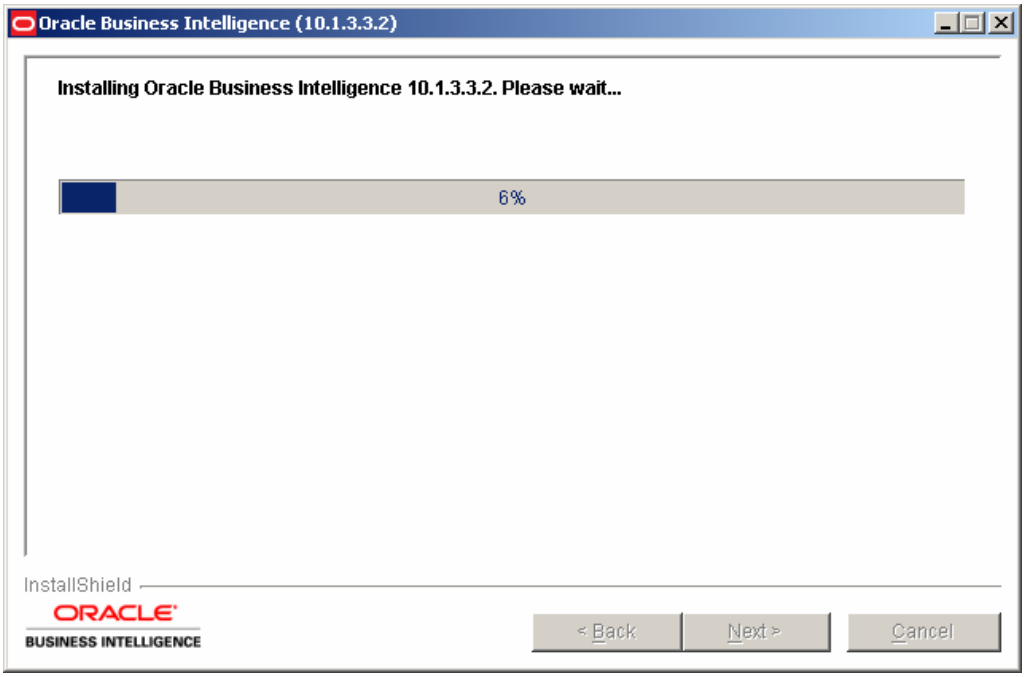
Click Finish.

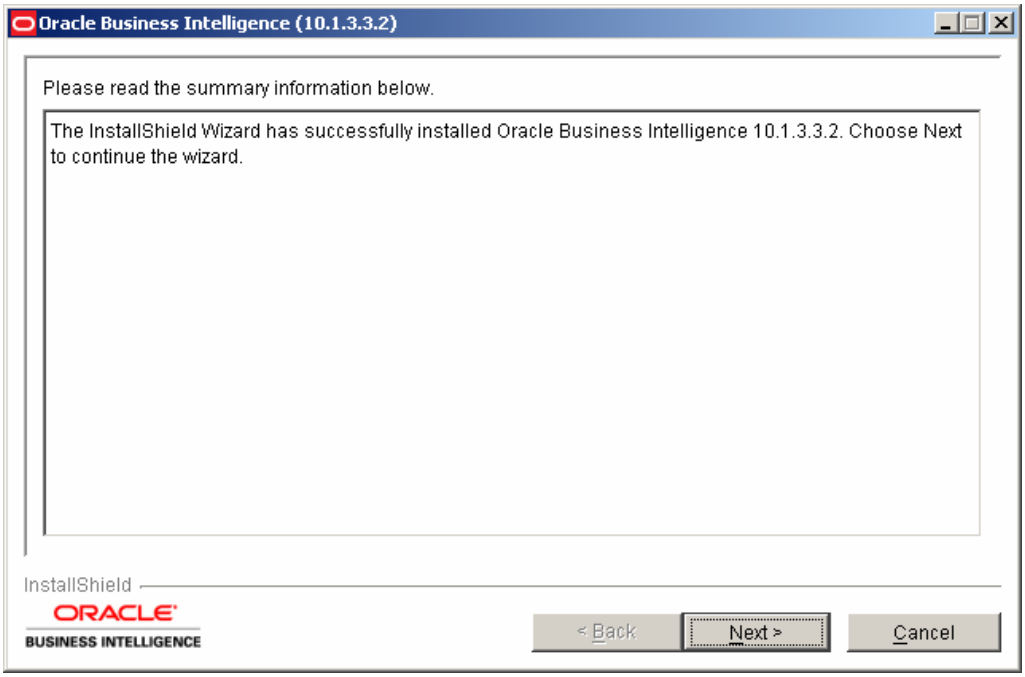
After the Microsoft .NET Framework 2.0 Installer completes, the Microsoft Visual C++ 2005 Redistributable will be installed.



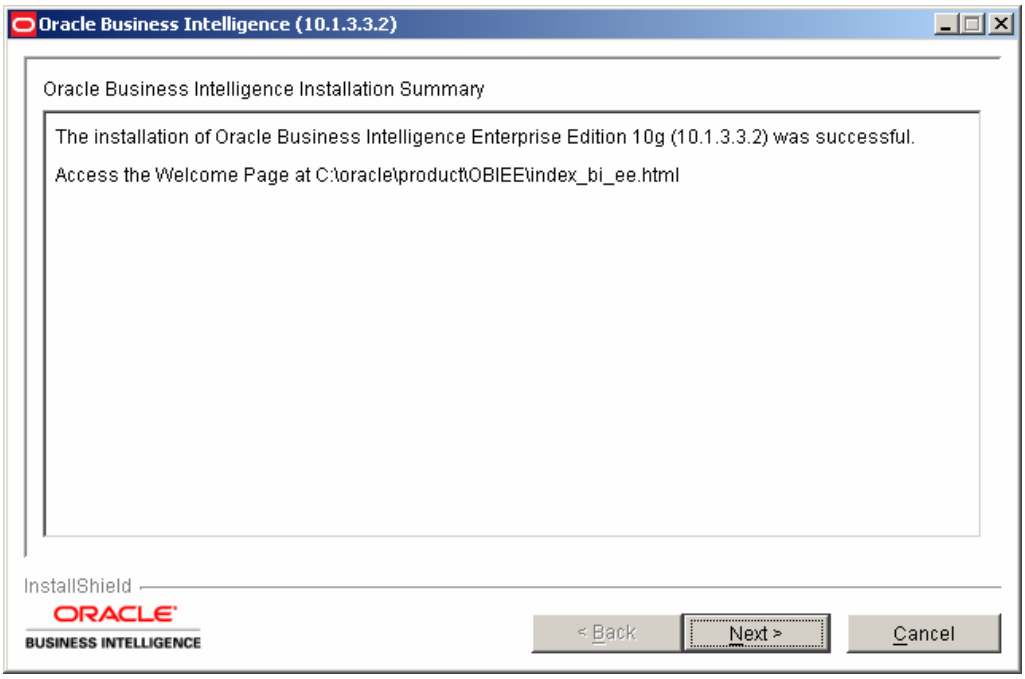
The Client Tools installation will begin once the Microsoft Visual C++ 2005 Redistributable Installer is complete.

M.3.8 Installation

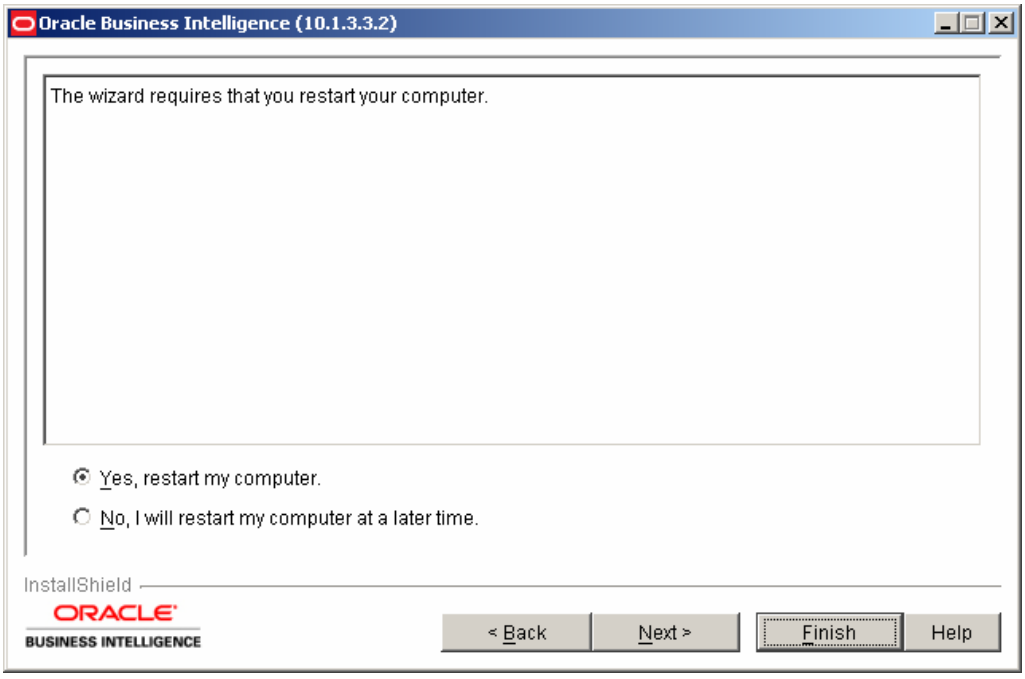




Click Next.



Click Next.



Click the **'Yes, restart my computer'** radio button.

Click Finish.

The installation of Oracle Business Intelligence Enterprise Edition 10*g* (10.1.3.3.2) Client Tools will be complete once the computer has restarted.

Annex N IBM GSKit 7 Installation

This annex provides a step by step guide to installing IBM GSKit 7 in the evaluated configuration for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2).

N.1 IBM GSKit 7 Windows Installation

Copy the `gskit7-windows.zip` file from the `Server_Ancillary\IBM_GSK` directory on the Windows Oracle Business Intelligence Installation CD and extract the contents to a directory on the file system.

Open a command prompt, navigate to the location of the extracted installation files and issue the following command:

```
setup LDAP –s –f1 setup.iss
```

IBM GSKit 7 will be installed in the `C:\Program Files\IBM\GSK7` directory.

Add a `SYSTEM` variable called `JAVA_HOME` and set its value to `C:\Program Files\Java\jdk1.5.0_16`.

Copy the following jar files from the `C:\Program Files\IBM\GSK7\classes\jre\lib\ext` directory to the `%JAVA_HOME%\jre\lib\ext` directory:

- ibmjceprovider.jar
- ibmpkcs.jar
- ibmjcefw.jar
- local_policy.jar
- US_export_policy.jar
- ibmjlog.jar
- ibmjsse.jar

Register the IBM JCE and IBM CMS service providers by updating the `%JAVA_HOME%\jre\lib\security\java.security` file to add the IBMJCE provider and IBMCMS provider after the list of providers.

```
security.provider.7=com.ibm.spi.IBMCMSProvider
security.provider.8=com.ibm.crypto.provider.IBMJCE
```

N.2 IBM GSKit 7 Linux Installation

Copy the `gskit7-linux.tar` file from the `RH_Linux\Server_Ancillary\IBM_GSK` directory on the Linux Oracle Business Intelligence Installation CD and extract the contents to a directory on the file system.

Change directory to the `gskit` directory and issue the following command as the `root` user:

```
rpm -ihv gsk7bas-7.0-3.3.i386.rpm
```

Annex O References

[CC] Common Criteria for Information Technology Security Evaluation (Comprising Parts 1-3: [CC1], [CC2], and [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model
CCMB-2006-09-001, Version 3.1 Release 1, September 2006

[CC2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements
CCMB-2007-09-002, Version 3.1 Release 2, September 2007

[CC3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements
CCMB-2007-09-003, Version 3.1 Release 2, September 2007

[CEM] Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology
CCMB-2007-09-004, Version 3.1 Release 2, September 2007

[ECGDB] *Evaluated Configuration for Oracle Database 10g Release 2 (10.2.0)*, Issue 0.6, November 2007, Oracle Corporation.

[ECGOID] *Evaluated Configuration for Oracle Internet Directory 10g (10.1.4.0.1)*, Issue 0.3, March 2008, Oracle Corporation

[ECGOIDIG] *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1): Oracle Internet Directory Installation*, Oracle Corporation**.**

[ECGHTTP] *Evaluated Configuration for Oracle HTTP Server 10g Release 2 (10.1.2)*, Issue 0.9, January 2007, Oracle Corporation.

[ECGOEL4] *CC EAL4+ Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5*, Version 1.3, 23rd August 2007, Oracle Corporation.

[ST] Security Target for Oracle Business Intelligence Enterprise Edition (10.1.3.3.2) with Quick Fix 090406, Oracle Corporation, version 1.6, June 2009.