



Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1): Oracle Virtual Directory Installation

February 2008

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

February 2008

Author: Julian Skinner.

Contributors: James Belton, Peter Goatly, Adam O'Brien.

Copyright © 2008, Oracle Corporation. All rights reserved. This documentation contains proprietary information of Oracle Corporation; it is protected by copyright law. Reverse engineering of the software is prohibited. If this documentation is delivered to a U.S. Government Agency of the Department of Defense, then it is delivered with Restricted Rights and the following legend is applicable:

RESTRICTED RIGHTS LEGEND

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of DFARS 252.227-7013, Rights in Technical Data and Computer Software (October 1988).

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Oracle Corporation does not warrant that this document is error free.

Oracle is a registered trademark and Oracle Application Server 10g, Oracle Identity and Access Management 10g and Oracle Virtual Directory 10g are trademarks or registered trademarks of Oracle Corporation. Other names may be trademarks of their respective owners.

Contents

1 Introduction.....	1
1.1 Intended Audience.....	1
1.2 Organization	1
2 Installing OVD	3
2.1 Prerequisites	3
2.2 Installation Preparation	3
2.3 Installing OVD Server.....	3
2.4 Installing OVD Manager.....	17
2.5 Configuring OVD Server	18
2.6 Configuring Access Controls	20
2.7 Creating Adapters.....	24

This Page Intentionally Blank

1

Introduction

This installation guide contains a step by step guide to installing Oracle Virtual Directory 10g (10.1.4.0.1).

1.1 Intended Audience

This document is designed to cover the needs of people installing Oracle Virtual Directory as part of the the evaluated configuration for Oracle Identity and Access Management 10g (10.1.4.0.1).

1.2 Organization

This document is composed of the following chapters:

Chapter 1 contains the introduction to the document;

Chapter 2 contains a step by step guide to installing Oracle Virtual Directory in the evaluated configuration for Oracle Identity and Access Management 10g (10.1.4.0.1).

With the exception of Issue 0.1, change bars indicate changes since the previous issue.

This Page Intentionally Blank

Installing OVD

This chapter contains a step by step guide to installing Oracle Virtual Directory in the evaluated configuration for Oracle Identity and Access Management 10g (10.1.4.0.1), running on the Red Hat Enterprise Linux AS Version 4 Update 5 operating system.

The information to be supplied by the administrator for each step is indicated underneath the relevant screenshot in this chapter. These screenshots illustrate the screens that were displayed in a particular installation of Oracle Virtual Directory.

2.1 Prerequisites

The actions to be taken before installing Oracle Virtual Directory in the relevant evaluated configuration are given in the document *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1)*.

2.2 Installation Preparation

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 `/space/src/oracle/OVD`).

This directory should contain an archive file in cpio format. Extract the installation files as follows:

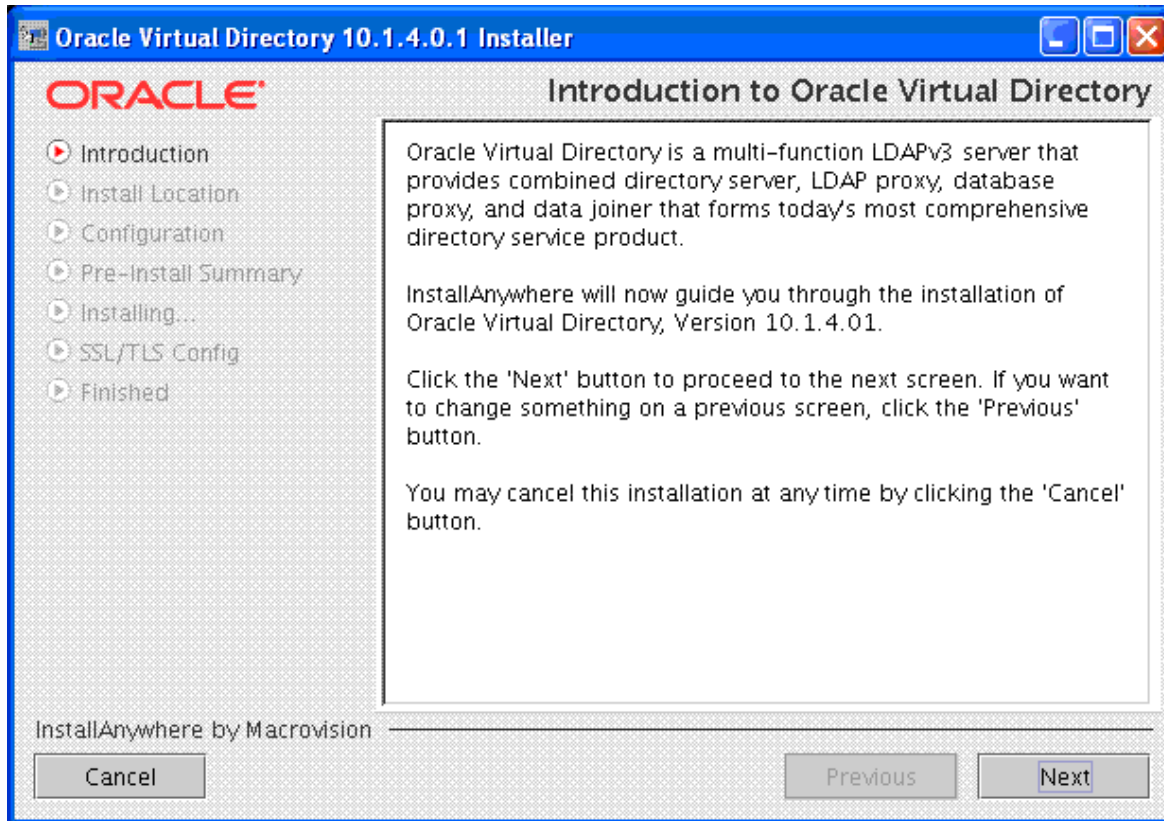
```
$ cpio -idm < as_linux_x86_oracle_virtual_directory_101401.cpio
```

This will create 3 directories named `docs`, `server` and `manager`. The following sections will explain how to install and configure the OVD Server and Manager.

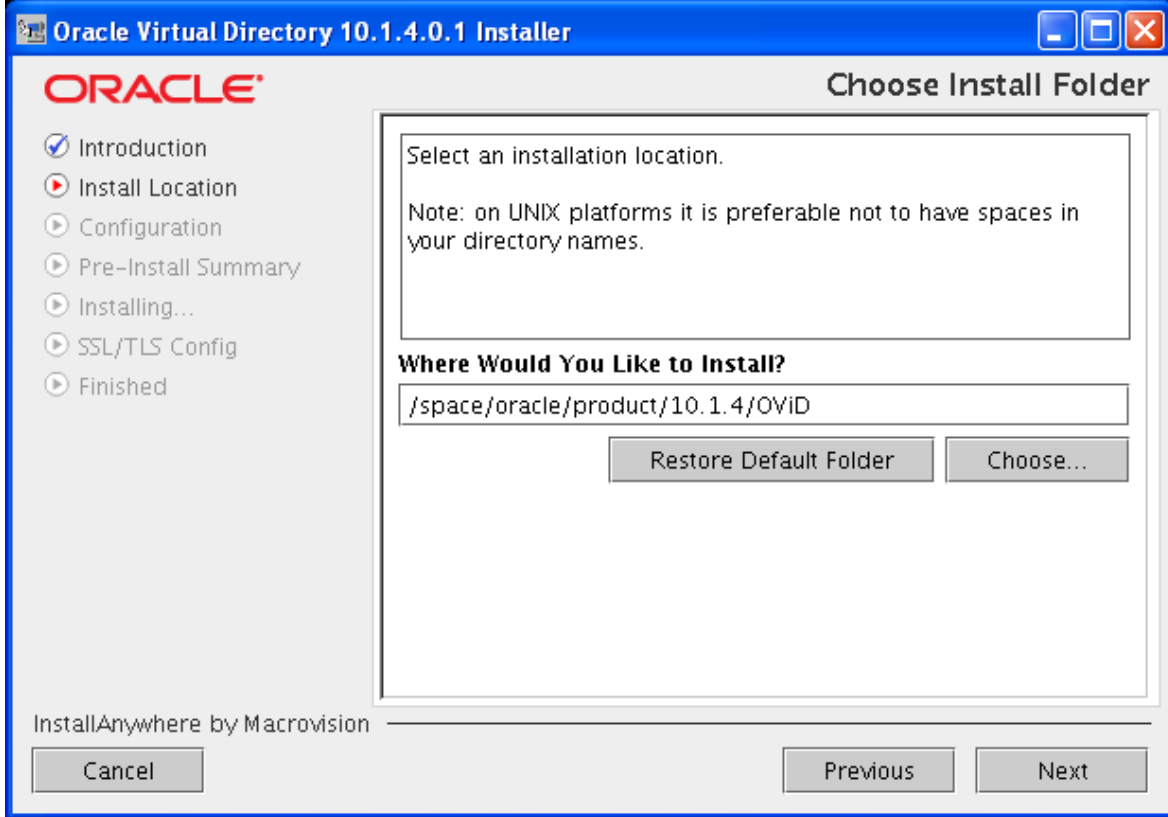
2.3 Installing OVD Server

Navigate to the `server` directory and run the following to start the installation:

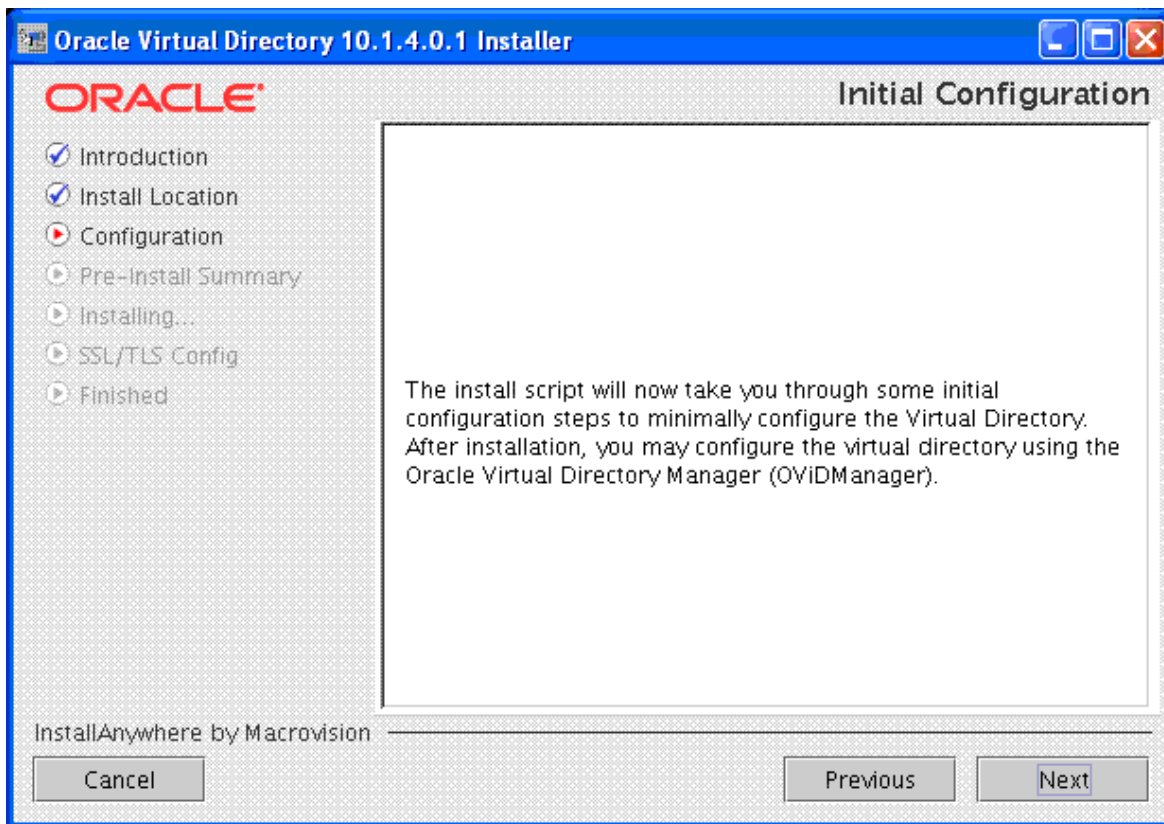
```
$ ./ovid1014.bin
```



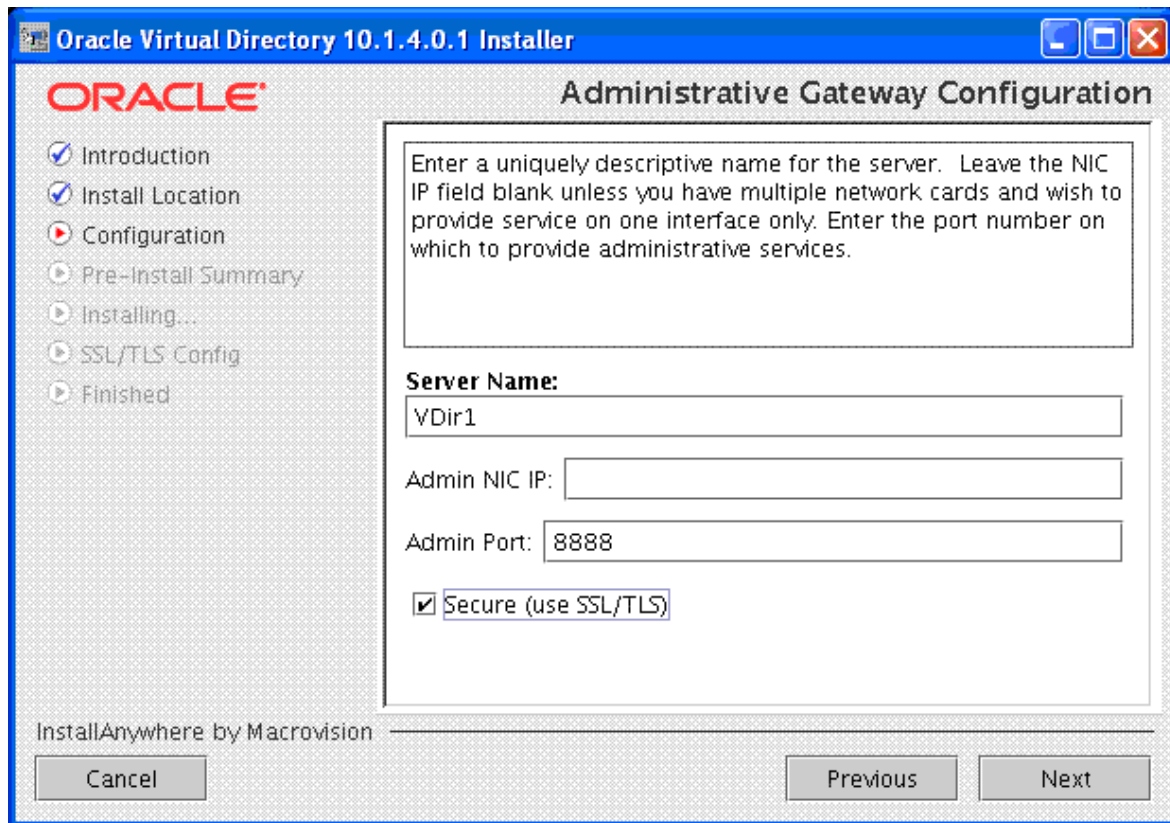
The installer will run in Graphical Mode. Click Next.



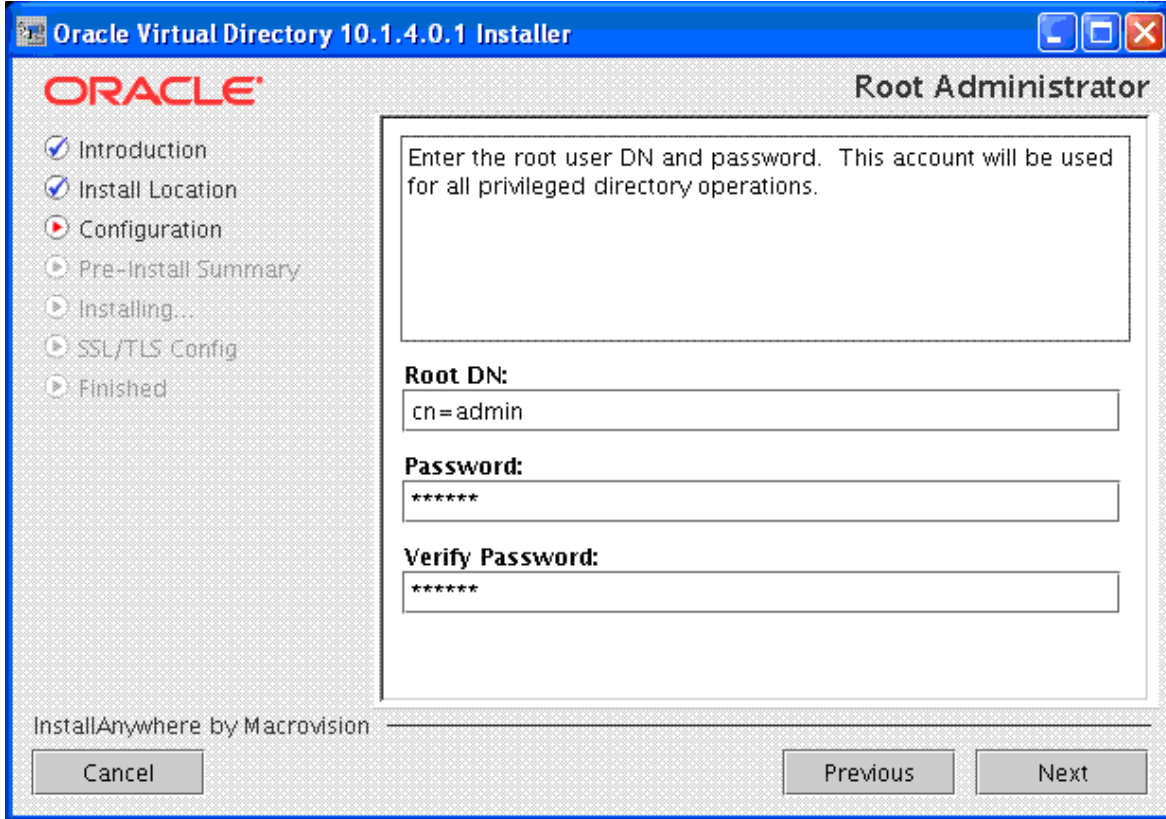
Enter the home directory for the installation and click Next.



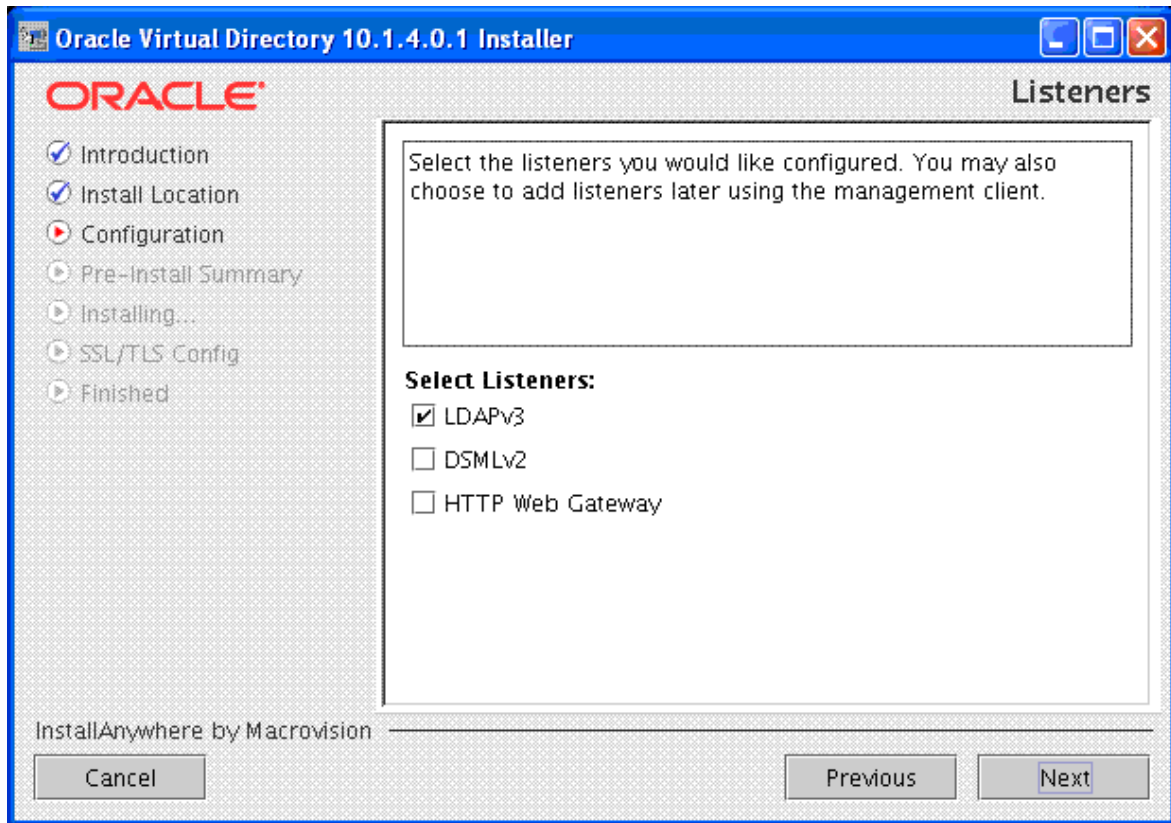
Click Next.



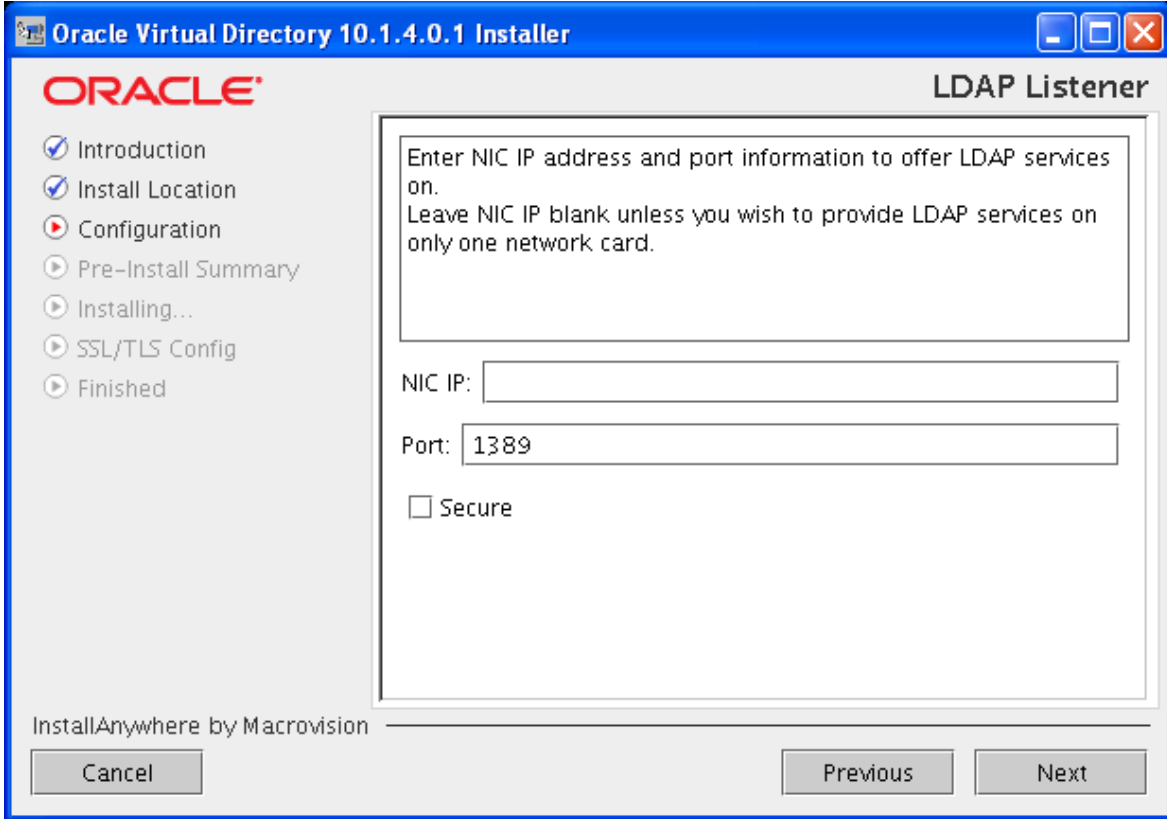
Enter a Server Name, leave the NIC IP blank and accept the default Admin Port. Click Next.



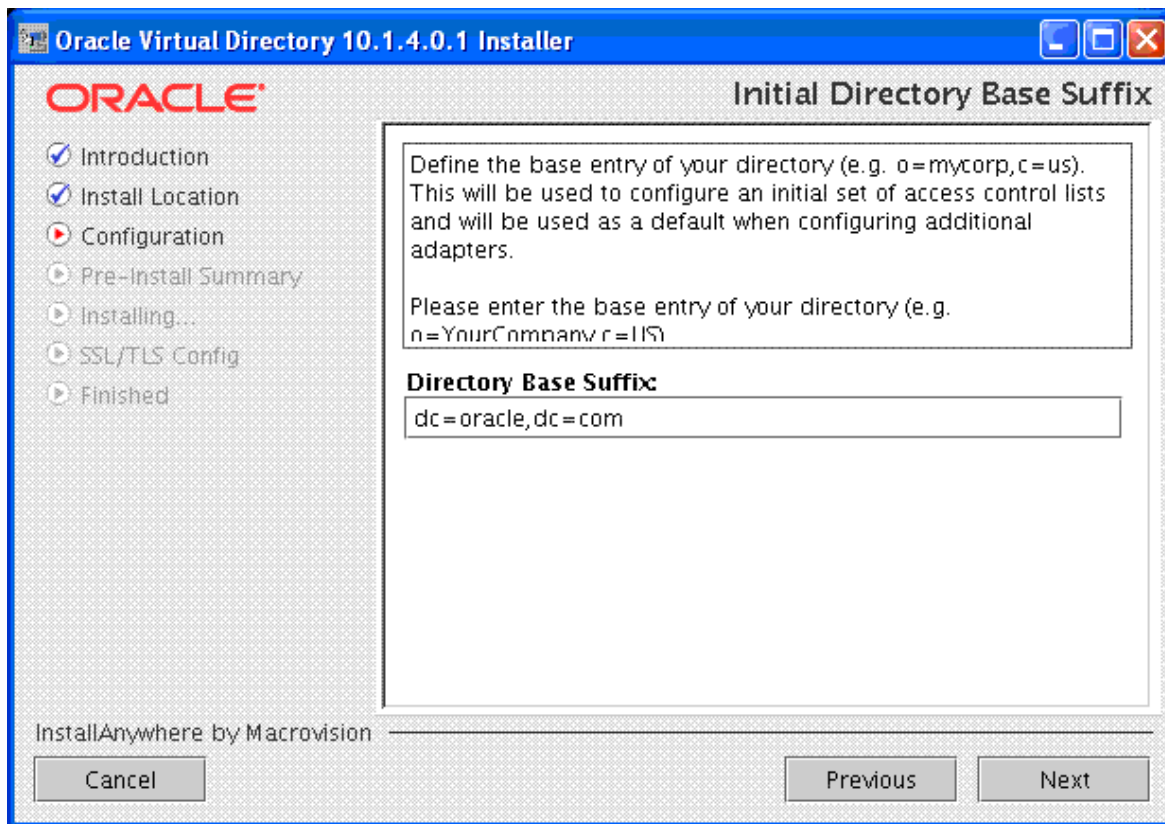
This creates the admin account for OVD. Click Next.



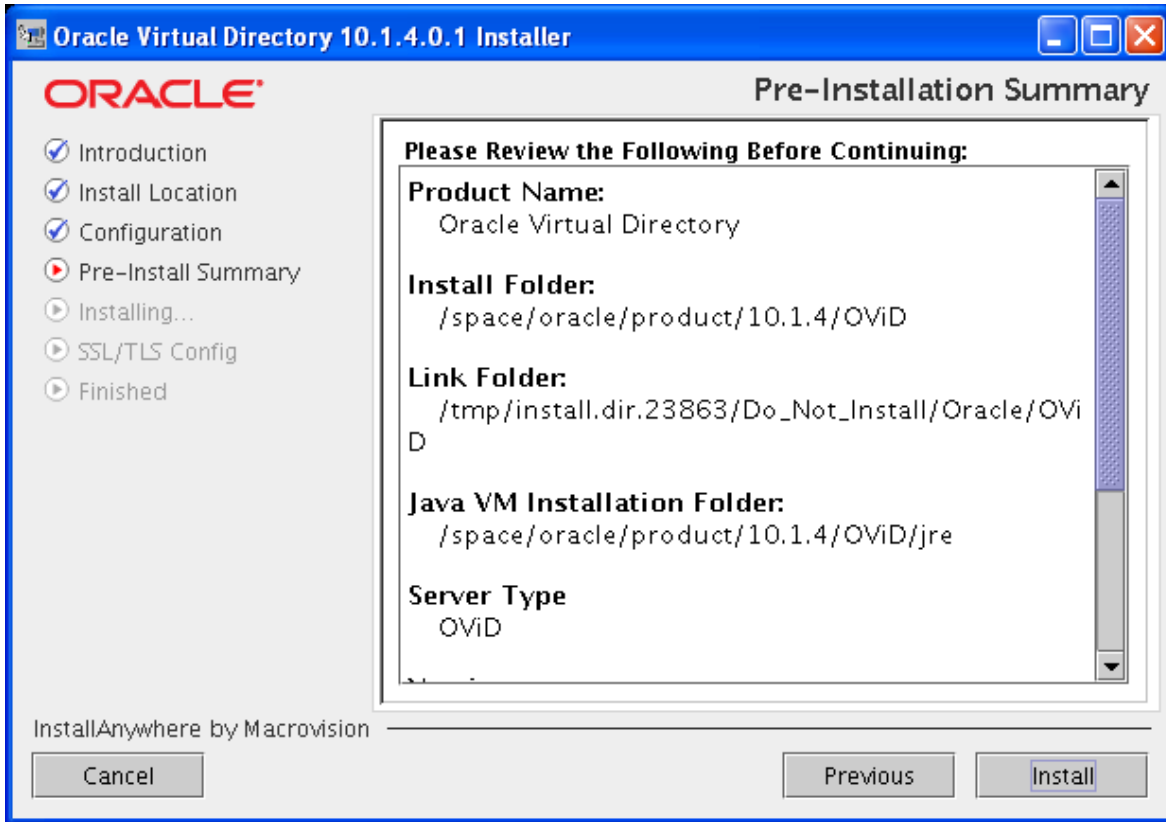
Accept the default settings and click Next.



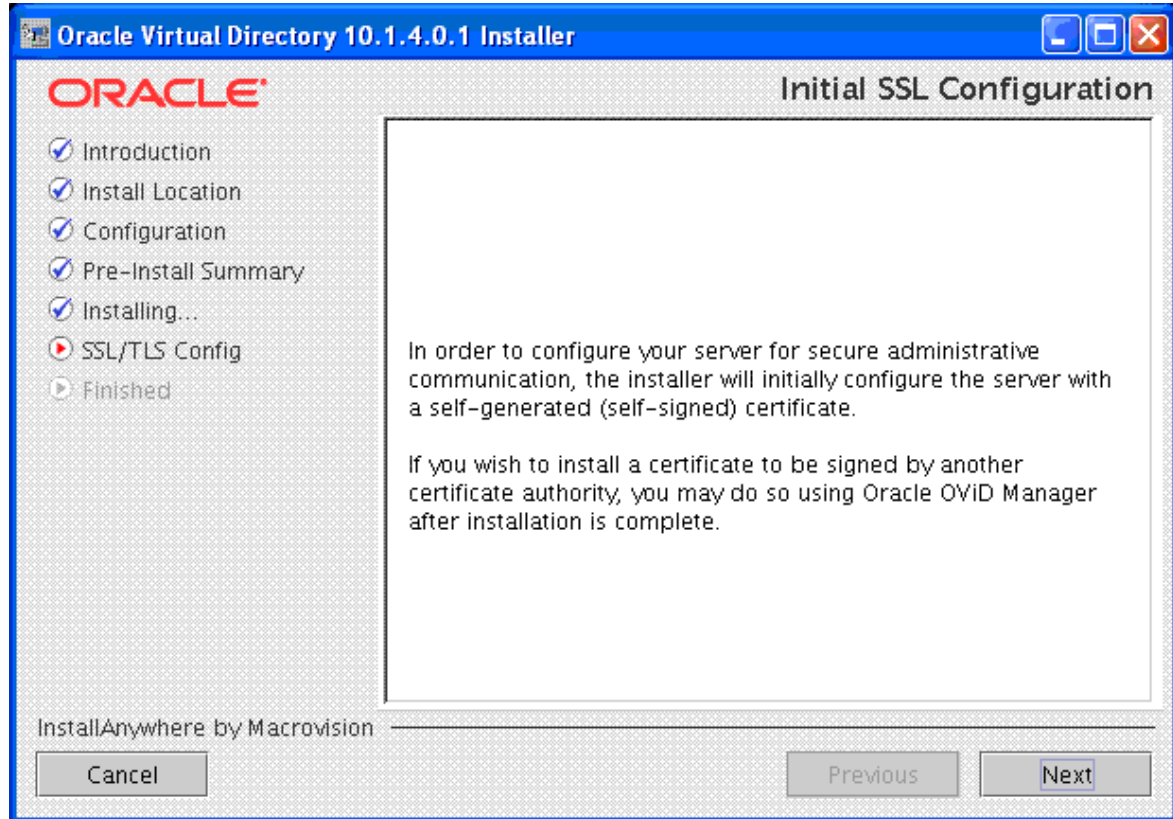
Enter the port that you want OVD to run on. Note that the default port of 389 has been changed to 1389 because 389 is already being used by OID. Click Next.



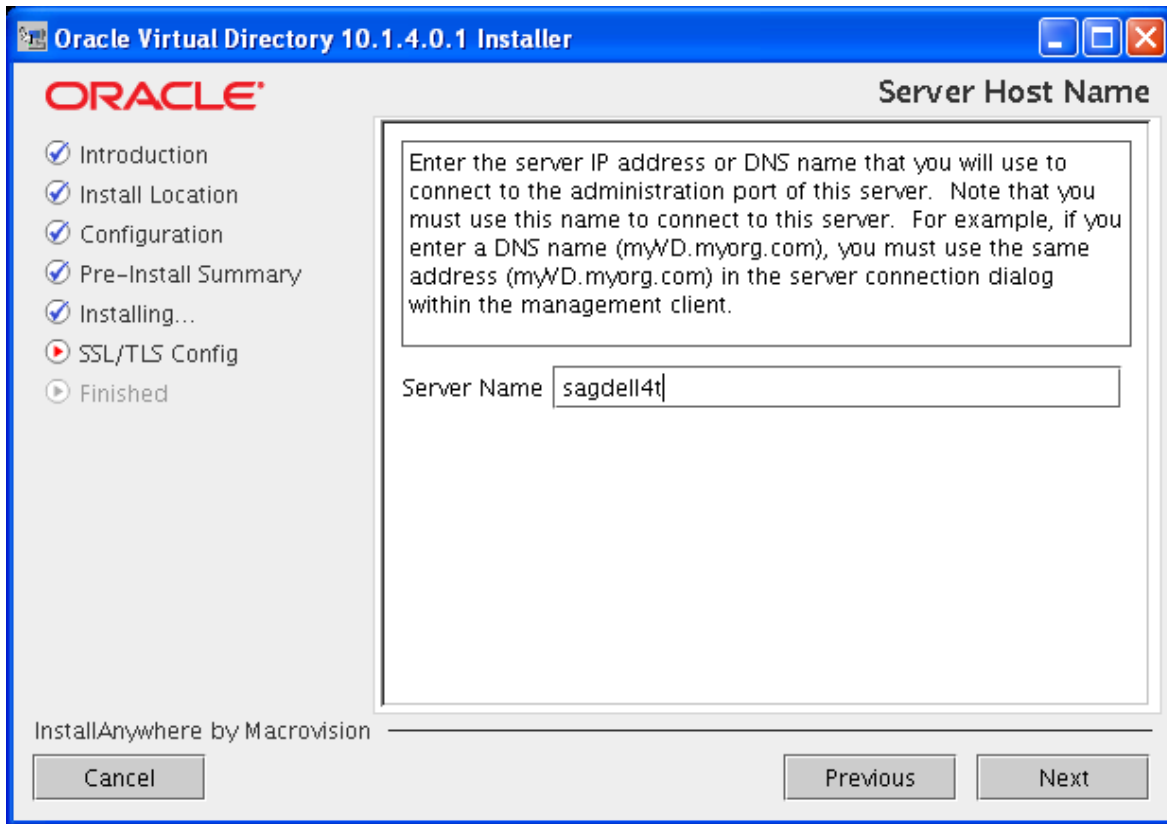
Enter the Directory Base. Click Next .



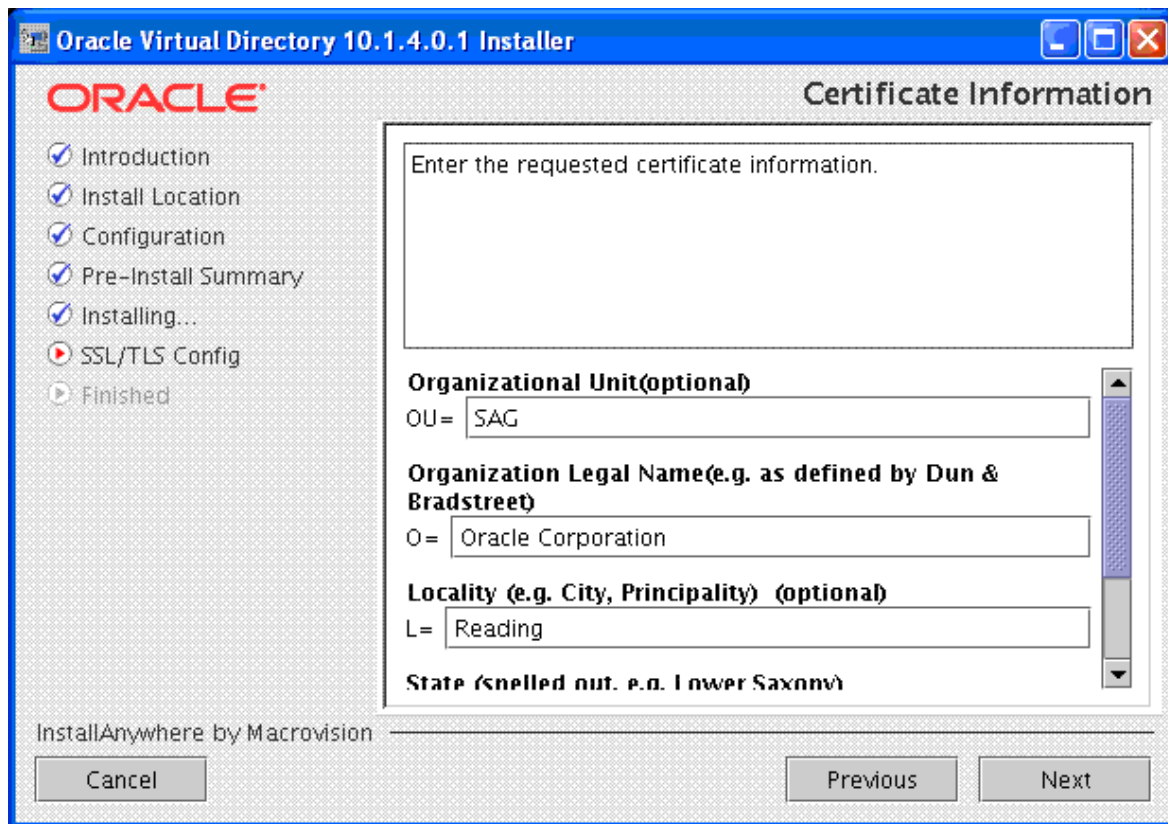
Review and click Install.



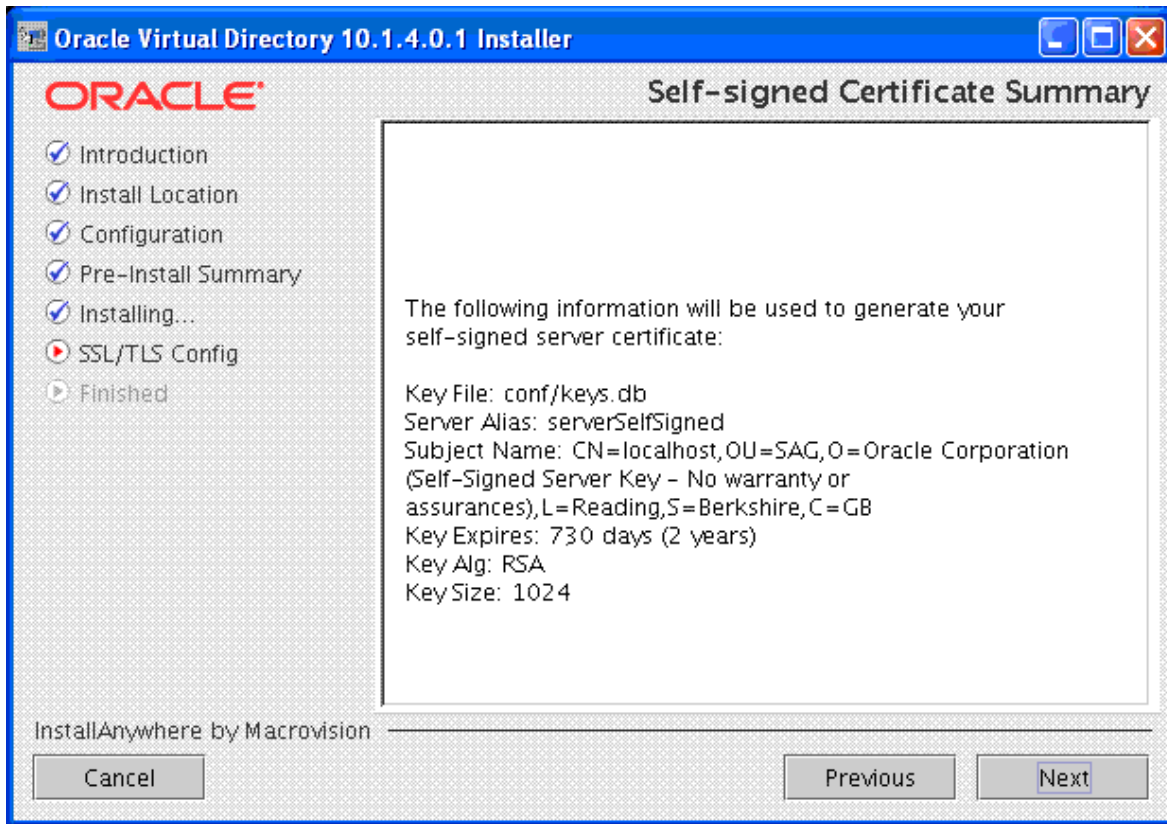
Click Next.



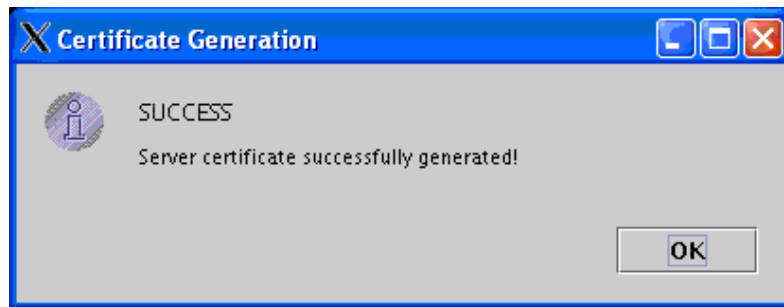
Enter the server host name and click Next .



Enter Certificate Information. Click Next .



Click Next.



Click OK.

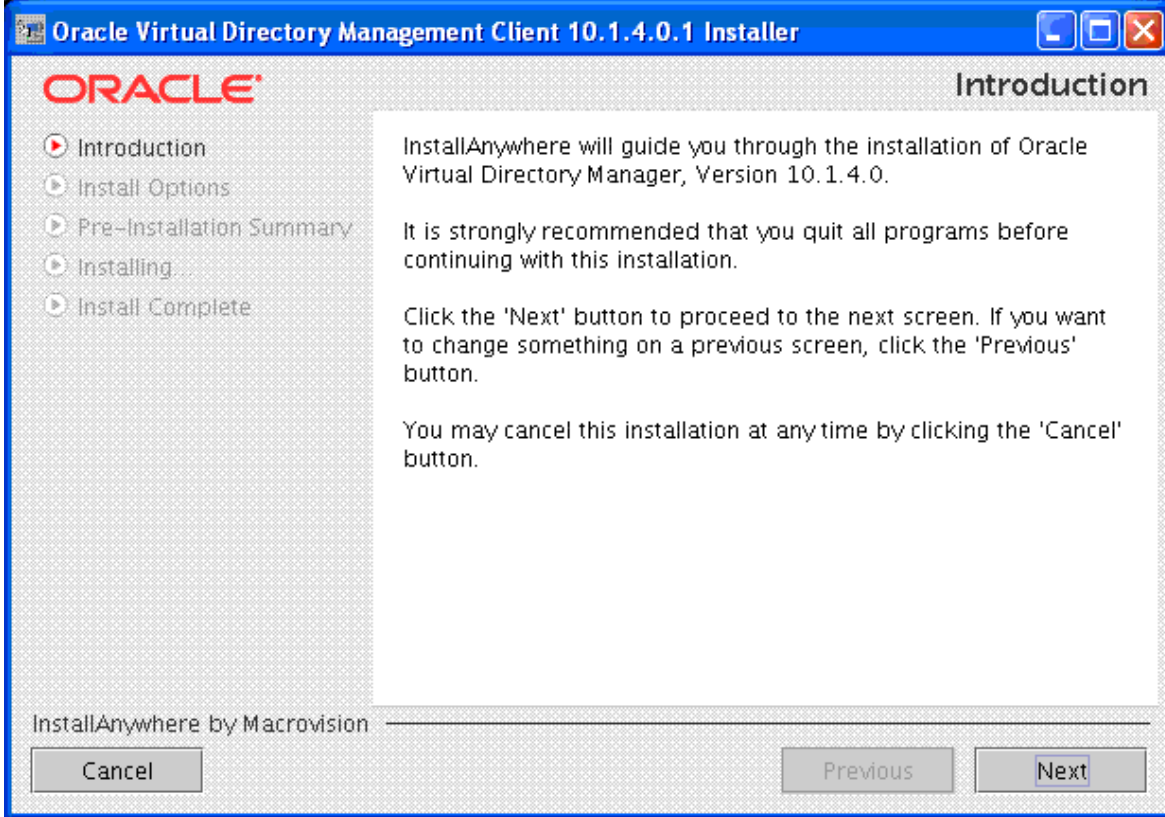
The final screen will be displayed confirming the Installation is complete. Click the "Done" button and then start the server as follows:

```
$ cd /space/oracle/product/10.1.4/OvID
$ ./vde.sh start
```

2.4 Installing OVD Manager

Navigate to the `/space/src/oracle/OVD/manager/linux` directory and run the following to start the installation:

```
$ chmod 744 ovidm1014.bin
$ ./ovidm1014.bin
```



During Installation the Installer will run through the stages listed on the left hand side of the above screen shot. Inputs are required for the following:

Installation Folder:

`/space/oracle/product/10.1.4/OViDManager`

and

Workspace Folder:

`/space/oracle/product/10.1.4/OViDManager/workspace`

2.5 Configuring OVD Server

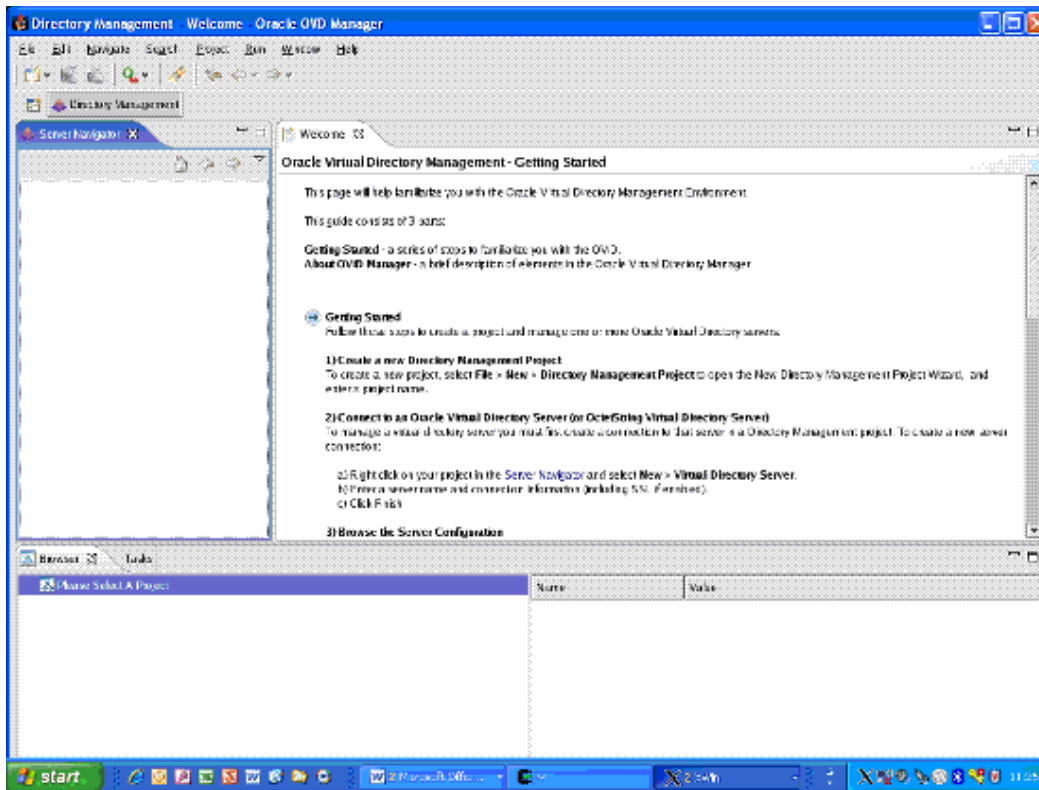
The initial configuration of OVD is most easily accomplished via OVD Manager.

To start OVD Manager navigate to the

`/space/oracle/product/10.1.4/OViDManager` directory and run the following command:

```
$ ./OViDManager
```

When OVD Manager first starts the following screen will appear:



Follow the instructions in the "Welcome" panel to create a Project.

Once created the project name will appear in the left-hand "Server Navigator" panel. Right click on the project and navigate to New > Virtual Directory server. Complete the required information as per the following:

New OVID Server

New OVID(VDE) Server

This wizard defines a new OVID(VDE) server to be managed through the server editor.

Local Document Information:

Document Folder: /OVD_ECD_Test

Server name: OVD_Test

Manage Existing Server

Existing OVID(VDE) Server To Be Managed:

Host DNS/IP: 5agDell4t

Admin Port: 8888

Admin DN: cn=Admin

Admin Pwd: *****

Secure

< Back Next > Finish Cancel

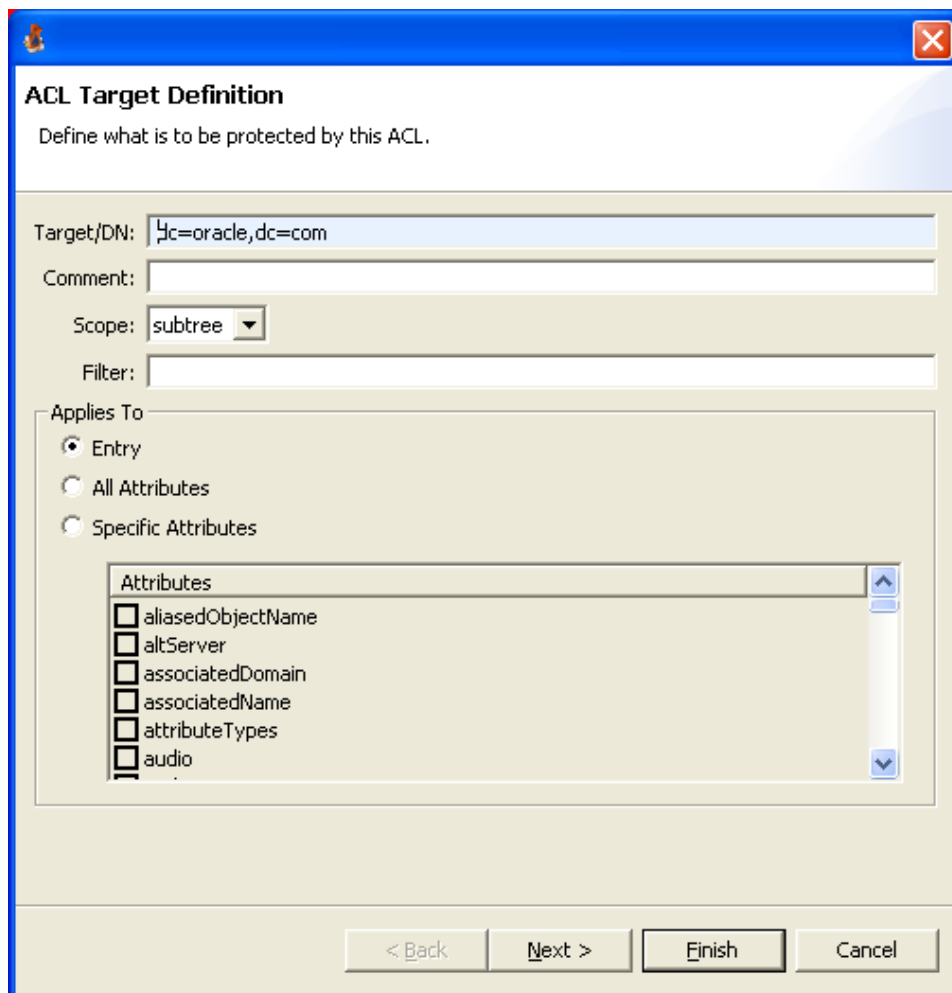
2.6 Configuring Access Controls

In the Server Navigator pane click on the Engine node and go to the Settings tab at the bottom of the main screen. Check that the Access Control checking Enabled check box is ticked.

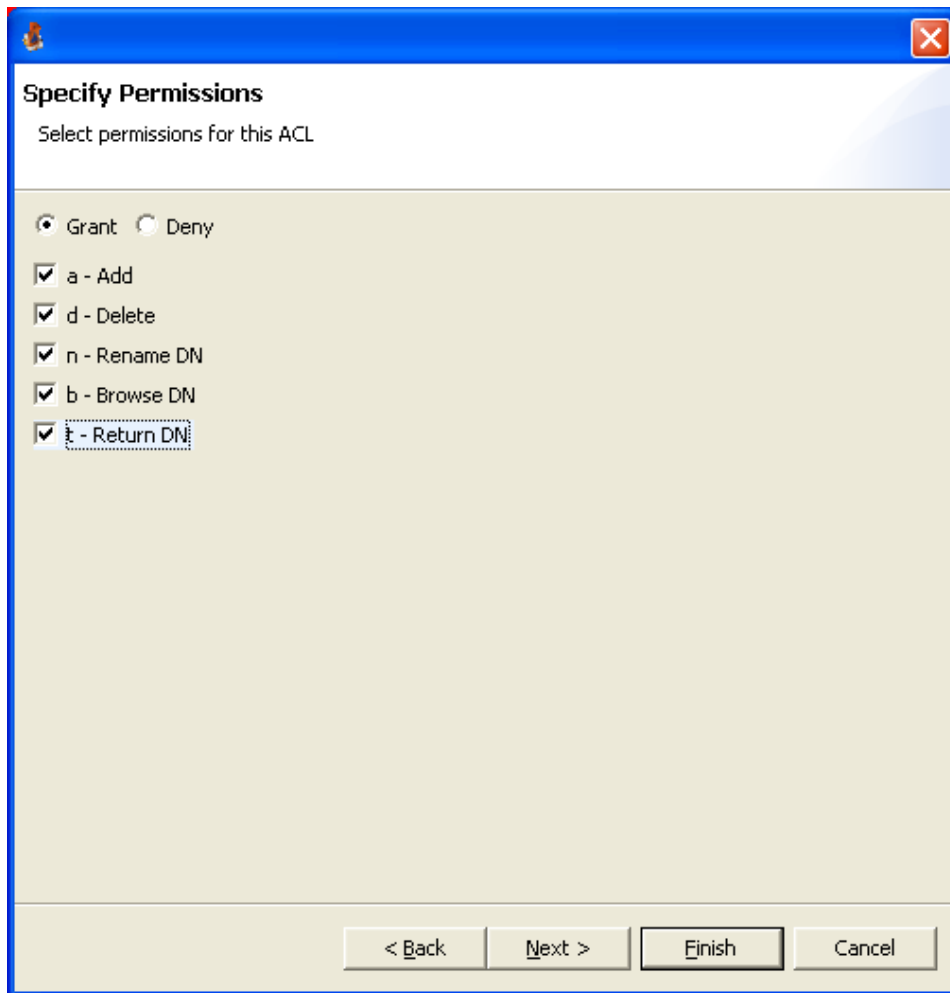
The next step is to create the Access Control rules.

Expand the Engine node in the Server Navigator pane, select the Access Control node and then select the ACLs tab at the bottom of the main screen.

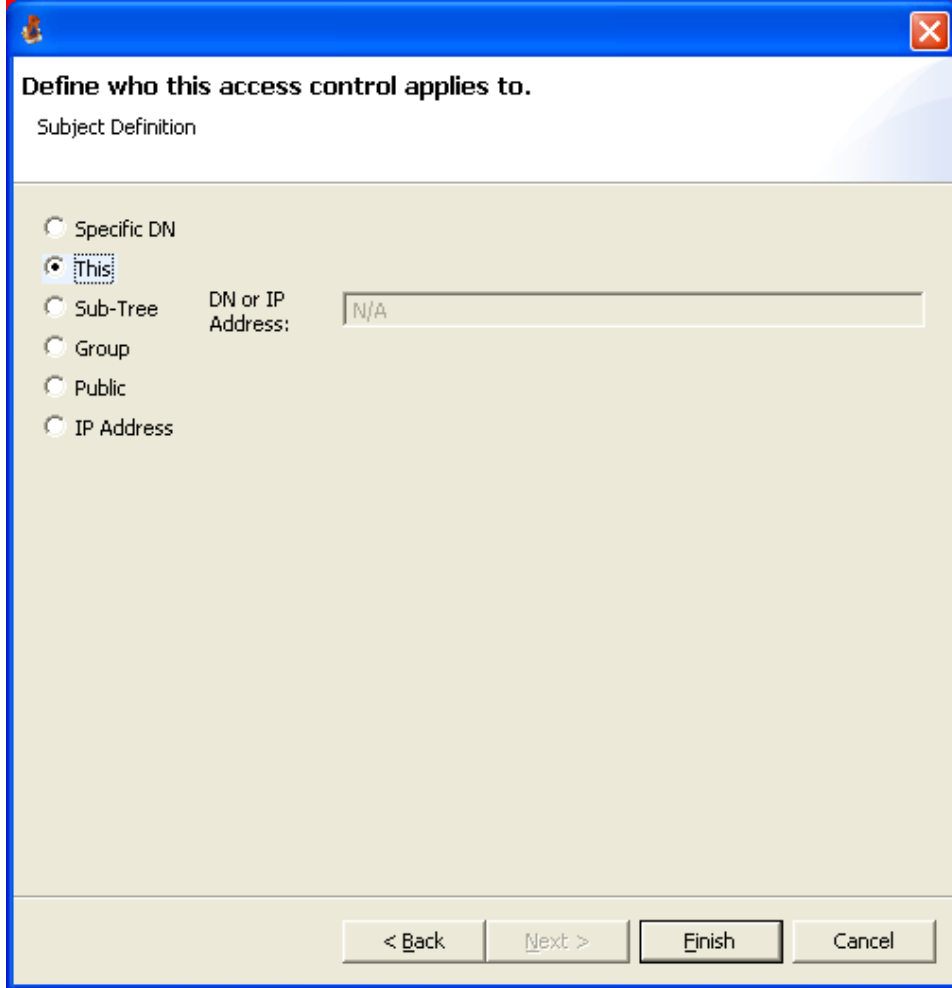
In the Access Control Rules screen click on the New ACL button.



Input the Target/DN, change the scope to subtree and click the Next button.

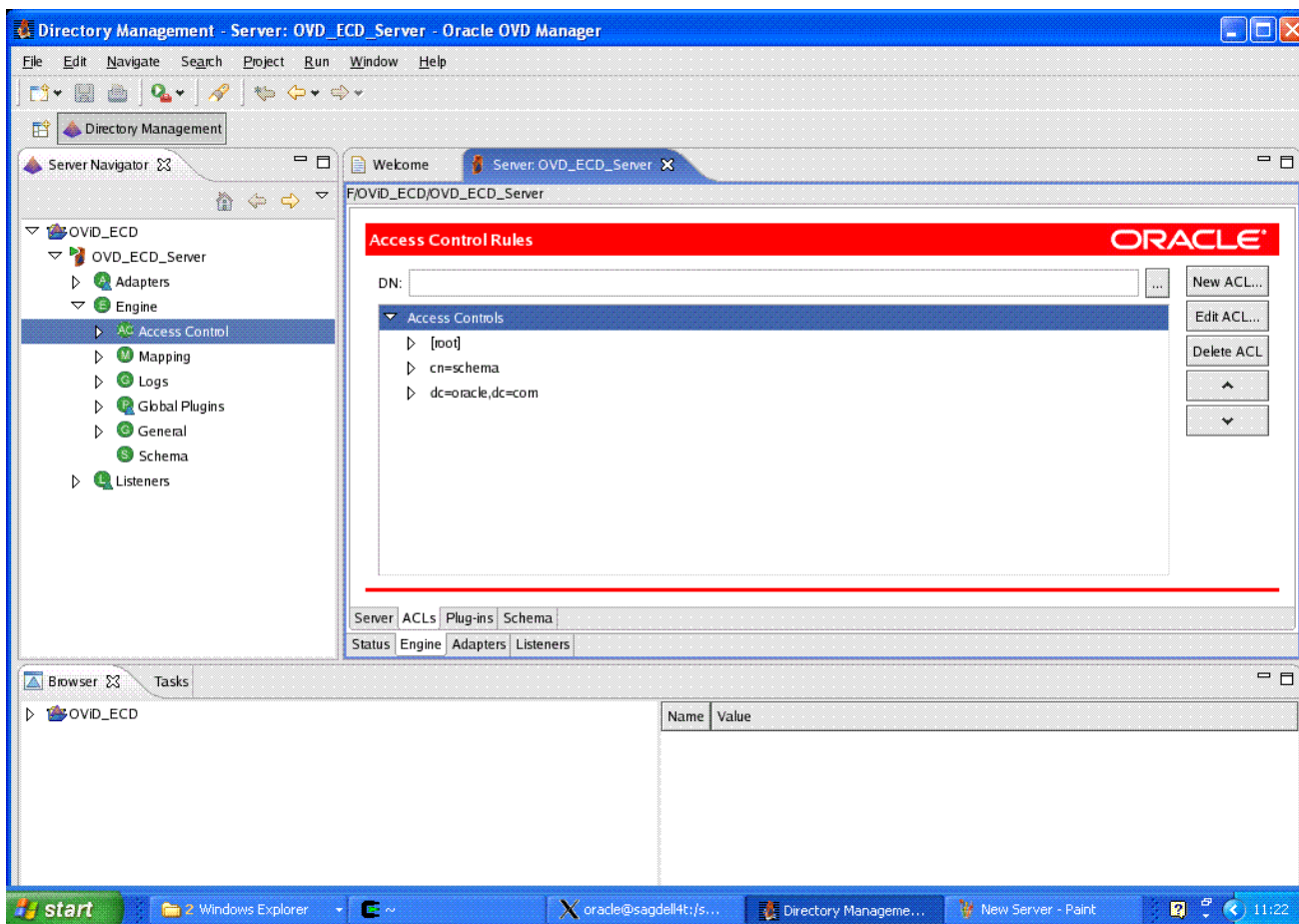


Select the Grant radio button then select all the check boxes and then select Next.



Select the radio button labelled "This", and then select Finish.

Create another Access Control Rule in exactly the same way as the above except in the first screen shot select the "Applies To" radio button to be "All Attributes":



Select the server in the Server Navigator pane, right click and select "Save All To Server".

Select OK at the "Please confirm" prompt and Select OK on the "Save Succeeded" prompt.

Access Controls have now been successfully configured.

2.7 Creating Adapters

In order to test the TOE in its Evaluated Configuration, OVD is used to virtualize two instances of OID servers that are both on the same physical machine. To provide a common search base, LDAP Adapters are to be used to map to each instance and a Local Store adapter is created to sit above these two.

To create the adapters, in the Server Navigation panel expand the server node to expose the Adapter, Engine and Listeners nodes.

Right click on the Adapters node. Select New -> LDAP Adapter.

Enter the details as per the following screenshot:

New LDAP Adapter

LDAP Proxy Remote Server Connection Information

Enter information necessary to allow the VDE to connect to the remote LDAP directory.

Server: /OVID_ECD/OVD_ECD_Server

Adapter Template: Oracle_Internet_Directory

Adapter Name: LDAP Adapter 1

DNS Host Discovery: No

	Server DNS/IP	Port	Load %	RW	
✓	sagde11st	389	100	TRU	Add

LDAP Servers:

Server Proxy Bind DN: cn=orcladmin

Proxy Password: *****

Pass Through Credentials: Always

Connection Options: Secure SSL/TLS Kerberos Bind

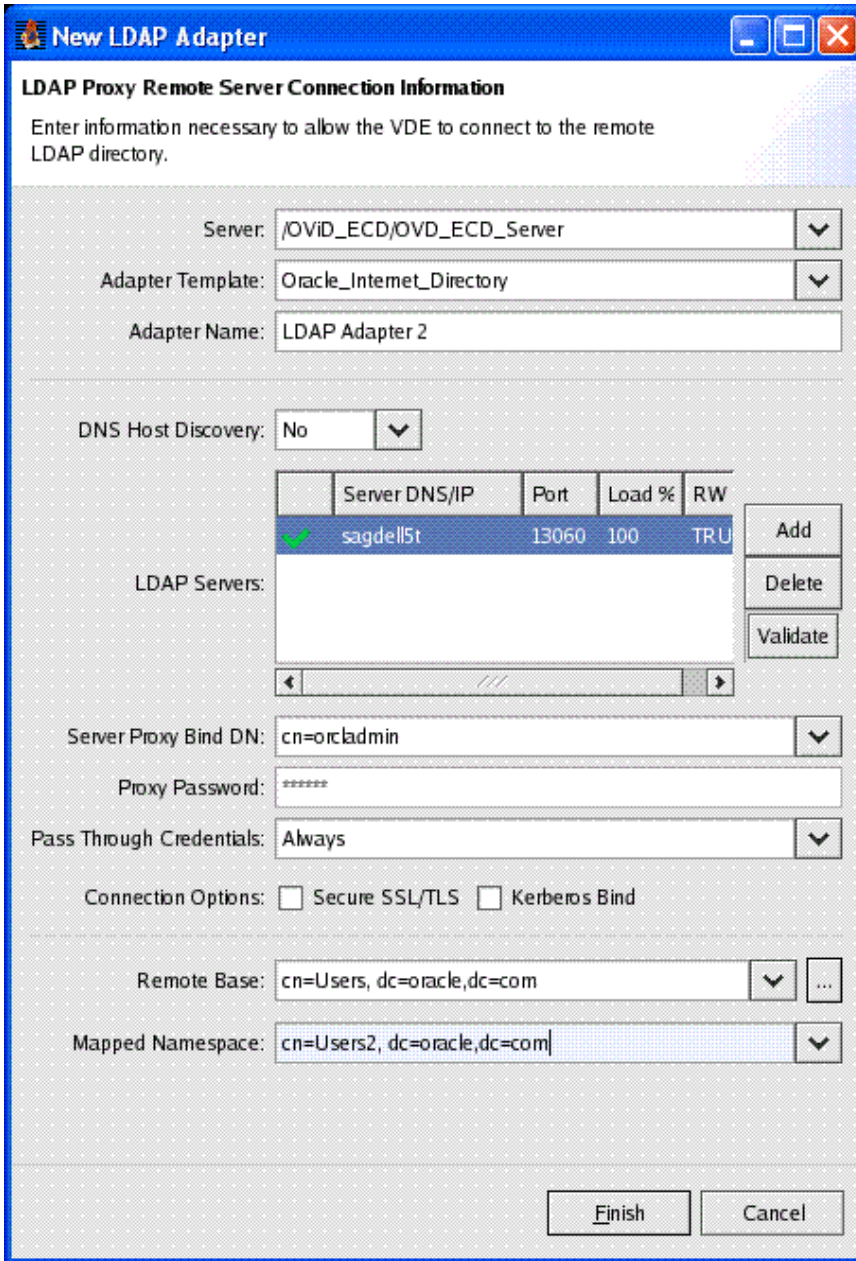
Remote Base: cn=Users, dc=oracle, dc=com

Mapped Namespace: cn=Users, dc=oracle, dc=com

Finish Cancel

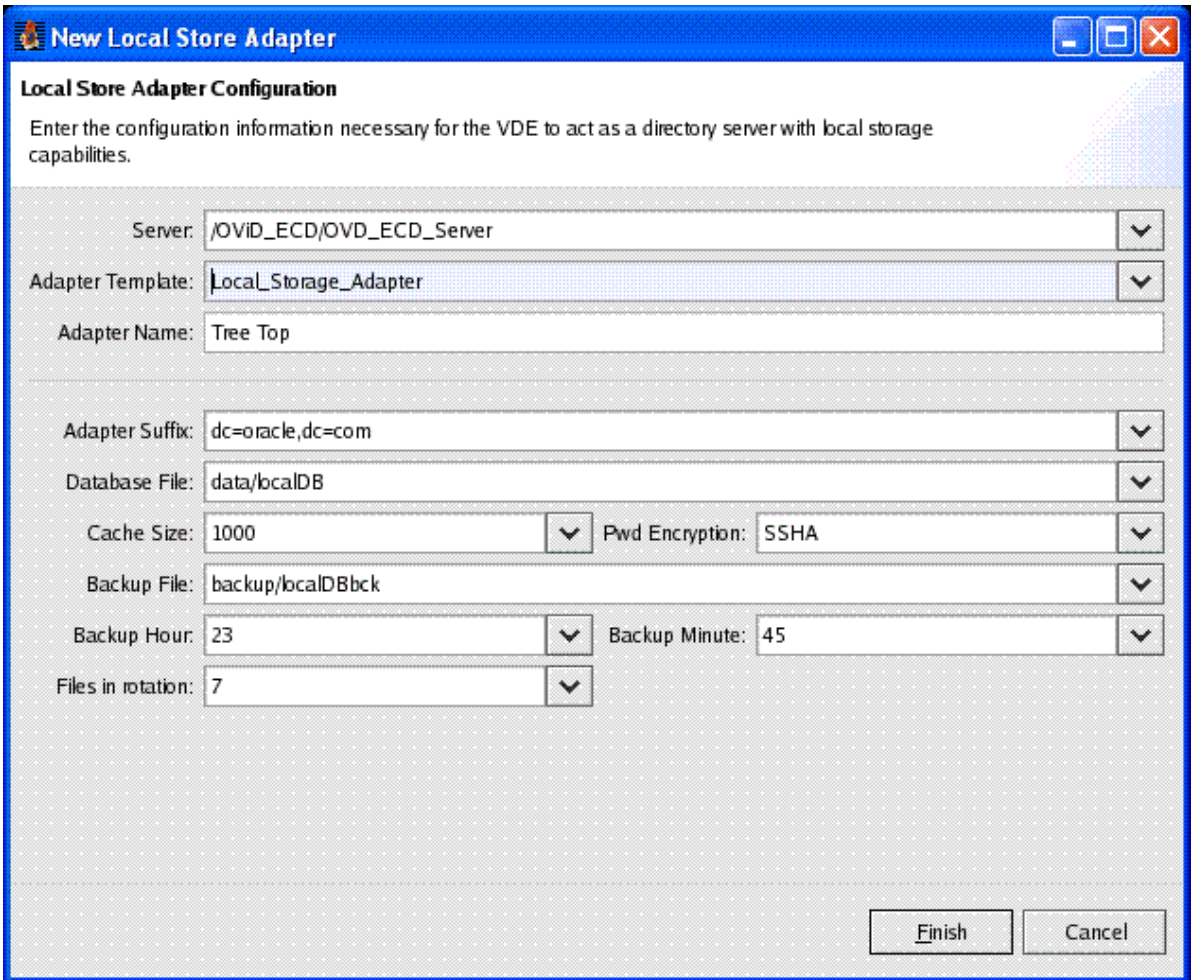
Note that before clicking the Validate button, the LDAP Server information, the Server Proxy Bind DN and the Proxy Password fields should be completed. Once the LDAP server has passed the validation the Remote Base field can be expanded to show the LDAP tree of the LDAP server.

Repeat for the second LDAP adapter:



Note the Port number is not the standard 389 and the Mapped Namespace has been changed so it forms a distinct part of the DIT.

Now create a Local Store Adapter:



Expose the Tree Top adapter to clients by hiding the OID and Database adapters so that all client connections come through the local store adapter. To do so, unset the visibility attribute from the routing section of the 2 LDAP adapters.

Save All to server.

To complete the configuration of OVD, an LDAP object needs to be created for the DN of the Tree Top "Adapter Suffix" (in the above screen shot). This is easily achieved via standard LDAP tools.

On the server create a file (`treetop.ldif`) in the `/home/oracle` directory:

```
version: 1
dn: dc=oracle,dc=com
objectclass: domain
objectclass: top
dc: oracle
```

Ensure the ORACLE_HOME is set to the correct path.

```
$cd $ORACLE_HOME/bin
```

```
$. /ldapadd -D cn=admin -w oral0g -h localhost -p 1389 -f  
/home/oracle/treetop.ldif
```

The OVD configuration is now complete.