

Oracle9i

Security and Network Integration Guide

Release 2 (9.2) for Windows

March 2002

Part No. A95492-01

ORACLE®

Oracle9i Security and Network Integration Guide, Release 2 (9.2) for Windows

Part No. A95492-01

Copyright © 1996, 2002 Oracle Corporation. All rights reserved.

Primary Authors: Craig B. Foch and Herbert Kelly III

Contributors: Toby Close, David Colello, Mark Kennedy, Chithra Ganesh Ramamurthy, Helen Slattery, and Deborah Steiner

The Programs (which include both the software and documentation) contain proprietary information of Oracle Corporation; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent and other intellectual and industrial property laws. Reverse engineering, disassembly or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained 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. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Oracle Corporation.

If the Programs are delivered to the U.S. Government or anyone licensing or using the programs on behalf of the U.S. Government, the following notice is applicable:

Restricted Rights Notice Programs delivered subject to the DOD FAR Supplement are "commercial computer software" and use, duplication, and disclosure of the Programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, Programs delivered subject to the Federal Acquisition Regulations are "restricted computer software" and use, duplication, and disclosure of the Programs shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software - Restricted Rights (June, 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and Oracle Corporation disclaims liability for any damages caused by such use of the Programs.

Oracle is a registered trademark, and Oracle Names, Oracle Store, Oracle7, Oracle8, Oracle8i, Oracle9i, Oracle*MetaLink*, PL/SQL, and SQL*Plus are trademarks or registered trademarks of Oracle Corporation. Other names may be trademarks of their respective owners.

Contents

Send Us Your Comments	vii
Preface.....	ix
Audience	x
Organization.....	x
Related Documentation	xi
Conventions.....	xii
Documentation Accessibility	xviii
What's New in Oracle9i for Windows.....	xix
Oracle9i Release 2 (9.2) New Features.....	xix
Oracle9i Release 1 (9.0.1) New Features.....	xx
1 Authenticating Database Users with Windows	
Windows Native Authentication Overview	1-2
Windows Authentication Protocols	1-2
User Authentication and Role Authorization Methods.....	1-4
Authentication and Authorization Methods To Use.....	1-5
Oracle9i Integration with Active Directory	1-5
Task 1: Install and Configure Components.....	1-6
Task 2: Set Registry Parameter OSAUTH_X509_NAME.....	1-6
Task 3: Start and Use Oracle Enterprise Security Manager	1-7
Using Oracle9i Directory Server Features with Active Directory.....	1-7
Operating System Authentication Enabled at Installation	1-8

2 Administering External Users and Roles

Using Oracle Administration Assistant for Windows NT	2-2
Managing a Remote Computer	2-3
Adding a Computer and Saving Your Configuration	2-4
Granting Administrator Privileges for All Databases on a Computer	2-5
Granting Operator Privileges for All Databases on a Computer	2-7
Connecting to a Database	2-8
Troubleshooting Connection Problems	2-10
Viewing Database Authentication Parameter Settings	2-12
Creating an External OS User	2-13
Creating a Local Database Role	2-18
Creating an External OS Role	2-22
Granting Administrator Privileges for a Single Database	2-26
Granting Operator Privileges for a Single Database	2-28
Manually Administering External Users and Roles	2-30
Manually Creating an External OS User	2-30
External User Authentication Tasks on the Oracle9i Database Server	2-31
External User Authentication Tasks on the Client Computer	2-34
Manually Granting Administrator and Operator Privileges for Databases	2-36
SYSDBA/SYSOPER Authentication Tasks on the Oracle9i Database Server	2-37
SYSDBA/SYSOPER Authentication Tasks on the Client Computer	2-39
Manually Creating an External Role	2-40
External Role Authorization Tasks on the Oracle9i Database Server	2-41
External Role Authorization Tasks on the Client Computer	2-45
Manually Migrating Users	2-46

3 Administering Enterprise Users and Roles

Enterprise User Authentication	3-2
Enterprise Role Authorization	3-2

4 Storing Oracle Wallets in the Windows Registry

Storing Private Keys and Trust Points	4-2
Storing User's Profile	4-2
Registry Parameters for Wallet Storage	4-2

Oracle Wallet Manager	4-3
Oracle Enterprise Login Assistant	4-4
Wallet Resource Locator	4-5

5 Windows 2000 PKI Integration

Oracle Public Key Infrastructure	5-2
Windows Public Key Infrastructure	5-2
Microsoft Certificate Stores	5-3
Microsoft Certificate Services	5-3
Wallet Resource Locator	5-4

A Oracle Net Services Configuration

Understanding Oracle Net Services Registry Parameter and Subkeys	A-2
Oracle Net Service Subkeys	A-2
Listener Requirements	A-2
Understanding Optional Configuration Parameters	A-3
LOCAL.....	A-3
TNS_ADMIN.....	A-3
USE_SHARED_SOCKET.....	A-4
Advanced Network Configuration	A-4
Configuring Authentication Method.....	A-4
Configuring Security for Named Pipes Protocol	A-4

Glossary

Index

Send Us Your Comments

Oracle9i Security and Network Integration Guide, Release 2 (9.2) for Windows

Part No. A95492-01

Oracle Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, please indicate the document title and part number, and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: ntdoc_us@oracle.com
- FAX: (650) 506-7365 Attn: Oracle Database for Windows Documentation
- Postal service:
Oracle Corporation
Oracle Database for Windows Documentation Manager
500 Oracle Parkway, Mailstop 1op6
Redwood Shores, CA 94065
USA

If you would like a reply, please give your name, address, telephone number, and (optionally) electronic mail address.

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This guide is your primary source of introductory, post-installation, configuration, and administration information for using Oracle9*i* security and network features for Windows operating systems.

This guide describes only the features of Oracle9*i* for Windows software that apply to the Windows NT, Windows 2000, Windows XP, and Windows 98 operating systems. Information on Oracle9*i* Personal Edition software on Windows 98 is not covered in this guide.

This preface contain these topics:

- [Audience](#)
- [Organization](#)
- [Related Documentation](#)
- [Conventions](#)
- [Documentation Accessibility](#)

Audience

Oracle9i Security and Network Integration Guide for Windows is intended for anyone configuring or administering Oracle9i network, directory, and security features for Windows operating systems.

To use this document, you need:

- Windows NT or Windows 2000 installed and tested on your computer system
- Knowledge of object-relational database management concepts

Organization

This guide is organized as follows:

"What's New in Oracle9i for Windows"

Oracle9i release 2 (9.2) adds support for very large memory configurations and User Migration Utility, a new command-line tool. Oracle9i release 1 (9.0.1) added support for Windows XP Professional Edition, enhanced integration with Windows, and improvements in Database Configuration Assistant and Oracle Internet Directory administration. Server Manager and `CONNECT INTERNAL` were desupported in Oracle9i release 1 (9.0.1).

Chapter 1, "Authenticating Database Users with Windows"

This chapter describes authentication of Oracle9i database users on Windows operating systems.

Chapter 2, "Administering External Users and Roles"

This chapter describes the administration of external users and roles.

Chapter 3, "Administering Enterprise Users and Roles"

This chapter describes the administration of enterprise users and roles.

Chapter 4, "Storing Oracle Wallets in the Windows Registry"

This chapter describes the storing and retrieving of Oracle Wallets in the Windows registry.

Chapter 5, "Windows 2000 PKI Integration"

This chapter describes the integration of Oracle public key infrastructure (PKI) with Windows 2000 public key infrastructure (Windows PKI) on Windows operating systems.

Appendix A, "Oracle Net Services Configuration"

This appendix describes Oracle Net Services configuration for Windows. For an overview of Oracle Net Services configuration in general, see *Oracle9i Net Services Administrator's Guide*.

Glossary

Related Documentation

For more information, see these Oracle resources:

- *Oracle9i Database Installation Guide for Windows*
- *Oracle9i Database Release Notes for Windows*
- *Oracle9i Database Administrator's Guide for Windows*
- *Oracle Advanced Security Administrator's Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Enterprise Manager Administrator's Guide*
- *Oracle9i Net Services Administrator's Guide*
- *Oracle9i Database New Features*
- *Oracle9i Database Reference*

In North America, printed documentation is available for sale in the Oracle Store at

<http://oraclestore.oracle.com/>

Customers in Europe, the Middle East, and Africa (EMEA) can purchase documentation from

<http://www.oraclebookshop.com/>

Other customers can contact their Oracle representative to purchase printed documentation.

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at

<http://otn.oracle.com/admin/account/membership.html>

If you already have a username and password for OTN, then you can go directly to the documentation section of the OTN Web site at

<http://otn.oracle.com/docs/index.htm>

To access the database documentation search engine directly, please visit

<http://tahiti.oracle.com>

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- [Conventions in Text](#)
- [Conventions in Code Examples](#)
- [Conventions for Windows Operating Systems](#)

Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an index-organized table .
<i>Italics</i>	Italic typeface indicates book titles or emphasis.	<i>Oracle9i Database Concepts</i> Ensure that the recovery catalog and target database do <i>not</i> reside on the same disk.

Convention	Meaning	Example
UPPERCASE monospace (fixed-width) font	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a NUMBER column. You can back up the database by using the BACKUP command. Query the TABLE_NAME column in the USER_TABLES data dictionary view. Use the DBMS_STATS.GENERATE_STATS procedure.
lowercase monospace (fixed-width) font	Lowercase monospace typeface indicates executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, usernames and roles, program units, and parameter values. Note: Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter sqlplus to open SQL*Plus. The password is specified in the orapwd file. Back up the datafiles and control files in the /disk1/oracle/dbs directory. The department_id, department_name, and location_id columns are in the hr.departments table. Set the QUERY_REWRITE_ENABLED initialization parameter to true. Connect as oe user. The JRepUtil class implements these methods.
<i>lowercase italic monospace (fixed-width) font</i>	Lowercase italic monospace font represents placeholders or variables.	You can specify the <i>parallel_clause</i> . Run <i>Uold_release</i> .SQL where <i>old_release</i> refers to the release you installed prior to upgrading.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
[]	Brackets enclose one or more optional items. Do not enter the brackets.	DECIMAL (<i>digits</i> [, <i>precision</i>])
{ }	Braces enclose two or more items, one of which is required. Do not enter the braces.	{ENABLE DISABLE}
	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	{ENABLE DISABLE} [COMPRESS NOCOMPRESS]
...	Horizontal ellipsis points indicate either: <ul style="list-style-type: none"> That we have omitted parts of the code that are not directly related to the example That you can repeat a portion of the code 	CREATE TABLE ... AS <i>subquery</i> ; SELECT <i>col1</i> , <i>col2</i> , ... , <i>coln</i> FROM employees;
.	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	SQL> SELECT NAME FROM V\$DATAFILE; NAME ----- /fsl/dbs/tbs_01.dbf /fsl/dbs/tbs_02.dbf . . . /fsl/dbs/tbs_09.dbf 9 rows selected.
Other notation	You must enter symbols other than brackets, braces, vertical bars, and ellipsis points as shown.	acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;
<i>Italics</i>	Italicized text indicates placeholders or variables for which you must supply particular values.	CONNECT SYSTEM/ <i>system_password</i> DB_NAME = <i>database_name</i>
UPPERCASE	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	SELECT last_name, employee_id FROM employees; SELECT * FROM USER_TABLES; DROP TABLE hr.employees;

Convention	Meaning	Example
lowercase	Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files. Note: Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	<pre>SELECT last_name, employee_id FROM employees; sqlplus hr/hr CREATE USER mjones IDENTIFIED BY ty3MU9;</pre>

Conventions for Windows Operating Systems

The following table describes conventions for Windows operating systems and provides examples of their use.

Convention	Meaning	Example
Choose Start >	How to start a program. For example, to start Database Configuration Assistant, you must click the Start button on the taskbar and then choose Programs > Oracle - <i>HOME_NAME</i> > Configuration and Migration Tools > Database Configuration Assistant.	Choose Start > Programs > Oracle - <i>HOME_NAME</i> > Configuration and Migration Tools > Database Configuration Assistant
File and Directory Names	File/directory names are not case sensitive. The special characters <, >, :, ", /, , and - are not allowed. The special character \ is treated as an element separator, even when it appears in quotes. If the file name begins with \\, Windows assumes it uses the Universal Naming Convention.	c:\winnt "\"system32 is the same as C:\WINNT\SYSTEM32
C:\>	Represents the Windows command prompt of the current hard disk drive. The escape character in a command prompt is "^". Your prompt reflects the subdirectory in which you are working. Referred to as the command prompt in this guide.	C:\oracle\oradata>
Special characters	The backslash special character (\) is sometimes required as an escape character for the double quote (") special character at the Windows command prompt. Parentheses and the single quote (') do not require an escape character. See your Windows operating system documentation for more information on escape and special characters.	C:\>exp scott/tiger TABLES=emp QUERY=\"WHERE job='SALESMAN' and sal<1600\" C:\>imp SYSTEM/ <i>password</i> FROMUSER=scott TABLES=(emp, dept)
<i>HOME_NAME</i>	Represents the Oracle home name. The home name can be up to 16 alphanumeric characters. The only special character allowed in the home name is the underscore.	C:\> net start Oracle <i>HOME_NAME</i> TNSListener

Convention	Meaning	Example
<i>ORACLE_HOME</i> and <i>ORACLE_BASE</i>	<p>In releases prior to Oracle8i release 8.1.3, when you installed Oracle components, all subdirectories were located under a top level <i>ORACLE_HOME</i> directory that by default was:</p> <ul style="list-style-type: none"> ■ C:\orant for Windows NT ■ C:\orawin98 for Windows 98 <p>or whatever you called your Oracle home.</p> <p>This release complies with Optimal Flexible Architecture (OFA) guidelines. All subdirectories are not under a top level <i>ORACLE_HOME</i> directory. There is a top level directory called <i>ORACLE_BASE</i> that by default is C:\oracle. If you install the latest Oracle release on a computer with no other Oracle software installed, then the default setting for the first Oracle home directory is C:\oracle\orann where <i>nn</i> is the latest release number. The Oracle home directory is located directly under <i>ORACLE_BASE</i>.</p> <p>All directory path examples in this guide follow OFA conventions.</p> <p>See <i>Oracle9i Database Getting Started for Windows</i> for additional information on OFA compliances and for information on installing Oracle products in non-OFA compliant directories.</p>	Go to the <i>ORACLE_BASE\ORACLE_HOME\rdcms\admin</i> directory.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation JAWS, a Windows screen reader, may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, JAWS may not always read a line of text that consists solely of a bracket or brace.

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

What's New in Oracle9i for Windows

This section describes new features of Oracle9i release 2 (9.2) and provides pointers to additional information. New features information from the previous release is also retained to help those users migrating to the current release.

The following sections describe new features:

- [Oracle9i Release 2 \(9.2\) New Features](#)
- [Oracle9i Release 1 \(9.0.1\) New Features](#)

Oracle9i Release 2 (9.2) New Features

This section contains these topics:

- [Very Large Memory Support](#)
- [User Migration Utility](#)

Very Large Memory Support

Oracle9i release 2 (9.2) for Windows supports Very Large Memory (VLM) configurations in Windows 2000 and Windows XP, which allows Oracle9i release 2 (9.2) to access more than 4 gigabyte (GB) of RAM traditionally available to Windows applications. For more information, see "Oracle Scalability on Windows" in *Oracle9i Database Getting Started for Windows*.

User Migration Utility

A new command-line tool, User Migration Utility, simplifies conversion of local or external database users to enterprise users. For more information, see:

- "Database Tools Overview" in *Oracle9i Database Getting Started for Windows*

- ["Manually Migrating Users"](#) on page 2-46
- ["Migrating Local or External Users to Enterprise Users"](#) in *Oracle Advanced Security Administrator's Guide*

Oracle9i Release 1 (9.0.1) New Features

This section contains these topics:

- [Windows XP Support](#)
- [Windows Integration](#)
- [Database Configuration Assistant Improvements](#)
- [Oracle Internet Directory Administration Improvements](#)
- [Using Oracle9i on Windows 2000](#)
- [CONNECT INTERNAL Not Supported](#)
- [Server Manager Not Supported](#)

Windows XP Support

Oracle9i release 1 (9.0.1.1.1) for Windows is certified on the 32-bit version of Windows XP Professional Edition.

Oracle Corporation provides support information for components on various platforms, lists compatible client and database versions, and identifies patches and workaround information. Find latest certification information at:

<http://metalink.oracle.com/>

You must register online before using Oracle*MetaLink*. After logging into Oracle*MetaLink*, select Product Lifecycle from the left-hand column.

Windows Integration

Oracle9i supports enhanced integration with Microsoft Transaction Services and Internet Information Services. Public key infrastructure and Single Sign-On capabilities in Oracle9i have also been integrated with Windows 2000, Active Directory, and Microsoft Certificate Store.

Oracle9i integration with Windows security supports Oracle Wallets in the registry and Active Directory, and it allows Oracle products to use Microsoft Certificate Store.

Synchronization between Active Directory and Oracle Internet Directory facilitates centralized scheduling and configuration of Oracle and third party meta-directory components.

Database Configuration Assistant Improvements

Database Configuration Assistant has been redesigned to include database definitions saved as templates. The templates can generate databases. Users can define new templates, modify existing templates, or use the ones Oracle provides. When creating a database with Database Configuration Assistant, users can include Oracle's new Sample Schemas.

Oracle Internet Directory Administration Improvements

Administration of Oracle Internet Directory replication server has been improved with addition of new replication queue management and reconciliation tools.

Using Oracle9i on Windows 2000

There are some differences between using Oracle9i on Windows 2000 and Windows NT 4.0. For more information, see "Using Oracle9i on Windows 2000" in *Oracle9i Database Getting Started for Windows*

CONNECT INTERNAL Not Supported

CONNECT INTERNAL and CONNECT INTERNAL/PASSWORD are not supported in Oracle9i. Use the following instead:

```
CONNECT / AS SYSDBA
CONNECT username/password AS SYSDBA
```

Server Manager Not Supported

Server Manager is not supported in Oracle9i. Use SQL*Plus instead. Most Server Manager scripts should work in a SQL*Plus environment, but some scripts may need to be modified.

Authenticating Database Users with Windows

This chapter describes authentication of Oracle9i database users with Windows operating systems.

This chapter contains these topics:

- [Windows Native Authentication Overview](#)
- [Windows Authentication Protocols](#)
- [User Authentication and Role Authorization Methods](#)
- [Operating System Authentication Enabled at Installation](#)

Windows Native Authentication Overview

Oracle9i database can use Windows user login **credentials** to **authenticate** database users. Benefits include:

- Enabling users to connect to Oracle9i databases without supplying a **username** or password
- Centralizing Oracle9i database user authentication and role **authorization** information in Windows NT or Windows 2000, which frees Oracle9i from storing or managing user passwords or **role** information

The Windows native authentication adapter (automatically installed with **Oracle Net Services**) enables database user authentication through Windows NT or Windows 2000. This enables client computers to make secure connections to an Oracle9i database on a Windows NT or Windows 2000 server. The server then permits the user to perform database actions on the server.

Note: This chapter describes using Windows native authentication methods with Windows NT 4.0 and Windows 2000. For information on Secure Sockets Layer (SSL) protocol and Oracle Internet Directory, see *Oracle Advanced Security Administrator's Guide* and *Oracle Internet Directory Administrator's Guide*.

Windows Authentication Protocols

The Windows native authentication adapter works with Windows authentication protocols to enable access to your Oracle9i database.

- Kerberos is the default authentication protocol for Windows 2000.
- NT LAN Manager (NTLM) is the default protocol for Windows NT 4.0.

If the user is logged on as a Windows 2000 domain user from a Windows 2000 computer, then Kerberos is the authentication mechanism used by the NTS adapter.

For all other users (local users, Windows NT 4.0 domain users, Windows 95 users, and Windows 98 users), NTLM is the authentication mechanism used by the NTS adapter.

If authentication is set to NTS on a standalone Windows 2000 or Windows NT 4.0 computer, ensure that Windows Service NT LM Security Support Provider is started. If this **service** is not started on a standalone Windows 2000 or Windows NT

4.0 computer, then NTS authentication fails. This issue is applicable only if you are running Windows 2000 or Windows NT 4.0 in standalone mode.

Client computers do not need to specify an authentication protocol when attempting a connection to an Oracle9i database. Instead, Oracle9i database determines the protocol to use, completely transparent to the user. The only Oracle requirement is to ensure that parameter `SQLNET.AUTHENTICATION_SERVICES` contains `nts` in the following file on both the client and database server:

```
ORACLE_BASE\ORACLE_HOME\network\admin\sqlnet.ora
```

This is the default setting for both after installation. For Oracle8 8.0 releases, you must manually set this value.

If typical, your Oracle9i database network includes client computers and database servers, and computers on this network may use different Oracle software releases on different Windows operating systems on different domains. For example, you may be running an Oracle release 8.0.5 client installed on Windows 95 that connects to an Oracle9i database installed on a Windows NT 4.0 computer that runs in a Windows 2000 domain. This combination of different releases means that the authentication protocol being used can vary.

[Table 1-1](#) lists Oracle software and Windows operating system releases required to enable Kerberos as the default authentication protocol:

Table 1-1 Software Requirements to Enable Kerberos Authentication Protocol

Location	Windows Software	Oracle Software
Client Computer	Windows NT 4.0 or Windows 2000	Oracle8i Client or later
Database Computer	Windows NT 4.0 or Windows 2000	Oracle8i Database or later
Domain	Windows 2000	None

For *all* other combinations of Windows operating system and Oracle software releases used in your network, the authentication protocol used is NTLM.

See Also: Microsoft Windows documentation for more information on each authentication protocol

User Authentication and Role Authorization Methods

This section describes how user login credentials are authenticated and database roles are authorized in Windows NT 4.0 or Windows 2000 domains. User authentication and role authorization are defined in [Table 1–2](#).

Table 1–2 User Authentication and Role Authorization Defined

Feature	Description	More Information
User authentication	Process by which the database uses the user's Windows login credentials to authenticate the user.	<i>Oracle9i Database Administrator's Guide</i>
Role authorization	Process of granting an assigned set of roles to authenticated users.	<i>Oracle9i Database Administrator's Guide</i>

Oracle supports user authentication and role authorization in Windows NT 4.0 domains. [Table 1–3](#) provides descriptions of these basic features.

Table 1–3 Basic Features of User Authentication and Role Authorization

Feature	Description
Authentication of external users	Users are authenticated by the database using the user's Windows login credentials enabling them to access Oracle9i database without being prompted for additional login credentials.
Authorization of external roles	Roles are authorized using Windows NT local groups . Once an external role is created, you can grant or revoke that role to a database user. Initialization parameter <code>OS_ROLES</code> is set to <code>false</code> by default. You must set <code>OS_ROLES</code> to <code>true</code> to authorize external roles.

For Oracle8i release 8.1.6 or later, enhancements were made to support **enterprise user** authentication and **enterprise role** authorization. Enhancements were also made to support Windows native authentication in Windows 2000 domains, and in Active Directory in addition to integration with Oracle Internet Directory. These enhancements are available *only* if you:

- Configure Oracle8i release 8.1.6 or later release to work with Active Directory
- Are running Oracle8i Client release 8.1.6 or later and Oracle8i database or later in a Windows 2000 domain

Enterprise user authentication (also called global user authentication) is enabled by setting **registry** parameter `OSAUTH_X509_NAME` to `true` on the computer on which Oracle9i database is running in a Windows 2000 domain. If this parameter is set to

`false` (the default setting) in a Windows 2000 domain, then Oracle9i database authenticates the user as an **external user** (described in "[Enterprise User Authentication](#)" on page 3-2). Setting this parameter to `true` in a Windows NT 4.0 domain is meaningless and does *not* enable you to use enterprise users.

See Also: "[Enterprise User Authentication](#)" on page 3-2 for more information on using registry parameter `OSAUTH_X509_NAME`.

Authentication and Authorization Methods To Use

[Table 1-4](#) describes user authentication and role authorization methods to use based on your Oracle9i database environment:

Table 1-4 User Authentication and Role Authorization Methods

Method	Database Environment
Enterprise users and roles	<p>You have many users connecting to multiple databases.</p> <p>Enterprise users have the same identity across multiple databases. Enterprise users require use of a directory server.</p> <p>Use enterprise roles in environments where enterprise users assigned to these roles are located in many geographic regions and must access multiple databases. Each enterprise role can be assigned to more than one enterprise user in the directory. If you do not use enterprise roles, then you have to assign database roles manually to each database user. Enterprise roles require use of a directory server.</p>
External users and roles	<p>You have a smaller number of users accessing a limited number of databases. External users must be created individually in each database and do not require use of a directory server.</p> <p>External roles must also be created individually in each database, and do not require use of a directory server. External roles are authorized using group membership of the users in local groups on the system.</p>

Oracle9i Integration with Active Directory

Oracle9i integration with Active Directory enables you to take advantage of operating system user authentication and role authorization. Perform the following tasks to integrate Oracle components with Active Directory:

- [Task 1: Install and Configure Components](#)
- [Task 2: Set Registry Parameter `OSAUTH_X509_NAME`](#)
- [Task 3: Start and Use Oracle Enterprise Security Manager](#)

Note: Operating system user authentication and role authorization are available only if you are running in a Windows 2000 domain.

Task 1: Install and Configure Components

Read "Using Enterprise User Security with Microsoft Active Directory" in *Oracle Advanced Security Administrator's Guide* and *Oracle9i Database Installation Guide for Windows* for information on pre-installation and configuration issues.

Task 2: Set Registry Parameter OSAUTH_X509_NAME

Set registry parameter `OSAUTH_X509_NAME` to `true` to enable client users to access Oracle9i database as X.509-compliant enterprise users. Active Directory will then be used to identify the client username and authorize roles. This parameter setting is required *only* if you want to use enterprise users and roles.

When the parameter is set to `false` (the default setting), the client user is identified as an external user, and the user's role authorization uses the Oracle9i database **data dictionary**.

To set registry parameter `OSAUTH_X509_NAME`:

1. Go to the computer on which Oracle9i database is installed.
2. Choose Start > Run.
3. Enter `regedt32` in the Open field, and choose OK.

The Registry Editor window appears.

4. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOMEID`.

where *ID* is the Oracle home that you want to edit.

5. If registry value `OSAUTH_X509_NAME` exists, double-click `OSAUTH_X509_NAME`.

A String Editor dialog box appears.

Otherwise, add `OSAUTH_X509_NAME` as a registry value of type `REG_EXPAND_SZ`.

6. Click Enter.
7. Set the value to `true` in the String field.
8. Click OK.

9. Choose Exit from the Registry menu.

Registry Editor exits.

Task 3: Start and Use Oracle Enterprise Security Manager

Oracle Enterprise Security Manager is included as an integrated application with Oracle Enterprise Manager. You can use Oracle Enterprise Security Manager to create and manage enterprise users, roles, and domains. You can also use it to assign enterprise users and groups to enterprise roles.

See Also: *Oracle Advanced Security Administrator's Guide* for information on using Oracle Enterprise Security Manager

The administrator using Oracle Enterprise Security Manager must be a member of security group `OracleDBSecurityAdmin`. By default, the administrator who created the Oracle Context (that is, configured Oracle9i database to work with a directory server) is a member of this security group. Only members of this security group are authorized to use all features of Oracle Enterprise Security Manager. To add additional users manually, see "Access Control List Management for Oracle Directory Objects" in *Oracle Advanced Security Administrator's Guide*.

Select Login from the Directory Server main menu to access a dialog box for selecting the authentication protocol appropriate to your environment. Choose NT Native Authentication if you are running an Oracle9i database on a Windows NT 4.0 or Windows 2000 computer in a Windows 2000 domain with Active Directory. Oracle Enterprise Security Manager automatically uses Windows native authentication if running in a Windows 2000 domain.

Choose Simple Authentication if the other available selections do not work. Simple authentication can be used with either Oracle Internet Directory or Active Directory, but it is less secure.

Using Oracle9i Directory Server Features with Active Directory

For information on the following topics, see "Using Enterprise User Security with Microsoft Active Directory" in *Oracle Advanced Security Administrator's Guide*:

- LDAP and Active Directory Overview
- Oracle9i Directory Server Features
- Integration with Active Directory
- Requirements for Using Oracle9i with Active Directory

- Oracle9i Installation and Configuration with Active Directory
- Testing Connectivity
- Access Control List Management for Oracle Directory Objects
- Creating Enterprise Domains

Operating System Authentication Enabled at Installation

When you install Oracle9i database, a special Windows NT local group called `ORA_DBA` is created (if it does not already exist from an earlier Oracle installation), and your Windows username is automatically added to it. Members of local group `ORA_DBA` automatically receive the **SYSDBA privilege**.

Membership in `ORA_DBA` enables you to:

- Connect to local Oracle9i databases without a password with the command

```
CONNECT / AS SYSDBA
```

- Connect to remote Oracle9i databases without a password with the command

```
CONNECT /@net_service_name AS SYSDBA
```

where `net_service_name` is the **net service name** of the remote Oracle9i database

- Perform database administration procedures such as starting and shutting down local databases
- Add additional Windows NT users to `ORA_DBA`, enabling them to have the `SYSDBA` privilege

Administering External Users and Roles

External users and roles are in general defined by something external to Oracle9i database. In a Windows environment, they are defined by the operating system.

This chapter describes **external user** and **external role** creation and management using either Oracle Administration Assistant for Windows NT or by a combination of Oracle command line tools, Registry Editor, and Windows NT User Manager.

Note: Both methods can also administer external users and roles in Windows 2000 domains, but cannot be used to administer an **enterprise user** or an **enterprise role**. See [Chapter 3, "Administering Enterprise Users and Roles"](#) for more information on tools available for administering enterprise users and roles.

This chapter contains these topics:

- [Using Oracle Administration Assistant for Windows NT](#)
- [Manually Administering External Users and Roles](#)

Using Oracle Administration Assistant for Windows NT

Oracle Administration Assistant for Windows NT runs from **Microsoft Management Console** and enables you to configure the following Oracle database users and roles so that the Windows operating system can **authenticate** them, and they can access Oracle9i database without a password:

- Regular Windows NT domain users and **global groups** as external users
- Windows NT database administrators (with the **SYSDBA privilege**)
- Windows NT database operators (with the **SYSOPER** privilege)

In addition, Oracle Administration Assistant for Windows NT can create and grant local and external database roles to Windows NT domain users and global groups.

With Oracle Administration Assistant for Windows NT, none of the following need be done manually:

- Create NT **local groups** that match the database **system identifier (SID)** and **role**
- Assign NT domain users to these local groups
- Authenticate users in SQL*Plus with `CREATE USER username IDENTIFIED EXTERNALLY`

This section describes how to perform the following tasks with Oracle Administration Assistant for Windows NT:

- [Adding a Computer and Saving Your Configuration](#)
- [Granting Administrator Privileges for All Databases on a Computer](#)
- [Granting Operator Privileges for All Databases on a Computer](#)
- [Connecting to a Database](#)
- [Viewing Database Authentication Parameter Settings](#)
- [Creating an External OS User](#)
- [Creating a Local Database Role](#)
- [Creating an External OS Role](#)
- [Granting Administrator Privileges for a Single Database](#)
- [Granting Operator Privileges for a Single Database](#)

Note: Oracle Administration Assistant for Windows NT runs from Microsoft Management Console, which is automatically included in Windows 2000. If you are using Windows NT 4.0, you must do one of the following:

- Install Microsoft Windows NT 4.0 Option Pack, which includes Microsoft Management Console
 - Download Microsoft Management Console from the Microsoft Web site: <http://www.microsoft.com>
-
-

Managing a Remote Computer

If you want to use Oracle Administration Assistant for Windows NT to manage a **remote computer**, you must have administrator privileges for the remote computer. Oracle Administration Assistant for Windows NT always creates users in Oracle9i database with the domain name as the prefix. If you are managing Oracle7 release 7.x or later databases remotely, you must set registry parameter `OSAUTH_PREFIX_DOMAIN` to `true` on the remote computer. This parameter is located in

```
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOMEID
```

If a Windows 2000 computer is not identified with a Domain Name System (DNS) domain name, you will receive the following error message:

```
Calling query w32RegQueries1.7.0.17.0 RegGetValue
Key = HKEY_LOCAL_MACHINE
SubKey = SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value = Domain
Query Exception: GetValueKeyNotFoundException
Query Exception Class: class oracle.sysman.oii.oii.OiiQueryException
...
```

To assign a DNS name:

1. Choose Control Panel > System > Network Identification > More > Primary DNS.
2. Enter a domain name, such as `US.ORACLE.COM`.

Adding a Computer and Saving Your Configuration

When you use Oracle Administration Assistant for Windows NT for the first time, it adds the local computer to its navigation tree. You can then add other computers.

To add a computer to the Microsoft Management Console tree:

1. Choose Start > Programs > Oracle - *HOME_NAME* > Configuration and Migration Tools > Administration Assistant for Windows NT.

Microsoft Management Console starts.

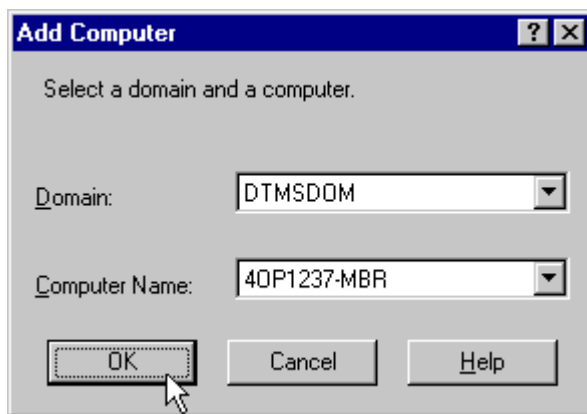
2. Double-click Oracle Managed Objects.

The Computer icon appears.

3. Right-click Computers.

4. Choose New > Computer.

The Add Computer dialog box appears.



5. Specify the domain and computer name for the computer on which your Oracle database is installed.
6. Click OK.
7. Double-click Computers to display the computer you added.
8. Double-click the computer you added. Several nodes for authenticating database administrators and operators appear.

The OS Database Administrators - Computer node creates an operating system-authenticated database administrator with SYSDBA privileges for every database **instance** on the computer. The OS Database Operators - Computer node creates an operating system-authenticated database operator with SYSOPER privileges for every database instance on the computer.

9. Save your configuration in a console file by choosing Save in the Console main menu. You can now authenticate database administrators and operators for all instances on the computer.

Granting Administrator Privileges for All Databases on a Computer

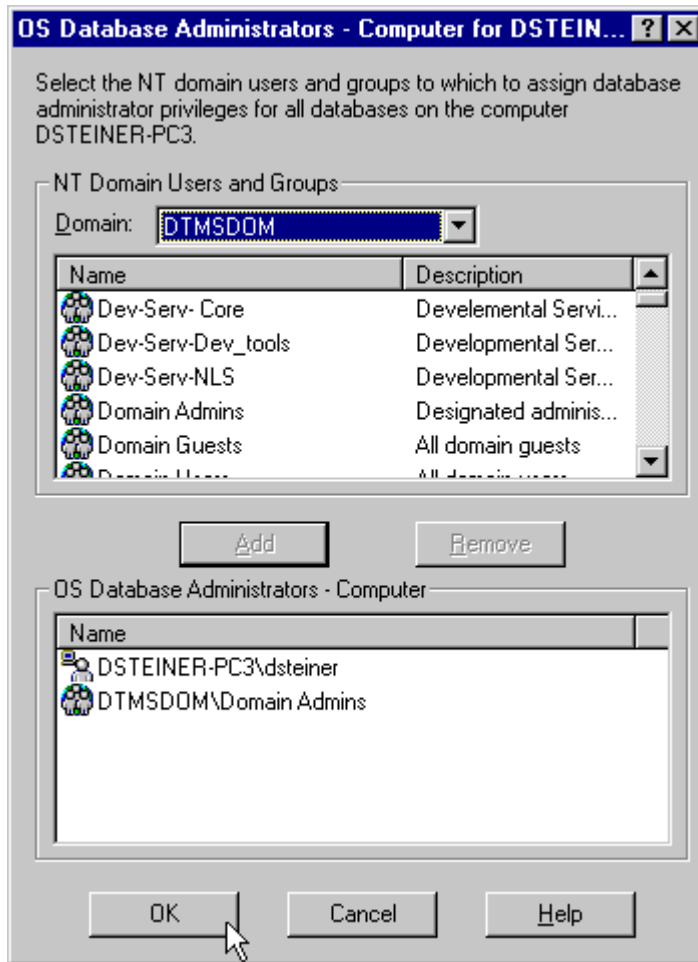
To grant database administrator (SYSDBA) privileges to database administrators (DBAs) for *all* databases on a computer:

1. Choose Start > Programs > Oracle - *HOME_NAME* > Configuration and Migration Tools > Administration Assistant for Windows NT.

Oracle Administration Assistant for Windows NT starts.

2. Right-click OS Database Administrators - Computer.
3. Choose Add/Remove.

The OS Database Administrators - Computer for *hostname* dialog appears.



4. Select the domain of the user to which to grant SYSDBA privileges from the Domain list box.
5. Select the user.
6. Click Add.
The user now appears in the OS Database Administrators - Computer window.
7. Click OK.

Granting Operator Privileges for All Databases on a Computer

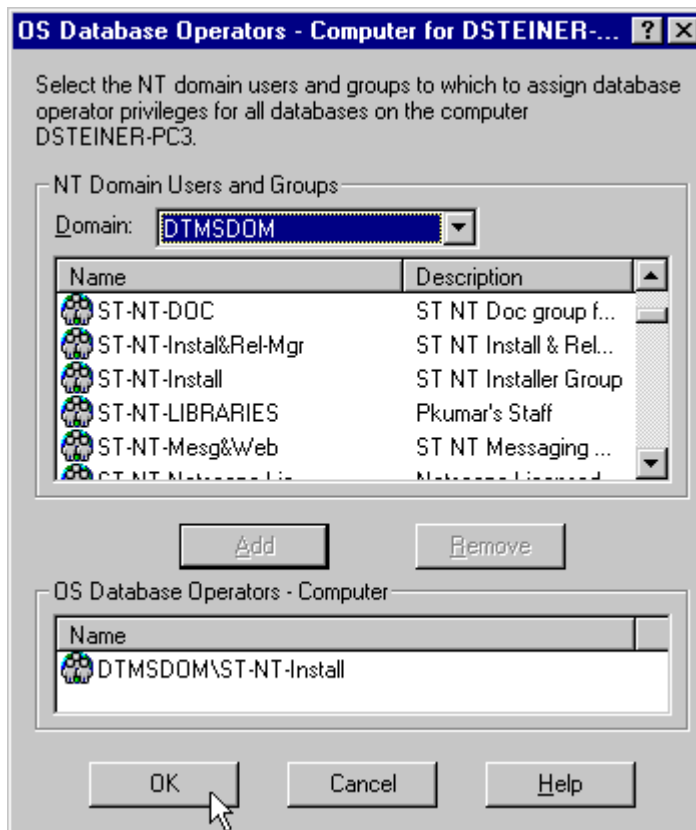
To grant database operator (*SYSOPER*) privileges to DBAs for *all* databases on a computer:

1. Choose Start > Programs > Oracle - *HOME_NAME* > Configuration and Migration Tools > Administration Assistant for Windows NT.

Oracle Administration Assistant for Windows NT starts.

2. Right-click OS Database Operators - Computer.
3. Choose Add/Remove.

The OS Database Operators - Computer for *hostname* dialog appears.



4. Select the domain of the user to which to grant `SYSOPER` privileges from the Domain list box.
5. Select the user.
6. Click Add.
The user now appears in the OS Database Operators - Computer window.
7. Click OK.

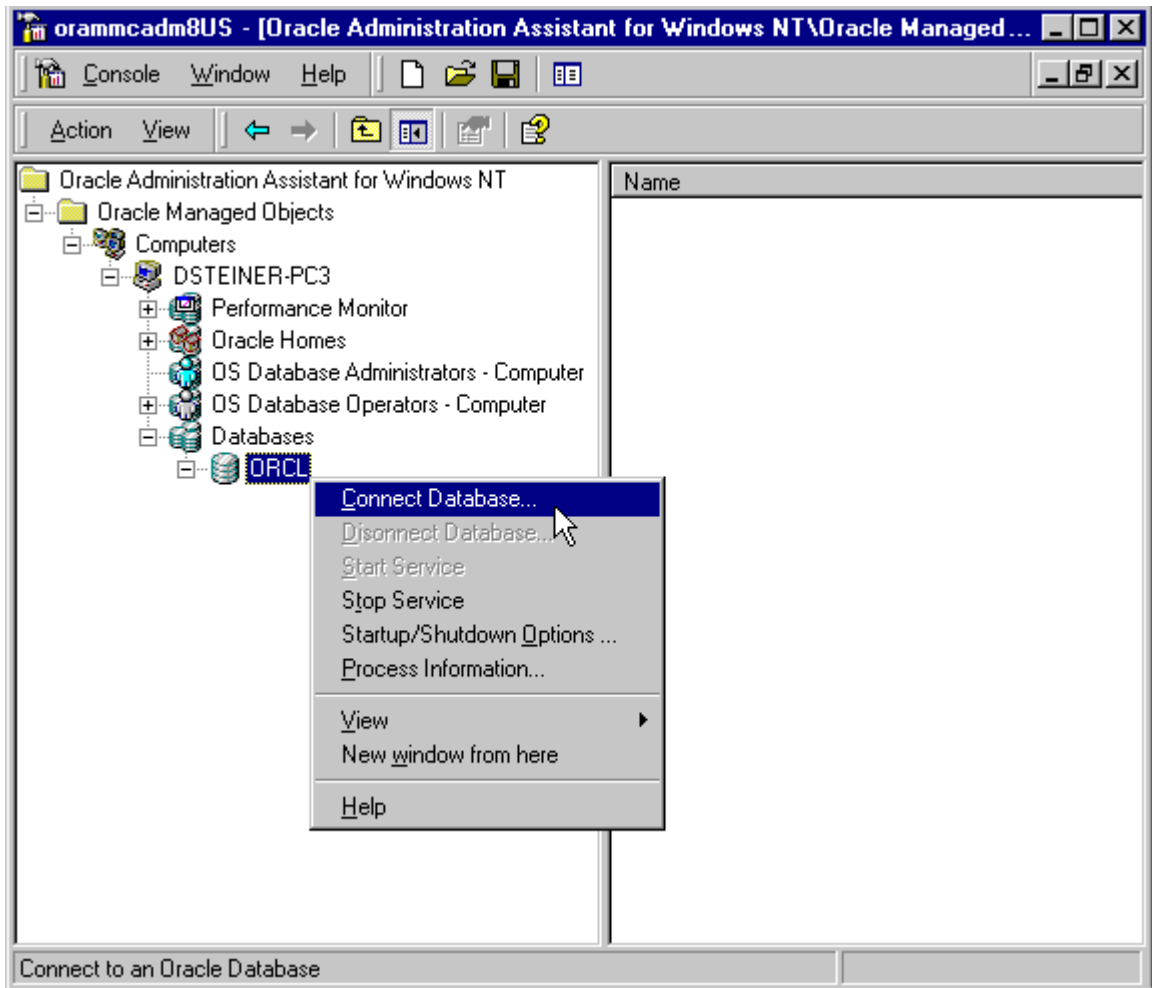
Connecting to a Database

To enable Secure Sockets Layer (SSL) when connecting to an Oracle database, start the **Oracle service** and the **listener** service in the same user account as the wallet created in Oracle Wallet Manager. Do not use the default user account in the Windows NT Services dialog box. If the Oracle service and the listener service are started in the default user accounts, then SSL does not work, and the listener does not start. Support for SSL is an Oracle Advanced Security feature. Oracle Wallet Manager is also an Oracle Advanced Security feature.

See Also: *Oracle Advanced Security Administrator's Guide* for more information on SSL support

To connect to a database:

1. Right-click the database instance you want to access in the Microsoft Management Console scope pane. In the example here, a connection is to be made to `ORCL`:



2. Choose Connect Database.

If you connect to the Oracle database, the following Windows NT nodes appear beneath the instance. If these nodes do not appear, double-click the instance.

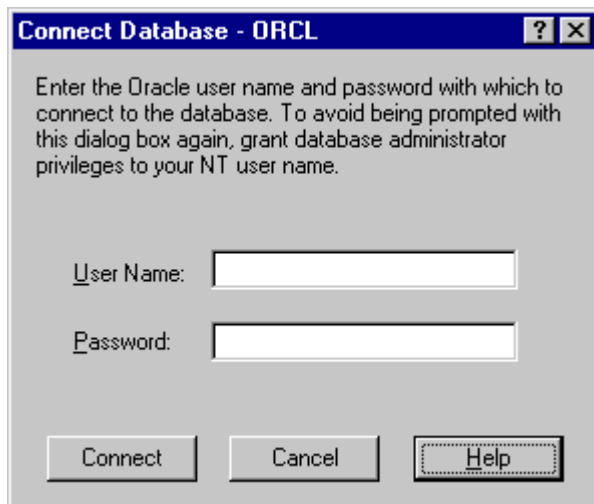
- External OS Users
- Local Roles
- External OS Roles

- OS Database Administrators
- OS Database Operators

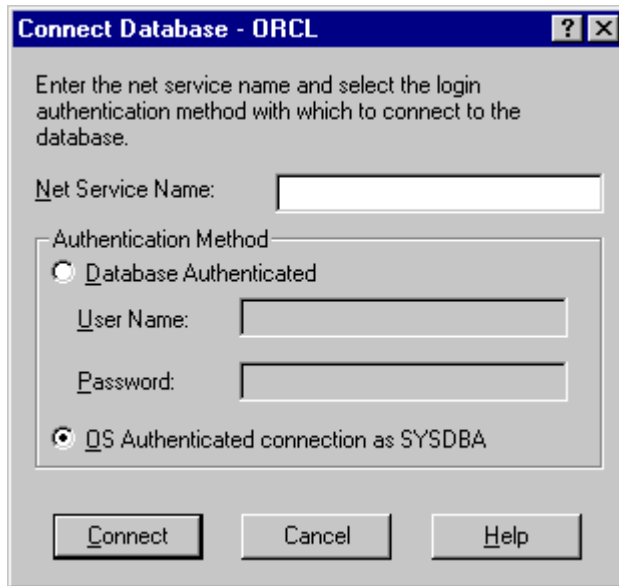
Troubleshooting Connection Problems

When connecting to a local computer, Oracle Administration Assistant for Windows NT first tries to connect to the database as a `SYSDBA`, using the Bequeath networking protocol. When connecting to a remote computer, Oracle Administration Assistant for Windows NT first tries to connect to the database using Windows native authentication as a `SYSDBA`, using the TCP/IP networking protocol (port 1521 or the deprecated 1526). If it is unsuccessful, one or more dialogs appear and prompt you to enter information to connect to the database.

The dialog shown here appears because the Windows NT domain user with which you are attempting to connect to the Oracle database is not recognized as an authenticated user with `SYSDBA` privileges. Enter an Oracle **username** and password to access the database. To avoid being prompted with this dialog again, configure your domain user to be a database administrator authenticated by the Windows NT operating system.



The next dialog appears because you are not using the TCP/IP networking protocol to connect to a remote Oracle database or the Oracle database is not running. Using a protocol other than TCP/IP (Named Pipes for example) causes this dialog box to appear each time you attempt a remote connection.



If you do not want this dialog to appear each time, then change to the TCP/IP protocol and make sure the [Oracle Net Services](#) listener for the database is listening on the default port 1521 (or the deprecated default port 1526). Otherwise, this dialog appears every time. Ensure also that the Oracle database is started.

1. Enter the **net service name** with which to connect to your Oracle database. You must enter a net service name regardless of the authentication method you select.
2. If you want to access the database with an Oracle username and password, select the Database Authenticated option. This username and password must exist in the Oracle database and have the SYSDBA privilege.
3. If you want to access the database with the Windows NT domain user with which you are currently logged in, select the OS Authenticated Connection as SYSDBA option. This domain user must already be recognized by Windows NT as an authenticated user with SYSDBA privileges. Otherwise, your logon fails.

Note: Oracle Net Services provides a new Trace Assistant tool that helps diagnose connection problems by converting existing trace file text into a more readable format. See "Using the Trace Assistant to Examine Trace Files" in *Oracle9i Net Services Administrator's Guide*.

Viewing Database Authentication Parameter Settings

To view database authentication parameter settings:

1. Right-click the database.
2. Choose Properties.
3. The Properties dialog box appears displaying the following parameter values:
 - OS_AUTHENT_PREFIX
 - OS_ROLES

OS_AUTHENT_PREFIX is an `init.ora` file parameter that authenticates external users attempting to connect to the Oracle database with the user's Windows NT username and password. The value of this parameter is attached to the beginning of every user's Windows username.

By default, the parameter is set to none (""), during Oracle9i database creation. Therefore, a Windows domain username of `frank` is authenticated as username `frank`. If you set this parameter to `xyz`, then Windows NT domain user `frank` is authenticated as user `xyzfrank`.

OS_ROLES is an `init.ora` file parameter that, if set to `true`, enables the Windows NT operating system to manage **authorization** of an **external role** for a database user. By default, OS_ROLES is set to `false`. You must set OS_ROLES to `true` and restart your Oracle database before you can create external roles. If OS_ROLES is set to `false`, the Oracle database manages granting and revoking of roles for database users.

If OS_ROLES is set to `true`, and you assign an external role to an NT global group, then it is granted only at the global group level, and not at the level of the individual user in this global group. This means that you cannot revoke or edit the external role assigned to an individual user in this global group through the Roles tab of the User Name Properties dialog box at a later time. Instead, you must use the Assign External OS Roles to an NT Global Group field in the dialog box to revoke the external role from this global group (and therefore all its individual users).

External roles assigned to an individual domain user or **local roles** (with `OS_ROLES` set to `false`) assigned to an individual domain user or NT global group are not affected by this issue. They can be edited or revoked.

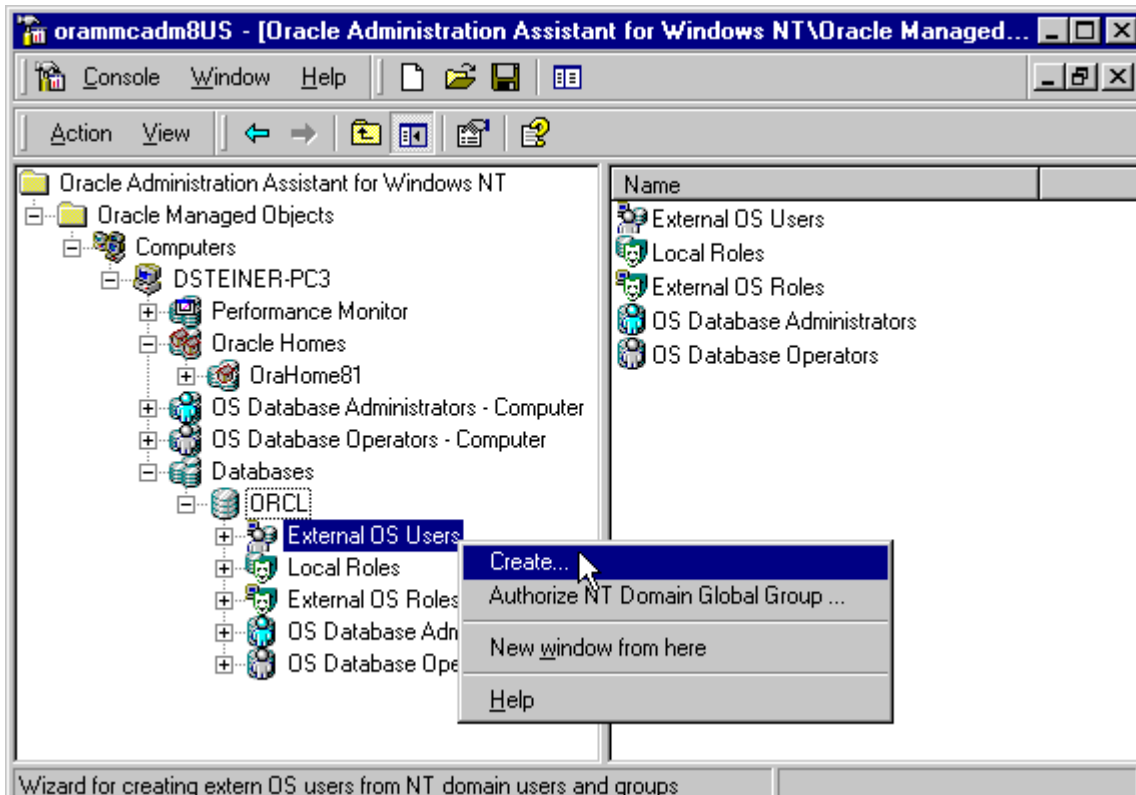
If `OS_ROLES` is set to `true`, you cannot grant local roles in the database to any database user. You must grant roles through Windows NT. See "[Creating a Local Database Role](#)" on page 2-18 and "[Creating an External OS Role](#)" on page 2-22 for more information.

Creating an External OS User

The External OS Users node of Oracle Administration Assistant for Windows NT enables you to authenticate a Windows NT user to access the Oracle database as an external user without being prompted for a password. External users are typically regular database users (not database administrators) to which you assign standard database roles (such as `CONNECT` and `RESOURCE`), but do not want to assign `SYSDBA` (database administrator) or `SYSOPER` (database operator) privileges.

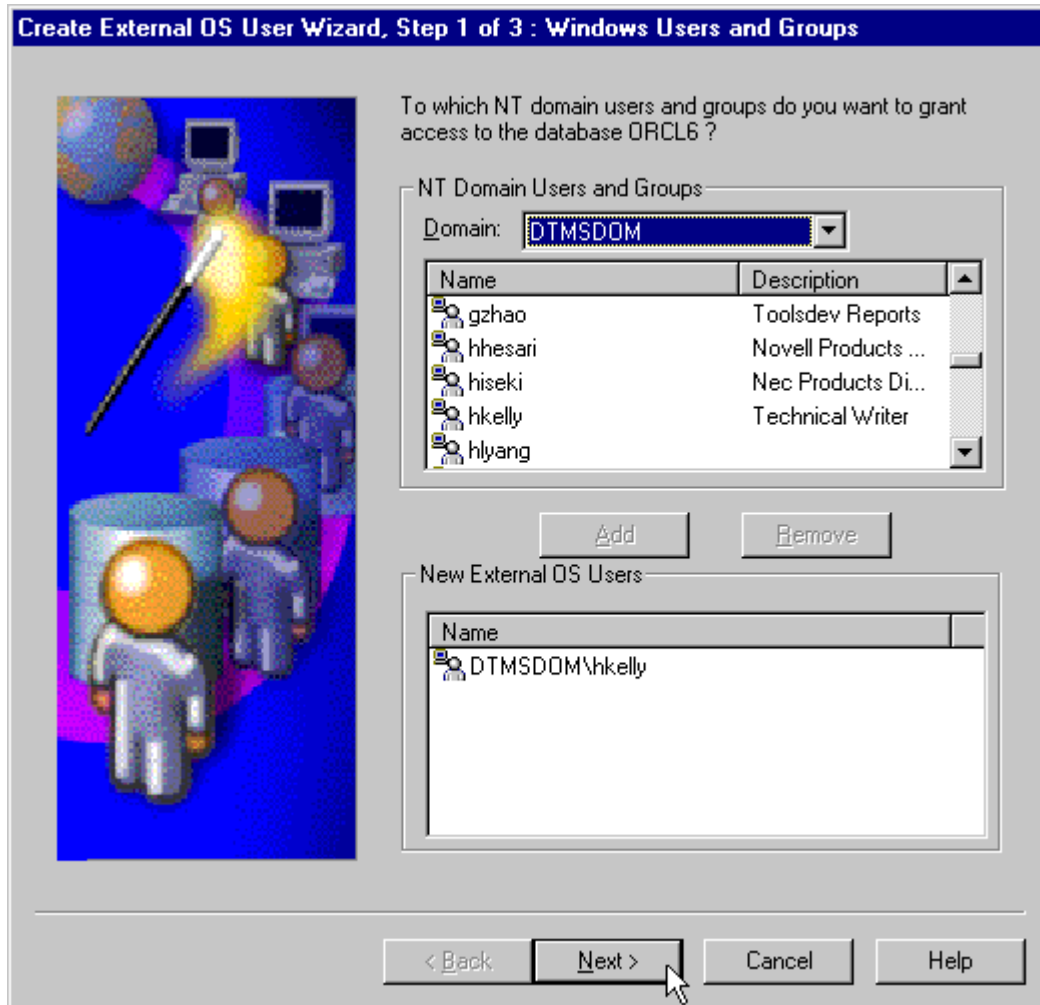
To create an external OS user:

1. Follow the steps in "[Connecting to a Database](#)" on page 2-8 to connect to a database.
2. Right-click External OS Users. A contextual menu appears.



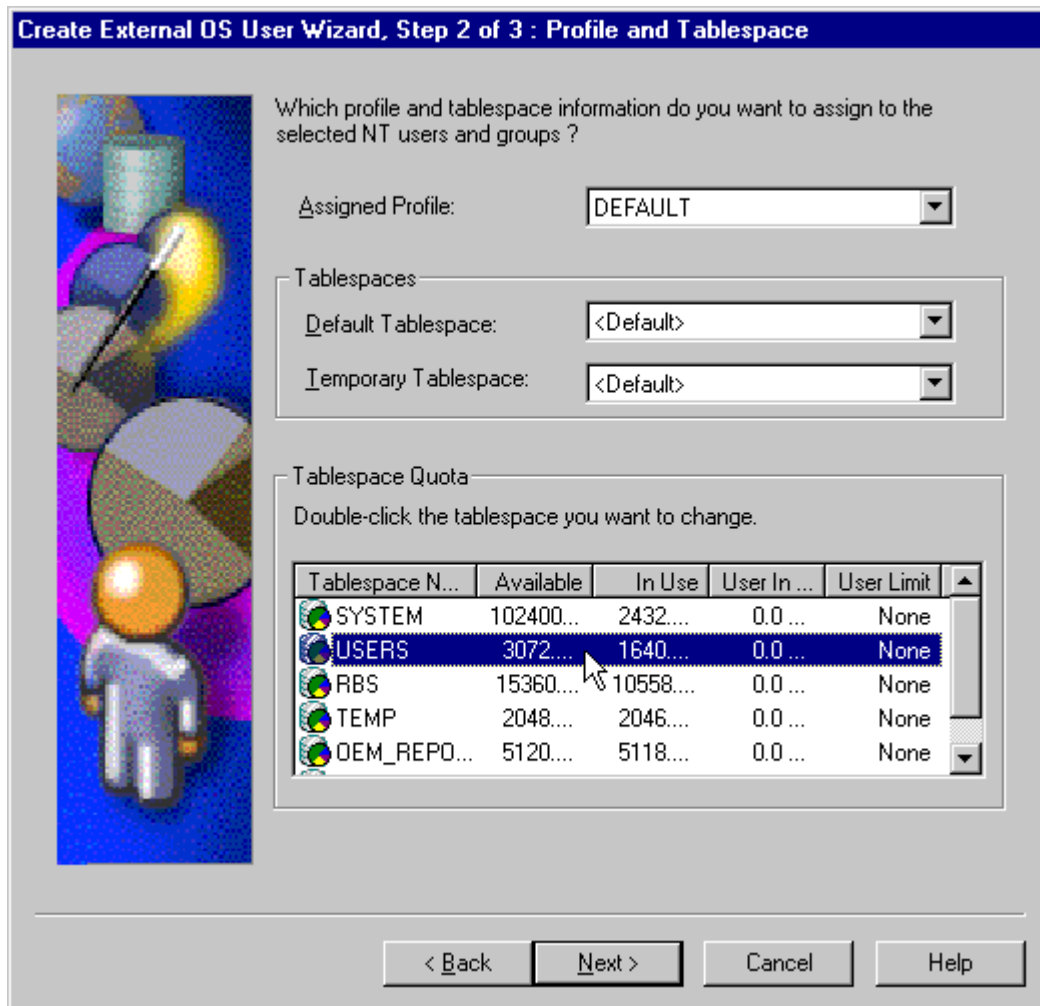
3. Choose Create.

Create External OS User Wizard starts, and the first of three wizard dialogs appears. The first dialog is for Windows Users and Groups.

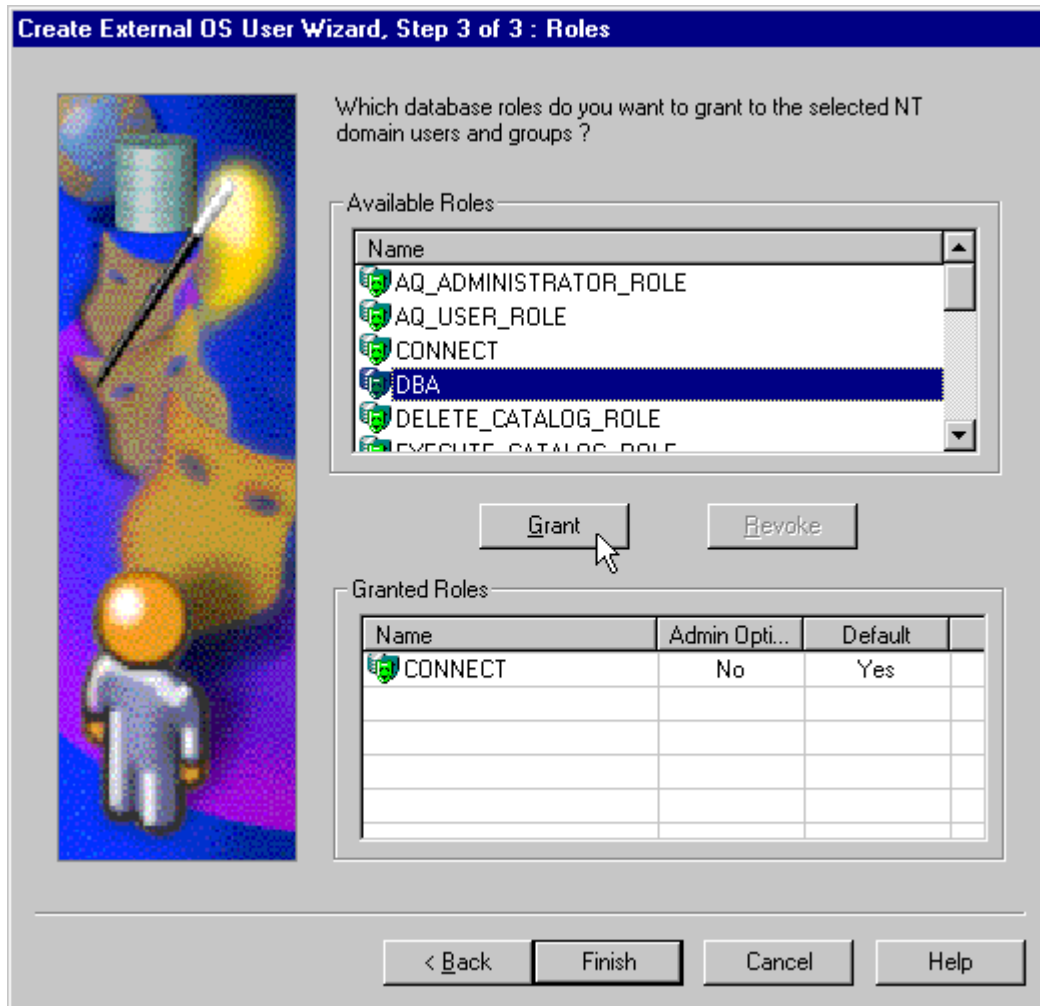


4. In the NT Domain Users and Groups box select the domain in which your Windows NT domain users and global groups are located.

5. Select the Windows NT domain users and global groups to which to grant access to the database.
6. Click Add. The selected users and groups now appear in the New External OS Users list box.
7. Click Next. The Profile and Tablespace dialog appears.



8. In the Assigned Profile list, select a profile for the new external users. A profile is a named set of resource limits. If resource limits are enabled, Oracle limits database usage and instance resources to whatever is defined in the user's profile. You can assign a profile to each user and a default profile to all users who do not have specific profiles.
9. In Tablespace Quota double-click the **tablespace** to assign a tablespace **quota**.
10. Click Next. The Roles dialog appears.



11. In Available Roles select the database roles to grant to the new external users.
12. Click Grant.
13. Click Finish.
14. Right-click the external user for which you want to view information and select Properties.

The assigned properties appear.

Note: If you select an NT global group for authentication when using Oracle Administration Assistant for Windows NT, all users currently in the group are added to the Oracle database. If at a later time, you use a Windows NT tool to add or remove users in this Windows NT global group, these updates are not reflected in the Oracle database. The newly added or removed users must be explicitly added or removed in the Oracle database with Oracle Administration Assistant for Windows NT.

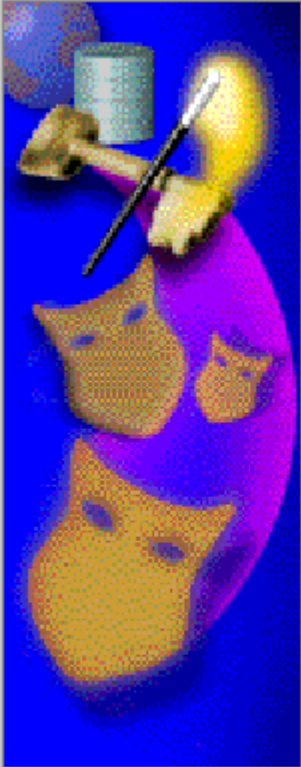
Creating a Local Database Role

The Local Roles node of Oracle Administration Assistant for Windows NT enables you to create a role and have it managed by the database. Once a local role is created, you can grant or revoke that role to a database user. To create a local database role:

1. Follow the steps in "[Connecting to a Database](#)" on page 2-8 to connect to a database.
2. Right-click Local Roles for the database for which you want to create a local role.
3. Choose Create.

Create Local Role Wizard starts, and the first of three wizard dialogs appears. The first dialog is for Name and Authentication.

Create Local Role Wizard, Step 1 of 3 : Name and Authentication



Which local role name do you want to use ?

Name:

Which role authentication method do you want to use ?

Authentication

None

Password

Enter Password:

Confirm Password:

< Back Next > Cancel Help

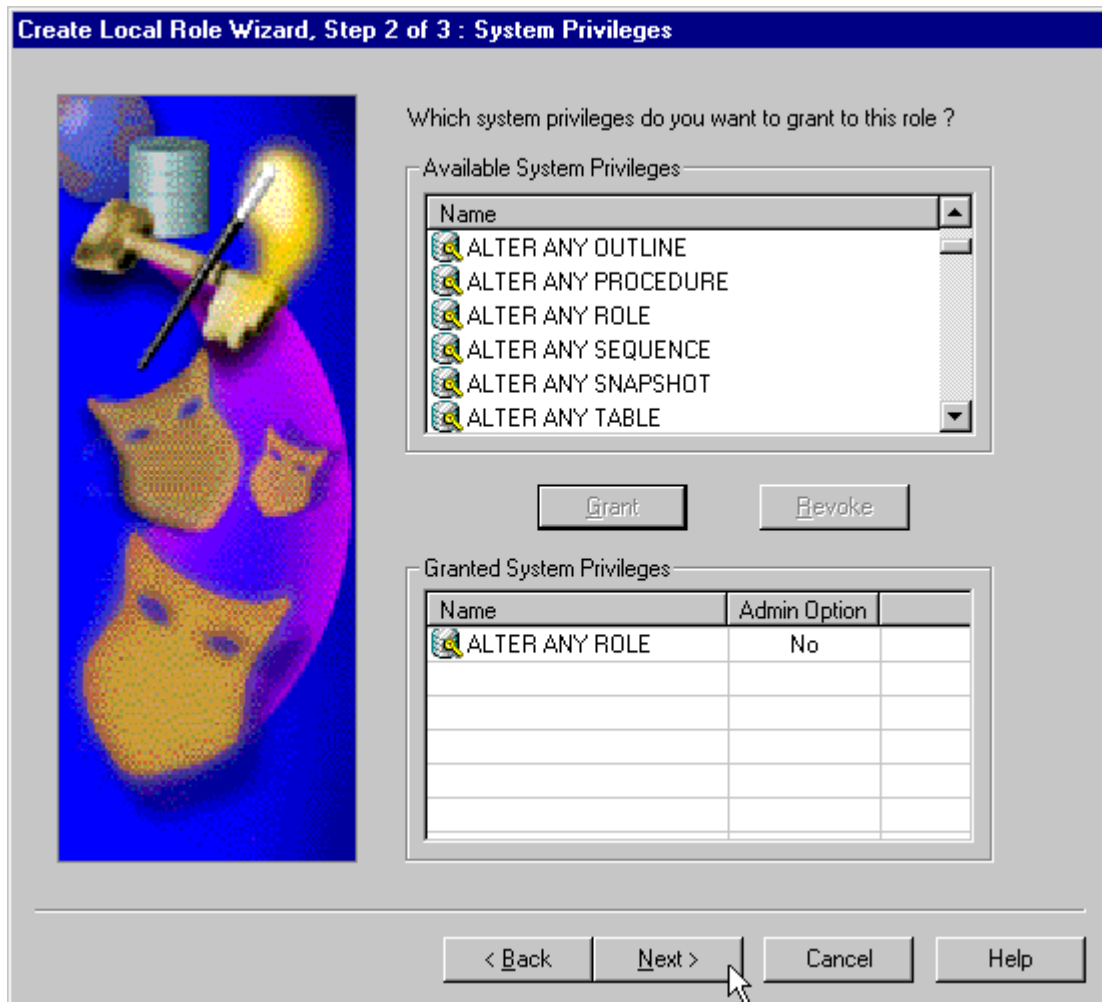
4. Enter a local role name to use.
5. In Authentication select None if you want a user to use this local role without being required to enter a password.

Select Password if you want use of this role to be protected by a password. These roles can only be used by supplying an associated password with the `SET ROLE` command. See *Oracle9i Database Administrator's Guide* for additional information.

Enter the password to use with this role.

Confirm the password by entering it a second time.

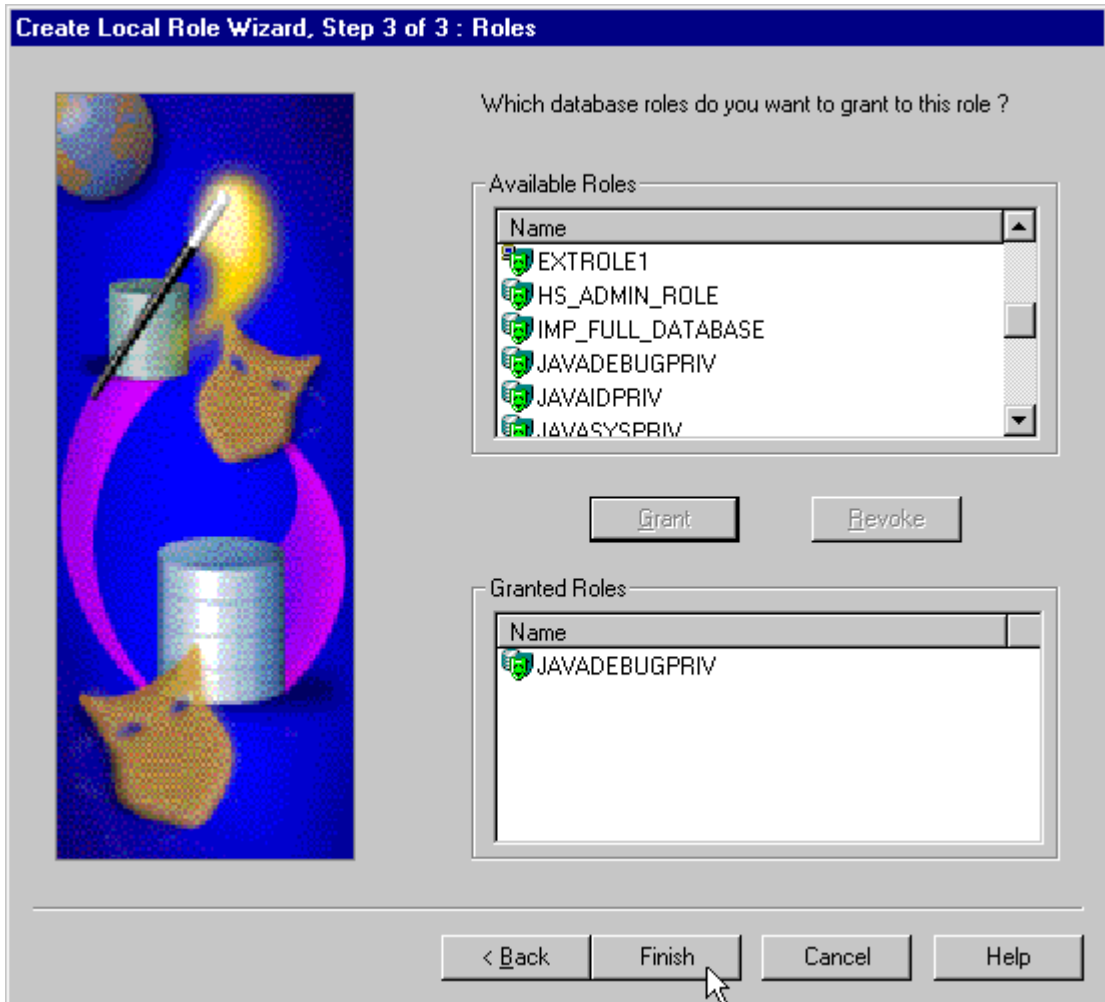
6. Click Next. The System Privileges dialog appears.



7. In Available System Privileges select the system privileges you want to assign to the local role.
8. Click Grant to grant the selected system privileges to the local role.

The Granted System Privileges field displays the list of system privileges granted to the local role. To revoke a system privilege, make an appropriate selection, then choose Revoke.

9. If you want to grant Admin Option to this role, click the value in the Admin Option column to display a list box. This enables you to select Yes.
10. Click Next. The Roles dialog appears.



11. In Available Roles select the roles you want to assign to the local role. Both local roles and external roles appear in this list.

12. Click Grant to grant the selected roles to the role.

The Granted Roles field displays the list of roles granted to the role. Both local roles and external roles can appear in this list. To revoke roles, make appropriate selections, then choose Revoke.

13. Click Finish.

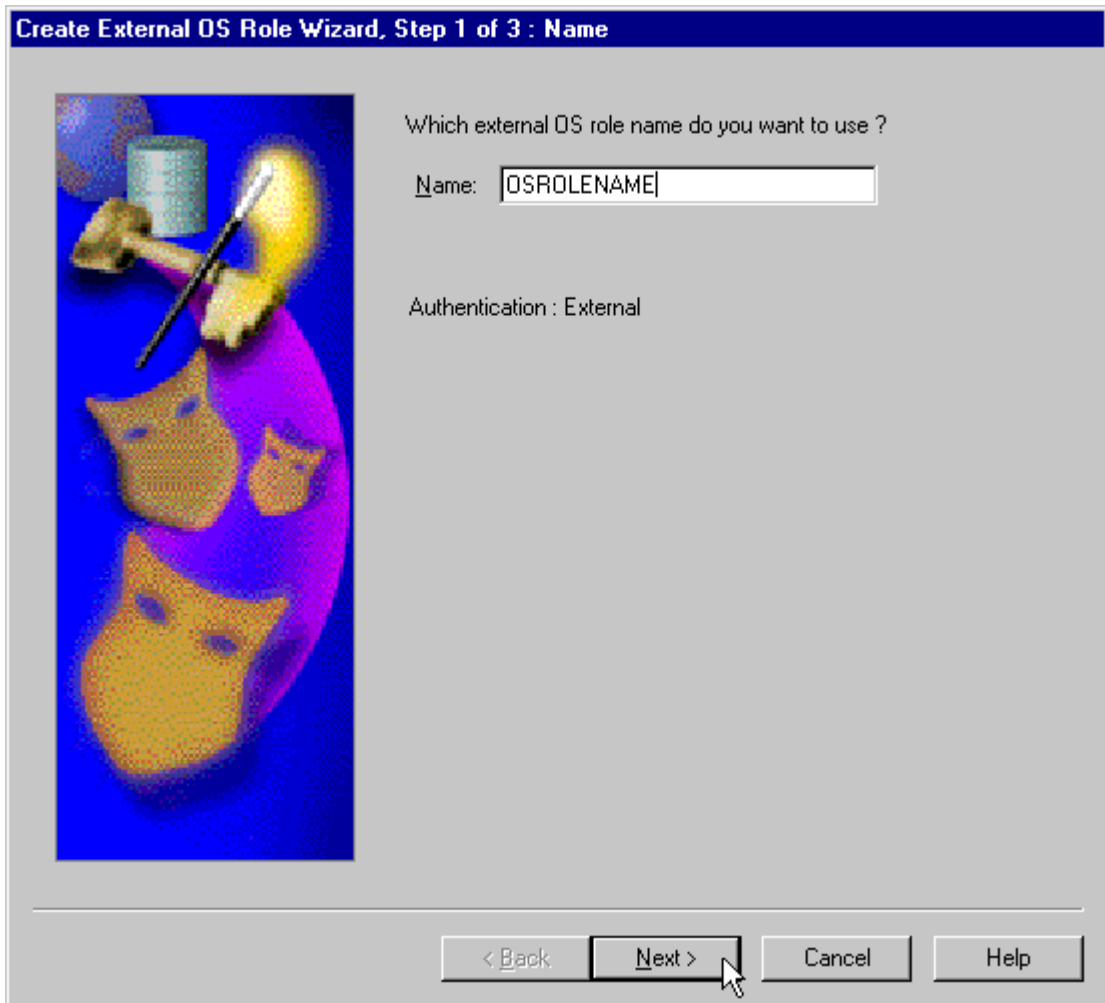
Creating an External OS Role

The External OS Roles node of Oracle Administration Assistant for Windows NT enables you to create an external role and have it managed by the Windows operating system. Once an external role is created, you can grant or revoke that role to a database user. To create an external role:

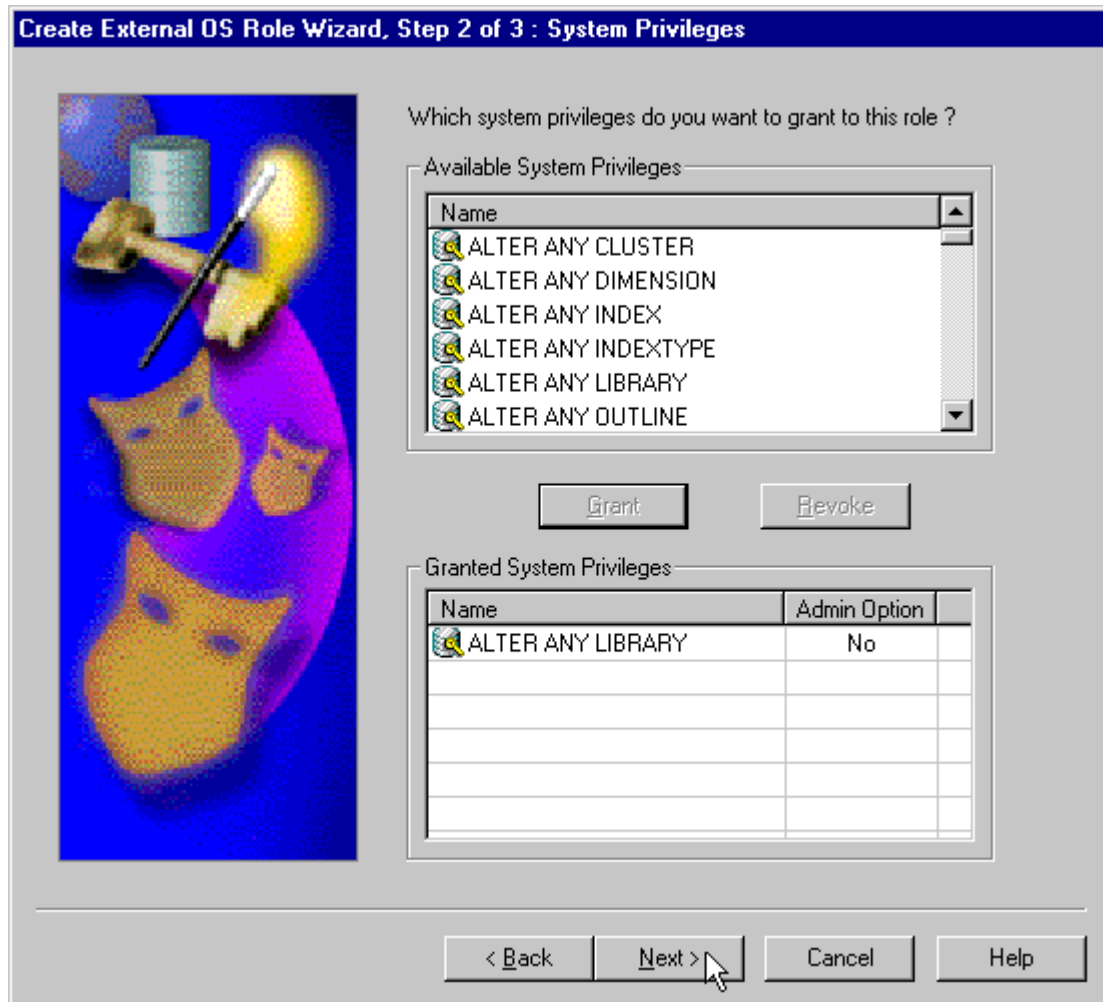
1. Follow the steps in "[Connecting to a Database](#)" on page 2-8 to connect to a database.
2. Right-click External OS Roles for the database for which to create an external role.
3. Choose Create.

Create External OS Role Wizard starts, and the first of three wizard dialogs appears. The first dialog is for Name. Authentication: External appears in this dialog to indicate that only external roles can be created.

Note: Create External OS Role Wizard is available only if `init.ora` parameter `OS_ROLES` is set to `true`. If it is set to `false`, then you must first change it to `true` and then restart the Oracle database.



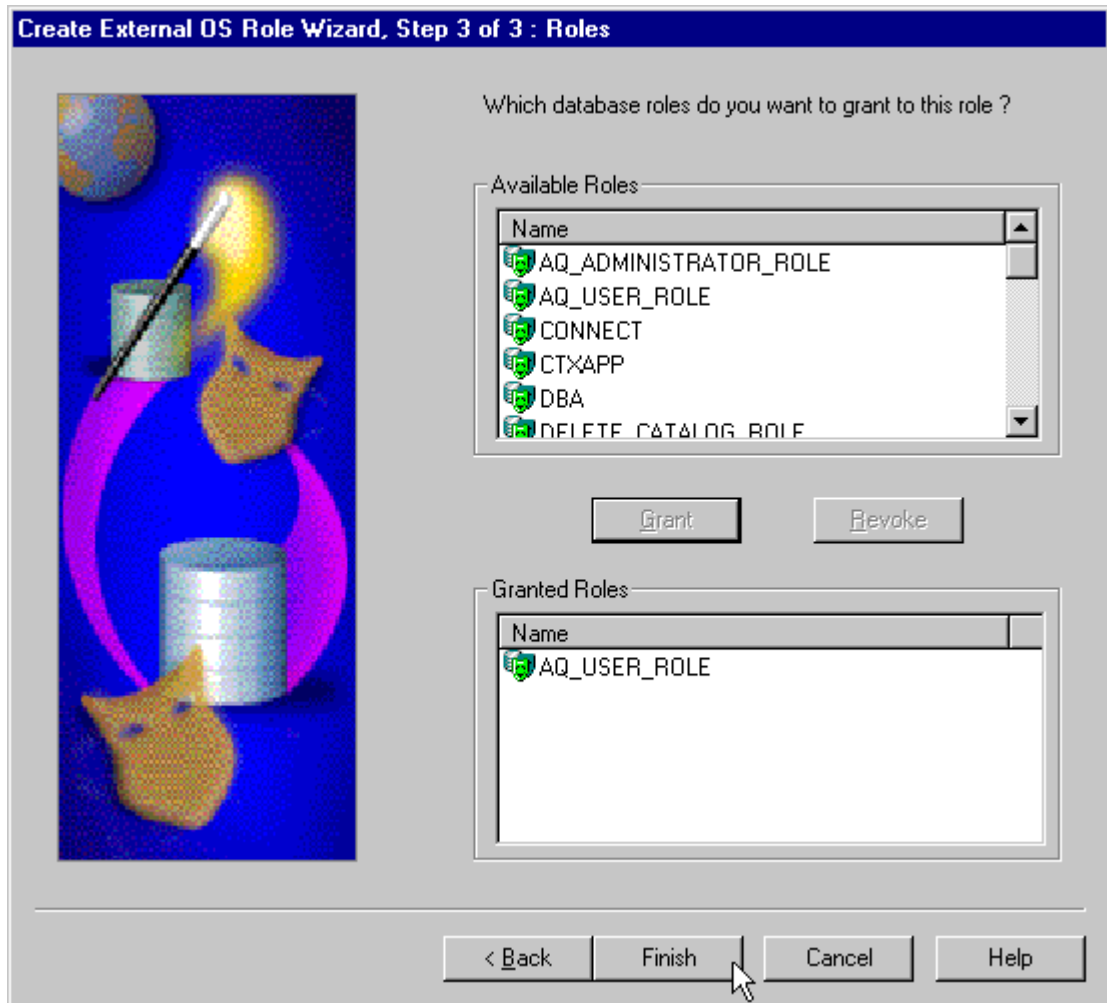
4. Enter an external role name to use. An external role is a role that is managed by the Windows operating system.
5. Click Next.
The System Privileges dialog appears.



6. In Available System Privileges select the system privileges you want to assign to the external role.
7. Choose Grant to grant the selected system privileges to the external role.
8. The Granted System Privileges field displays the list of system privileges granted to the external role. To revoke a system privilege, make an appropriate selection, then choose Revoke.

9. If you want to grant Admin Option to this role, choose the value in the Admin Option column to display a list box. This enables you to select Yes.
10. Click Next.

The Roles dialog appears.



11. In Available Roles select the roles you want to assign to the external role. Both local roles and external roles appear in this list.

12. Click Grant to grant the selected roles to the external role.

The Granted Roles field displays the list of roles granted to the external role.

13. Click Finish.

Granting Administrator Privileges for a Single Database

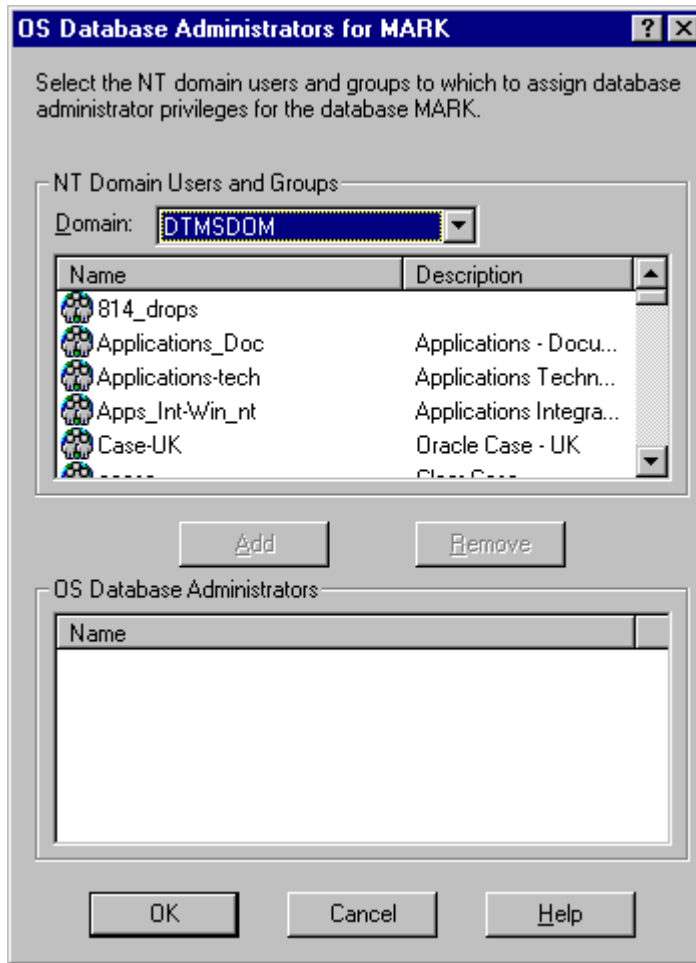
The OS Database Administrators node of Oracle Administration Assistant for Windows NT enables you to authorize a Windows NT user with `SYSDBA` privileges for a specific instance on a computer. To grant administrator (`SYSDBA`) privileges for a single database:

1. Follow the steps in "[Connecting to a Database](#)" on page 2-8 to connect to a database.
2. Right-click the database to access (for example, `orcl`) in the Microsoft Management Console scope pane.
3. Choose Connect Database.

Several icons, including OS Database Administrators and OS Database Operators, appear.

4. Right-click OS Database Administrators.
5. Choose Add/Remove.

The OS Database Administrators for *instance* dialog appears. In the example shown here, the instance is `MARK`:



6. In NT Domain Users and Groups select the domain of the user to which to grant SYSDBA privileges from the Domain: list box.
7. Select the user.
The user now appears in OS Database Administrators.
8. Click OK.

Granting Operator Privileges for a Single Database

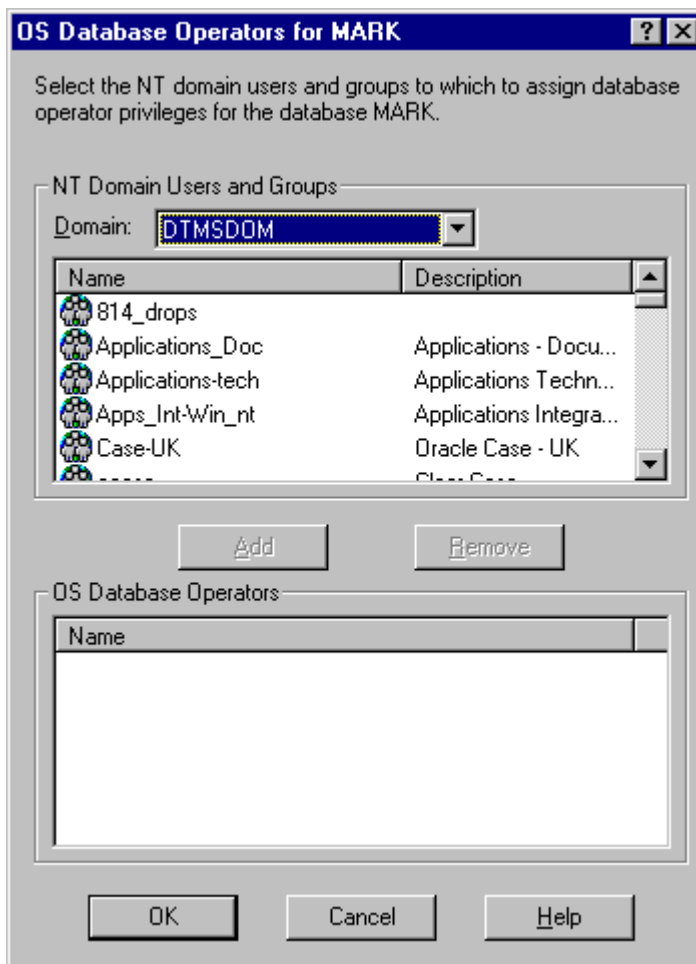
The OS Database Operators node of Oracle Administration Assistant for Windows NT enables you to authorize a Windows NT user with SYSOPER privileges for a specific instance on a computer. To grant operator (SYSOPER) privileges for a single database:

1. Follow the steps in "[Connecting to a Database](#)" on page 2-8 to connect to a database.
2. Right-click the database to access (for example, `orcl`) in the Microsoft Management Console scope pane.
3. Choose Connect Database.

Several icons, including OS Database Administrators and OS Database Operators, appear.

4. Right-click OS Database Operators.
5. Choose Add/Remove.

The OS Database Operators for *instance* dialog appears. In the example shown here, the instance is `MARK`:



6. In NT Domain Users and Groups select the domain of the user to which to grant SYSOPER privileges from the Domain: list box.
7. Select the user.
8. Click Add.
The user now appears in OS Database Operators.
9. Click OK.

Manually Administering External Users and Roles

Instead of using Oracle Administration Assistant for Windows NT, you can manually configure administrators, operators, users, and roles to be authenticated by the operating system. Manual configuration involves using Oracle command line tools, editing the registry, and creating local groups in Windows NT User Manager. All of the following can be manually configured to access the Oracle database without a password:

- External OS users
- Windows NT database administrators (with `SYSDBA` privilege)
- Windows NT database operators (with `SYSOPER` privilege)

In addition, you can manually create and grant local and external database roles to Windows NT domain users and global groups.

This section describes:

- [Manually Creating an External OS User](#)
- [Manually Granting Administrator and Operator Privileges for Databases](#)
- [Manually Creating an External Role](#)
- [Manually Migrating Users](#)

Note: Use extreme care when manually configuring administrators, operators, users, and roles to be authenticated by the operating system. If possible, use Oracle Administration Assistant for Windows NT to perform configuration procedures.

Manually Creating an External OS User

This section describes how to authenticate external OS users (not database administrators) using Windows NT, so that a password is not required when accessing the database. When you use Windows NT to authenticate external OS users, your database relies solely on Windows NT to restrict access to database usernames.

In the following procedure, two Windows NT usernames are authenticated:

- Local user `frank`
- Domain user `frank` on domain `sales`

Local user `frank` logs into its local Windows NT client computer to access an Oracle9i database, which can be on a different computer. To access other databases and resources on other computers, the local user must provide a username and password each time.

Domain user `frank` on domain `sales` logs into a `sales` domain that includes many other Windows NT computers and resources, one of which contains an Oracle9i database. The domain user can access all the resources the domain provides with a single username and password.

The procedure is divided into two sets of tasks performed on different computers:

- [External User Authentication Tasks on the Oracle9i Database Server](#)
- [External User Authentication Tasks on the Client Computer](#)

External User Authentication Tasks on the Oracle9i Database Server

1. Add parameter `OS_AUTHENT_PREFIX` to your `init.ora` file.

The `OS_AUTHENT_PREFIX` value is prefixed to local or domain usernames attempting to connect to the server with the user's operating system name and password. The prefixed username is compared with Oracle usernames in the database when a connection request is attempted. Using parameter `OS_AUTHENT_PREFIX` with Windows native authentication methods is the recommended method for performing secure, trusted client connections to your server.

2. Set a value for `OS_AUTHENT_PREFIX`. Your choices are:

- Any character string

If you specify `xyz`, as in this procedure's example, then `xyz` is prefixed to the beginning of the Windows NT username (for example, `xyzfrank` for local user `frank` or `xyzsales\frank` for domain user `frank` on domain `sales`). String values are case insensitive.

- `" "` (two double quotes with no space between)

This option is recommended, because it eliminates the need for any prefix to Windows NT usernames (for example, `frank` for local user `frank` or `sales\frank` for domain user `frank` on domain `sales`).

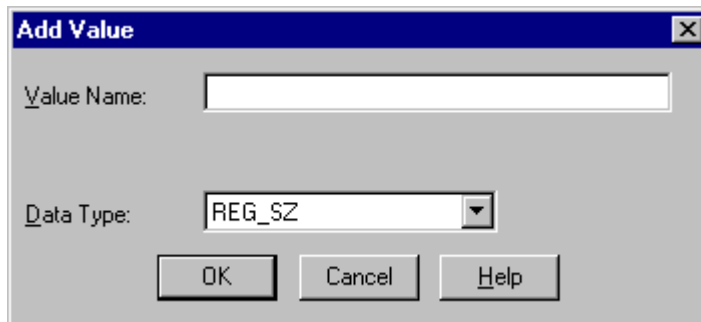
- No value specified

If you do not specify a value for `OS_AUTHENT_PREFIX`, it defaults to `OPS$` (for example, `OPS$frank` for local user `frank` or `OPS$sales\frank` for domain user `frank` on domain `sales`).

3. Create a Windows NT local or domain username for `frank` with User Manager (if the appropriate name does not currently exist). See your Windows NT documentation for detailed instructions.
4. Do this step *only* if you are *not* authenticating a domain name with a user (for example, just `frank` instead of `frank` on domain `sales`). Otherwise, go to step 5.
 - a. Start Registry Editor from the command prompt:

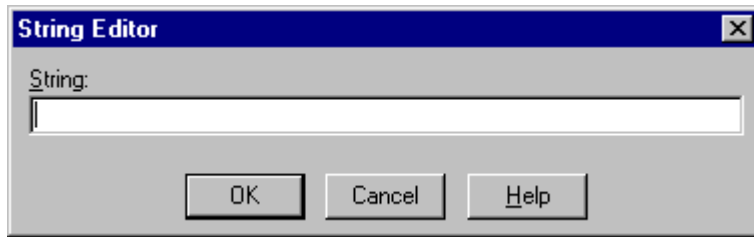
```
C:\> regedt32
```
 - b. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME ID`, where `ID` is the Oracle home directory you want to edit.
 - c. Choose Edit > Add Value.

The Add Value dialog box appears:



- d. Enter `OSAUTH_PREFIX_DOMAIN` in the Value Name field.
- e. Choose `REG_EXPAND_SZ` from the Data Type list box.
- f. Click OK.

The String Editor dialog box appears:



- g. Enter `true` in the String field to enable authentication at the domain level.
There may be multiple `frank` usernames on your network, including local user `frank`, domain user `frank` on `sales`, and possibly several domain users `frank` on other domains. Entering `true` enables the server to differentiate among them. Entering `false` causes the domain to be ignored and local user `frank` to become the default value of the operating system user returned to the server.
- h. Click OK.
Registry Editor adds the parameter.
- i. Choose Exit from the registry menu.
String Editor exits.

5. Ensure that parameter `SQLNET.AUTHENTICATION_SERVICES` in file `sqlnet.ora` contains `nts`.

6. Start SQL*Plus:

```
C:\> sqlplus
```

7. Connect to the database with the **SYSTEM** database administrator (DBA) name:

```
SQL> CONNECT
Enter user-name: SYSTEM/password
```

Unless you have changed it, the `SYSTEM` password is `MANAGER` by default.

8. Create a local external user by entering:

```
SQL> CREATE USER xyzfrank IDENTIFIED EXTERNALLY;
```

where `xyz` is the value you chose for initialization parameter `OS_AUTHENT_PREFIX`, and `frank` is the Windows NT local username.

9. Grant a local external user database roles by entering:

```
SQL> GRANT RESOURCE TO xyzfrank;  
SQL> GRANT CONNECT TO xyzfrank;
```

10. Create a domain external user by entering:

```
SQL> CREATE USER "XYZSALES\FRANK" IDENTIFIED EXTERNALLY;
```

where XYZ is the value you chose for initialization parameter OS_AUTHENT_PREFIX, and SALES\FRANK is the domain name and Windows NT domain username. Double quotes are required and the entire syntax must be in uppercase.

11. Grant a domain external user database roles by entering:

```
SQL> GRANT RESOURCE TO "XYZSALES\FRANK";  
SQL> GRANT CONNECT TO "XYZSALES\FRANK";
```

Double quotes are required and the entire syntax must be in uppercase.

12. Connect to the database with the SYSDBA name:

```
SQL> CONNECT / AS SYSDBA
```

13. Shut down the database:

```
SQL> SHUTDOWN
```

14. Restart the database:

```
SQL> STARTUP
```

This causes the change to the OS_AUTHENT_PREFIX parameter value to take effect.

External User Authentication Tasks on the Client Computer

1. Create Windows NT local or domain username frank with the same username and password that exist on the Windows NT server (if the appropriate name does not currently exist).
2. Ensure that parameter SQLNET.AUTHENTICATION_SERVICES in file sqlnet.ora contains nts.
3. Use Oracle Net Configuration Assistant to configure a network connection from your client computer to the Windows NT server on which your Oracle9i

database is installed. See *Oracle9i Net Services Administrator's Guide* for instructions.

4. Start SQL*Plus:

```
C:\> sqlplus / NOLOG
```

5. Connect to your Windows NT server:

```
SQL> CONNECT /@connect_identifier
```

where *connect_identifier* is the net service name for Oracle9i database.

Oracle9i database searches the **data dictionary** for an automatic login username corresponding to the Windows NT local or domain username, verifies it, and enables connection as xyzfrank or xyzsales\frank.

6. Verify that you have connected to Oracle9i database as local or domain user frank by viewing the roles assigned in steps 9 or 11 of "[External User Authentication Tasks on the Oracle9i Database Server](#)".

```
SQL> SELECT * FROM USER_ROLE_PRIVS;
```

which outputs for local user frank:

USERNAME	GRANTED_ROLE	ADM	DEF	OS_
XYZFRANK	CONNECT	NO	YES	NO
XYZFRANK	RESOURCE	NO	YES	NO

2 rows selected.

or, for domain user frank:

USERNAME	GRANTED_ROLE	ADM	DEF	OS_
XYZSALES\FRANK	CONNECT	NO	YES	NO
XYZSALES\FRANK	RESOURCE	NO	YES	NO

2 rows selected.

As the Oracle9i username is the whole name xyzfrank or xyzsales\frank, all objects created by xyzfrank or xyzsales\frank (that is, tables, **views**, indexes, and so on) are prefixed by this name. For another user to reference the table shark owned by xyzfrank, for example, the user must enter:

```
SQL> SELECT * FROM xyzfrank.shark
```

Note: Automatic authorization is supported for all [Oracle Net](#) protocols.

Manually Granting Administrator and Operator Privileges for Databases

This section describes how to enable Windows NT to grant the database administrator (SYSDBA) and database operator (SYSOPER) privileges to database administrators. With this privilege, database administrators can issue the following commands from a client computer and connect to Oracle9i database without entering a password:

```
CONNECT / AS SYSOPER
CONNECT / AS SYSDBA
```

To enable this feature, the Windows NT local or domain username of the database administrator must belong to one of the Windows NT local groups listed in [Table 2-1](#).

Table 2-1 *Windows NT Local Groups with SYSDBA and SYSOPER Privileges*

Local Group	Privileges
ORA_OPER	SYSOPER privileges for all databases on a computer
ORA_DBA ¹	SYSDBA privileges for all databases on a computer
ORA_SID_OPER	SYSOPER privileges for a single database (identified by <i>SID</i>)
ORA_SID_DBA	SYSDBA privileges for a single database (identified by <i>SID</i>)

¹ ORA_DBA is automatically created during installation. See section "[Operating System Authentication Enabled at Installation](#)" on page 1-8 for information.

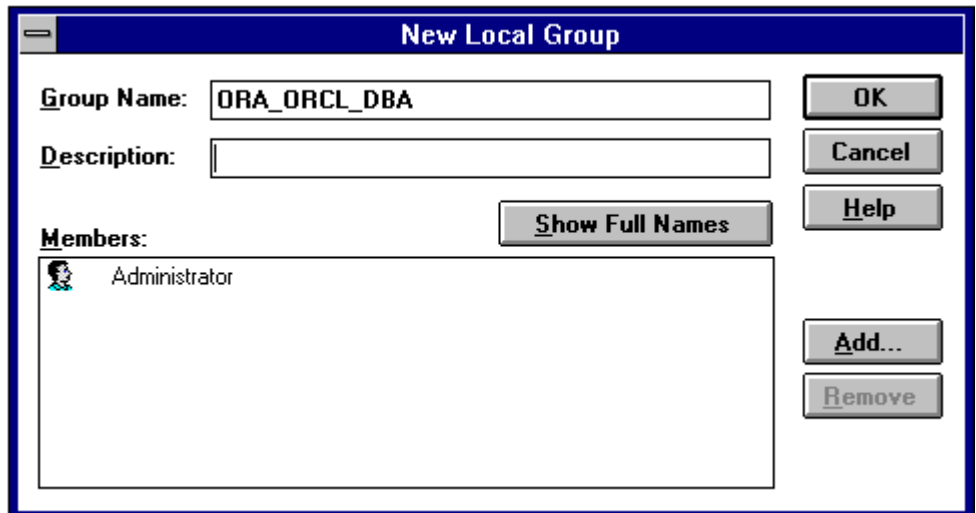
The manual procedure for enabling database administrators to connect as SYSOPER or SYSDBA without a password is divided into two sets of tasks performed on different computers:

- [SYSDBA/SYSOPER Authentication Tasks on the Oracle9i Database Server](#)
- [SYSDBA/SYSOPER Authentication Tasks on the Client Computer](#)

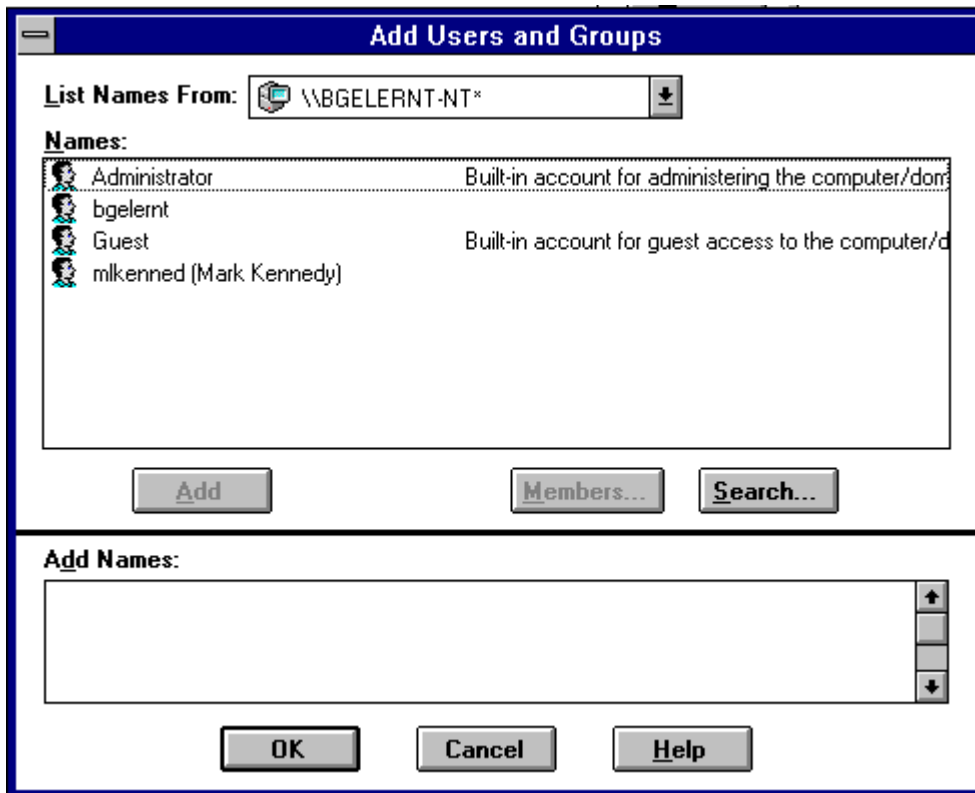
SYSDBA/SYSOPER Authentication Tasks on the Oracle9i Database Server

1. Open User Manager on the Windows NT server where your Oracle9i database is installed.
2. Choose New Local Group from the User Menu.

The New Local Group dialog appears:

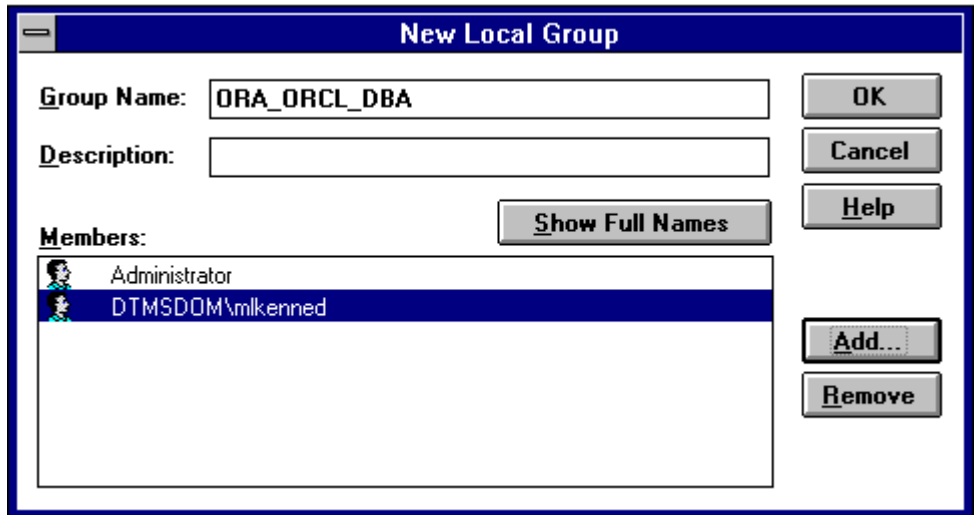


3. Enter the name you have chosen for the new Windows NT local group in the Group Name field. For this example, the **SID** entered is ORCL.
4. Click Add. The Add Users and Groups dialog appears:



5. Select one or more Windows NT users from the Names field and choose Add.
6. Click OK.

Your selection is added to the Members field of the New Local Group dialog:



7. Click OK.
8. Exit User Manager.
9. Ensure that parameter `SQLNET.AUTHENTICATION_SERVICES` in file `sqlnet.ora` contains `nts`.
10. Start Registry Editor from the command prompt:


```
C:\>regedt32
```
11. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME ID` where `ID` is the Oracle home that you want to edit.
12. Set parameter `OSAUTH_PREFIX_DOMAIN` to `true`.

SYSDBA/SYSOPER Authentication Tasks on the Client Computer

1. Create a Windows NT local or domain username with the same username and password that exist on the Windows NT server (if the appropriate username does not currently exist).
2. Ensure that parameter `SQLNET.AUTHENTICATION_SERVICES` in file `sqlnet.ora` contains `nts`.

3. Use Oracle Net Configuration Assistant to configure a network connection from your client computer to the Windows NT server on which your Oracle9i database is installed. See *Oracle9i Net Services Administrator's Guide* for instructions.

4. Start SQL*Plus:

```
C:\> sqlplus
```

5. Connect to Oracle9i database:

```
SQL> SET INSTANCE net_service_name
```

where *net_service_name* is the Oracle Net net service name for Oracle9i database.

6. If you specified `ORA_DBA` or `ORA_SID_DBA` in step 3 of "[SYSDBA/SYSOPER Authentication Tasks on the Oracle9i Database Server](#)", then enter either of the following:

```
SQL> CONNECT / AS SYSOPER
```

```
SQL> CONNECT / AS SYSDBA
```

If you specified `ORA_OPER` or `ORA_SID_OPER` in step 3, then enter:

```
SQL> CONNECT / AS SYSOPER
```

You are now connected to the Windows NT server. If you connect with `SYSDBA`, you are given DBA privileges.

Manually Creating an External Role

This section describes how to grant Oracle9i database roles to users directly through Windows NT (known as external roles). When you use Windows NT to authenticate users, Windows NT local groups can grant these users external roles. Through User Manager, you can create, grant, or revoke external roles to users.

All privileges for these roles are active when the user connects. When using external roles, all roles are granted and managed through the operating system. You cannot use both external roles and Oracle roles at the same time.

Consider the following example. With external roles enabled, you log on to a Windows NT domain with domain username `sales\frank` (`sales` is the domain name and `frank` is the domain username). You then connect to an Oracle9i database as Oracle database user `scott`. In this case, you receive the roles granted to `sales\frank` but *not* the roles granted to `scott`.

The procedure for manually creating an external role is divided into two sets of authorization tasks performed on different computers:

- [External Role Authorization Tasks on the Oracle9i Database Server](#)
- [External Role Authorization Tasks on the Client Computer](#)

External Role Authorization Tasks on the Oracle9i Database Server

1. Add initialization parameter `OS_ROLES` to the `init.ora` file.
2. Set `OS_ROLES` to `true`.
The default setting for this parameter is `false`.
3. Ensure that parameter `SQLNET.AUTHENTICATION_SERVICES` in file `sqlnet.ora` contains `nts`.
4. Start SQL*Plus:

```
C:\> sqlplus / NOLOG
```

5. Connect to your Windows NT server:

```
SQL> CONNECT / AS SYSDBA
```

6. Create a new database role. You can give this new role whatever name you want. In this example the role is named `DBSALES3`:

```
SQL> CREATE ROLE DBSALES3 IDENTIFIED EXTERNALLY;
```

7. Grant to `DBSALES3` whatever Oracle roles are appropriate to your database environment:

```
SQL> GRANT DBA TO DBSALES3 WITH ADMIN OPTION;
```

```
SQL> GRANT RESOURCE TO DBSALES3 WITH ADMIN OPTION;
```

```
SQL> GRANT CONNECT TO DBSALES3 WITH ADMIN OPTION;
```

8. Connect to the database as `SYSDBA`:

```
SQL> CONNECT / AS SYSDBA
```

9. Shut down the database:

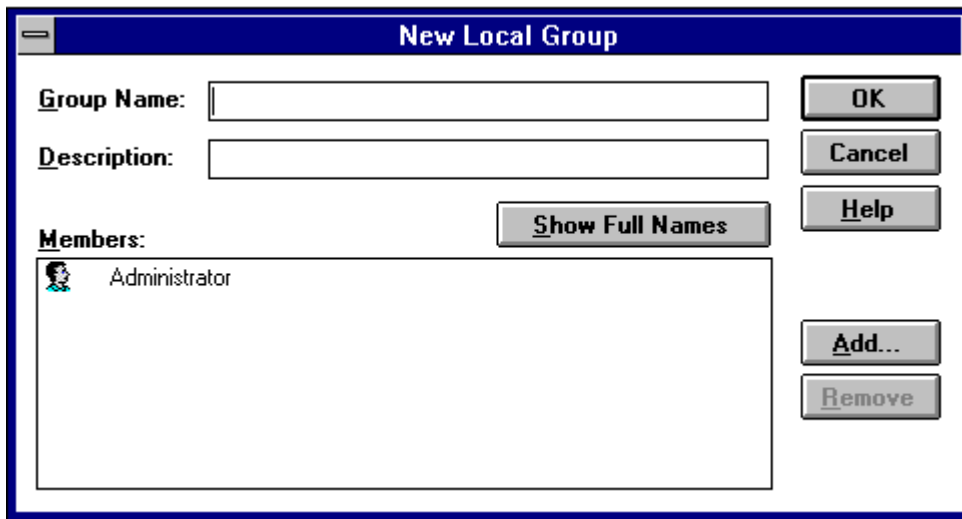
```
SQL> SHUTDOWN
```

10. Restart the database:

```
SQL> STARTUP
```

11. Open Windows NT User Manager.
12. Choose New Local Group from the User menu.

The New Local Group dialog appears:



13. Enter the Windows NT local group name corresponding to the database role in the Group Name field with the following syntax:

```
ORA_sid_rolename [_D] [_A]
```

where

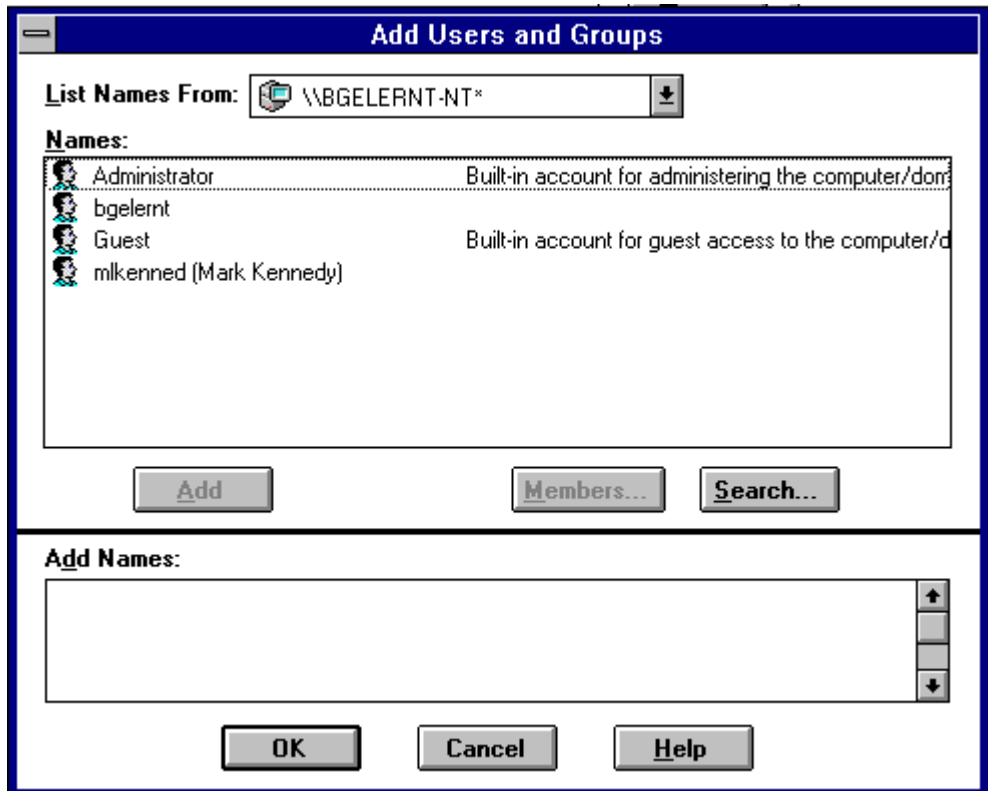
- *sid* identifies the database instance
- *rolename* identifies the database role granted
- *D* indicates that this database role is to be a default role of the database user
- *A* indicates that this database role includes ADMIN OPTION

Characters *D* and *A* are optional. If specified, they must be preceded by an underscore.

For this example, `ORA_orcl_dbsales3_D` is entered.

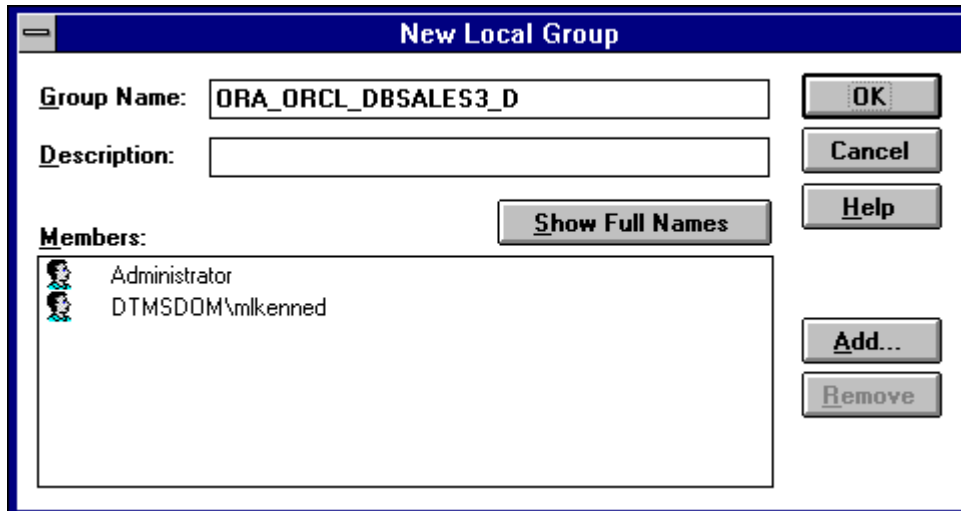
14. Click Add.

The Add Users and Groups dialog appears:



15. Select the Windows NT local or domain username you want to add and choose Add.
16. Click OK.

Your selection is added to the Members field of the New Local Group dialog:



You can create multiple database roles and grant them to several possible Windows NT groups with differing options, as shown in the following table. Users connecting to the ORCL instance and authenticated by Windows NT as members of all four of these Windows NT local groups will have the privileges associated with `dbsales3` and `dbsales4` by default (because of option `_D`). If these users first connect as members of `dbsales3` or `dbsales4` and use the `SET ROLE` command, then they can also gain access to database roles `dbsales1` and `dbsales2`. But if these users try to connect with `dbsales1` or `dbsales2` without first connecting with a default role, they are unable to connect. Finally, these users can grant `dbsales2` and `dbsales4` to other roles (because of option `_A`).

Database Roles	Windows NT Groups
<code>dbsales1</code>	<code>ORA_ORCL_dbsales1</code>
<code>dbsales2</code>	<code>ORA_ORCL_dbsales2_a</code>
<code>dbsales3</code>	<code>ORA_ORCL_dbsales3_d</code>
<code>dbsales4</code>	<code>ORA_ORCL_dbsales4_da</code>

Note: When Oracle9i database converts the group name to a role name, it changes the name to uppercase.

17. Click OK.
18. Exit User Manager.

External Role Authorization Tasks on the Client Computer

1. Create a Windows NT local or domain username with the same username and password that exist on the Windows NT server (if the appropriate username does not currently exist).
2. Ensure that parameter `SQLNET.AUTHENTICATION_SERVICES` in file `sqlnet.ora` contains `nts`.
3. Use Oracle Net Configuration Assistant to configure a network connection from your client computer to your Oracle9i database. See *Oracle9i Net Services Administrator's Guide* for instructions.

4. Start SQL*Plus:

```
C:\> sqlplus / NOLOG
```

5. Connect to the correct instance:

```
SQL> SET INSTANCE connect_identifier
```

where *connect_identifier* is the net service name for the Oracle9i database connection that you created in Step 3.

6. Connect to Oracle9i database:

```
SQL> CONNECT scott/tiger AS SYSDBA
```

You are connected to the Windows NT server over net service with Oracle username `scott/tiger`. Roles applied to Oracle username `scott` consist of all roles defined for the Windows NT username that were previously mapped to the database roles (in this case, `ORA_DBSALES3_D`). All roles available under an authenticated connection are determined by the Windows NT username and the Oracle-specific Windows NT local groups to which the user belongs (for example, `ORA_SID_DBSALES1` or `ORA_SID_DBSALES4_DA`).

Note: OSDBA and OSOPER are generic names for two special operating system groups that control database administrator logins when using operating system authentication. On Windows NT, OSDBA and OSOPER are mapped to local groups in User Manager. Windows NT-specific names for OSDBA and OSOPER are described in "[Manually Granting Administrator and Operator Privileges for Databases](#)" on page 2-36. See *Oracle9i Database Administrator's Guide* for more information on OSDBA and OSOPER.

Manually Migrating Users

You can migrate local or external users to enterprise users with User Migration Utility. Migrating from a database user model to an enterprise user model provides solutions to administrative, security, and usability challenges in an enterprise environment. In an enterprise user model, all user information is moved to an LDAP directory service, which provides the following benefits:

- Centralized storage and management of user information
- Centralized user authentication
- Enhanced security

User Migration Utility is a command-line tool. Its syntax is of the form:

```
C:\ umu parameters
```

To get a list of User Migration Utility parameters, enter:

```
C:\ umu help=yes
```

See Also: For more information on User Migration Utility, see "Migrating Local or External Users to Enterprise Users" in *Oracle Advanced Security Administrator's Guide*

Administering Enterprise Users and Roles

Use Oracle Enterprise Security Manager to create and manage enterprise users, roles, and domains. Oracle Enterprise Security Manager is included as an integrated application of Oracle Enterprise Manager Console. See *Oracle Advanced Security Administrator's Guide* for more information on using Oracle Enterprise Security Manager.

This chapter contains these topics:

- [Enterprise User Authentication](#)
- [Enterprise Role Authorization](#)

Note: You can administer an **external user** or an **external role** in Windows 2000 domains, but you cannot use Oracle Enterprise Security Manager to perform this administration. See [Chapter 2, "Administering External Users and Roles"](#) for more information on tools available for administering external users and roles.

Enterprise User Authentication

Enterprise users are created and managed centrally in a directory server (for example, Oracle Internet Directory or Active Directory). To allow access to multiple databases, enterprise users need to be defined in *each* database as an external user.

For example, assume there is an **enterprise user** (`cn=joe,cn=users,dc=acme,dc=com`) who needs access to two databases: `sales` and `marketing`. This enterprise user must be defined in both databases as an external user.

Most users typically need to access only application schemas in a database, so they usually do not need their own schemas. In Oracle9i, you can create one shared **schema** in the database and map multiple enterprise users in a directory server to this one shared schema with Oracle Enterprise Security Manager. This is especially useful in an Internet environment, where a number of users access an application at the same time. With a shared schema there is no need to create separate schemas for each user.

See Also: *Oracle Advanced Security Administrator's Guide* for more information

Enterprise user authentication is enabled, if you:

- Set **registry** parameter `OSAUTH_X509_NAME` to `true`. (See "[Oracle9i Integration with Active Directory](#)" on page 1-5 for instructions.)
- Operate your Oracle9i database in a Windows 2000 domain.
- Use Oracle Enterprise Security Manager. If you are using shared schema you must use Oracle Enterprise Security Manager to map enterprise users to the shared schema.

The Kerberos authentication protocol is used if Windows and Oracle releases match those listed in [Table 1-1, "Software Requirements to Enable Kerberos Authentication Protocol"](#) on page 1-3. Otherwise, NTLM is used.

Enterprise Role Authorization

An enterprise user is assigned an **enterprise role**; some users are assigned more than one. Enterprise roles **authorization** is supported with Oracle8i release 8.1.6 and later. An enterprise role is a single **role** created in a directory server with Oracle Enterprise Security Manager. Use Oracle Enterprise Security Manager to assign

global roles and groups located on multiple databases to an enterprise role. A **global role** must be created individually in each Oracle9i database.

For example, as an enterprise user you can be assigned enterprise role `HR` (which contains global role `HR user`) in the human resources database. You can also be assigned global role `employee` in the corporate information database. If you change jobs, your enterprise role assignment is changed only in the directory, altering your privileges in multiple databases throughout the enterprise. Also, an administrator can add capabilities to enterprise roles or remove a **privilege** from the enterprise role without having to update each user's privileges individually.

Use enterprise roles in environments where users assigned to these roles are located in many geographic regions and must access multiple databases.

See Also: *Oracle Advanced Security Administrator's Guide* for more information on creating and storing enterprise roles in a directory server with Oracle Enterprise Security Manager

Permissions authorized to an enterprise user are authorized for the enterprise role contained in the global role.

Users can belong to Windows 2000 **global groups** and **universal groups**. These groups can be assigned to enterprise roles using Oracle Enterprise Security Manager.

Note: Enterprise roles are authorized by the directory server, and not by setting initialization file parameter `OS_ROLES` to `true` (the method for enabling **external role** authorization).

Storing Oracle Wallets in the Windows Registry

This chapter describes storing and retrieving of Oracle Wallets in the Windows **registry**.

This chapter contains these topics:

- [Storing Private Keys and Trust Points](#)
- [Storing User's Profile](#)
- [Registry Parameters for Wallet Storage](#)
- [Oracle Enterprise Login Assistant](#)
- [Wallet Resource Locator](#)

Storing Private Keys and Trust Points

Oracle Wallets store **private keys**, **trust points**, and **digital certificates** used in public key applications for authentication and **encryption**. Oracle Wallet Manager creates and manages Oracle Wallets. Oracle Enterprise Login Assistant is used to create an **obfuscated** wallet. Oracle Public Key applications use obfuscated Oracle Wallets for authentication and encryption. You can log on once for each session with Oracle Enterprise Login Assistant, and all applications will use the same obfuscated wallet to **authenticate** until you log out. Encrypted and obfuscated Oracle Wallets can be stored in the file system or the user profile area in the Windows registry.

Note: Oracle Wallet Manager, Oracle Enterprise Login Assistant and their related functionality are features of Oracle Advanced Security, a separately licensable option to Oracle9i database.

Storing User's Profile

In a Windows 2000 or Windows NT 4.0 domain, a user's profile is stored on the local computer. When a local user logs on to that computer, that user's profile on the local computer is uploaded into the user profile in that computer's registry. When a user logs out, that user's profile stored on the local file system is updated, ensuring that the domain user or local user always has the most recent user profile version.

Registry Parameters for Wallet Storage

Parameter `WALLET_LOCATION` in file `sqlnet.ora` specifies whether Oracle Wallets are stored in the file system or in the user profile area in the registry:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS
```

It also specifies the location of the encrypted or obfuscated Oracle Wallet. The wallets are stored in the same format as those in the file system. All functionality is the same except for the location of the wallets.

For example, the `WALLET_LOCATION` parameter for storing an Oracle Wallet in the registry in:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\SALESAPP
```

would be:

```
WALLET_LOCATION = (SOURCE= (METHOD=REG) (METHOD_DATA= (KEY=SALESAPP)))
```

Continuing the example, the encrypted Oracle Wallet would be stored in the registry in:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\ORACLE\WALLETS\SALESAPP\EWALLET.P12
```

and the obfuscated Oracle Wallet would be stored in:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\ORACLE WALLETS\SALESAPP\CWALLET.SSO
```

Oracle Wallet Manager

Oracle Wallet Manager creates and manages Oracle Wallets. If you want to use the Windows registry for Oracle Wallets, then you must select the Use Windows System Registry check box. If Windows System Registry is selected, the tool shows a list of existing keys when it opens a wallet or saves a new wallet. The list appears in:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS
```

You can select one of the existing locations or enter the name for a new location (registry key). If you enter a new key called `key1`, for example, then the tool creates the following registry key:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\KEY1
```

The encrypted wallet will be stored in:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\KEY1\EWALLET.P12
```

The obfuscated wallet will be stored in:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\KEY1\CWALLET.SSO
```

If you do not select the Use Windows System Registry check box, then the tool displays all the available drives and directories on the local computer. You can select one of the existing directories or enter a new directory. The tool stores the encrypted or obfuscated wallet in the selected directory or creates the directory if it does not exist.

Oracle Enterprise Login Assistant

When you start Oracle Enterprise Login Assistant, the tool first looks for an obfuscated wallet at the registry location:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\DEFAULT
```

If the tool finds no obfuscated wallet in the registry, it looks for an obfuscated wallet at the file system location:

```
%USERPROFILE%\ORACLE\WALLETS
```

If Oracle Enterprise Login Assistant finds an obfuscated wallet at either location, then it returns a message stating that autologin has been enabled. If you select Logout at this point, then the tool removes the obfuscated wallet from wherever it found it (that is, either the registry or file system default locations). If you exit the tool without selecting Logout, then the obfuscated wallet is left where it was found.

If Oracle Enterprise Login Assistant does not find an obfuscated wallet at the default registry or file system locations, then the tool displays a message stating that autologin is not enabled.

If autologin is not enabled and you select Login, then Oracle Enterprise Login Assistant looks for an encrypted wallet at the registry location:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\DEFAULT
```

If the tool finds no encrypted wallet in the registry, then it looks for an encrypted wallet in the local computer at the file system location:

```
%USERPROFILE%\ORACLE\WALLETS
```

If the tool finds an encrypted wallet at either location, then you are prompted for the wallet password. If you enter the correct password, then the tool creates an obfuscated wallet in the registry or the file system, depending on where it found the encrypted wallet. At the next Logout in the same session of the tool, it removes the obfuscated wallet from the registry or file system. If you exit Oracle Enterprise Login Assistant without selecting Logout, then the tool does not remove the obfuscated wallet.

If you select Login and Oracle Enterprise Login Assistant finds no encrypted wallet in the default registry or file system locations, then the tool displays a message stating that no Oracle Wallet was found in the default locations.

Wallet Resource Locator

Parameter `WALLET_LOCATION` in file `sqlnet.ora` is extended to support Oracle Wallets in the registry. `WALLET_LOCATION` specifies the location of the obfuscated Oracle Wallet for use by Oracle PKI applications.

On Windows operating systems, if there is no value specified for parameter `WALLET_LOCATION` in file `sqlnet.ora`, Oracle PKI applications first look for the obfuscated wallet in registry key:

```
\\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\DEFAULT
```

If no obfuscated wallet is found there, Oracle PKI applications look for it in the file system of the local computer at location:

```
%USERPROFILE%\ORACLE\WALLETS
```

If no obfuscated Oracle Wallet is found in the registry or file system default locations, then a `No Oracle Wallet exists` error is displayed.

Windows 2000 PKI Integration

This chapter describes integration of Oracle public key infrastructure (PKI) with Windows 2000 public key infrastructure (Windows PKI) on Windows operating systems.

This chapter contains these topics:

- [Oracle Public Key Infrastructure](#)
- [Windows Public Key Infrastructure](#)

Oracle Public Key Infrastructure

Oracle public key infrastructure (PKI) is used by Oracle Enterprise Security Manager, **LDAP**-enabled Oracle Enterprise Manager, Oracle's Secure Socket Layer (SSL) authentication, Oracle9i database, and Oracle Application Server.

Oracle PKI includes the following components:

- Oracle Wallets
- Oracle Wallet Manager (OWM)
- Oracle Enterprise Login Assistant

Oracle Wallets store **digital certificates**, **trust points**, and **private keys** used in public key applications for **encryption**, **decryption**, **digital signature**, and verification. Oracle Wallet Manager (OWM) creates an encrypted Oracle Wallet that holds the digital certificates. Oracle Enterprise Login Assistant creates or deletes decrypted, **obfuscated** Oracle Wallets.

Windows Public Key Infrastructure

This section describes Windows public key infrastructure.

This section contains these topics:

- [Microsoft Certificate Stores](#)
- [Microsoft Certificate Services](#)
- [Wallet Resource Locator](#)

Note: Microsoft Certificate Store integration works only with digital certificates that use Microsoft Enhanced Cryptographic Provider. To create these certificates, you need to install Windows High Encryption Pack and select Microsoft Enhanced Cryptographic Provider. Also, when there are more than one of these certificates available for the same key usage (signature/key exchange), the first certificate retrieved will be used for Oracle SSL.

Microsoft Certificate Stores

Microsoft Certificate Stores are repositories for storing digital certificates and their associated properties. Windows 2000 stores digital certificates and certificate revocation lists in logical and physical stores. Logical stores contain pointers to **public key** objects in physical stores. Logical stores enable public key objects to be shared between users, computers, and services without requiring storage of duplicates of objects for each user, computer, or **service**. Public key objects are physically stored in the **registry** of the local computer or, for some user certificates, in Active Directory. Standard system certificate stores defined by Microsoft include:

- MY or Personal
- CA
- ROOT

MY or Personal holds a user's certificates for which the associated private key is available. The MY certificate store maintains certificate properties that indicate the Cryptographic Service Provider (CSP) associated with the private key. An application uses this information to obtain the private key from the CSP for the associated certificate. CA holds issuing or intermediate **certificate authority** (CA) certificates. ROOT holds only self-signed CA certificates for trusted root CAs.

Microsoft Certificate Services

Microsoft Certificate Services (MCS) consists of the following modules:

- Server Engine
- Intermediary
- Policy

Server Engine handles all certificate requests. It interacts with other modules at each processing stage to ensure that the proper action is taken based on the state of the request. The Intermediary module receives requests for new certificate from clients and then submits them to Server Engine. The Policy module contains the set of rules controlling the issuance of certificates. This module may be upgraded or customized as needed.

Wallet Resource Locator

Wallet Resource Locator (WRL) specifies that parameter `WALLET_LOCATION` in file `sqlnet.ora` identifies a particular PKI. You can choose between using Oracle Wallet or Microsoft Certificate Stores by setting parameter `WALLET_LOCATION` in `sqlnet.ora`. To use **credentials** from Microsoft Certificate Stores, set parameter `WALLET_LOCATION` in `sqlnet.ora` to:

```
WALLET_LOCATION = (SOURCE = (METHOD=MCS))
```

The Oracle application uses Oracle's TCP/IP with SSL protocol (TCPS) to connect to Oracle Server. The SSL protocol uses X.509 certificates and trust points from the user's Microsoft Certificate Store for SSL authentication.

Oracle Net Services Configuration

This appendix describes Oracle Net Services configuration for Windows. For more generic information on Oracle Net Services configuration, see *Oracle9i Net Services Administrator's Guide*.

This appendix contains these topics:

- [Understanding Oracle Net Services Registry Parameter and Subkeys](#)
- [Listener Requirements](#)
- [Understanding Optional Configuration Parameters](#)
- [Advanced Network Configuration](#)

See Also: Oracle Net Services integration with Active Directory for Windows 2000 in "Using Enterprise User Security with Microsoft Active Directory" in *Oracle Advanced Security Administrator's Guide*

Understanding Oracle Net Services Registry Parameter and Subkeys

The registry contains entries for Oracle Net Services parameters and subkeys. To successfully add or modify Oracle Net Services configuration parameters, you must understand where they are located and the rules that apply to them.

Oracle Net Service Subkeys

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services contains subkeys that correspond to services. Depending on what is installed, your Oracle Net Services consist of all or a subset of the following:

- OracleHOME_NAMEClientCache
- OracleHOME_NAMECMAdmin
- OracleHOME_NAMECMan
- OracleHOME_NAMETNSListener

Each service subkey contains the parameters shown in [Table A-1](#).

Table A-1 Service Subkey Parameters

Parameter	Description
DisplayName	Specifies service name.
ImagePath	Specifies fully qualified path name of executable invoked by service and any command line arguments passed to executable at runtime.
ObjectName	Specifies logon user account and computer to which service should log on.

Listener Requirements

In Oracle9i release 2 (9.2), the listener is set to start automatically at system restart. If you intend to use only the listener for all of your databases, ensure that only the Windows NT service for the listener, as listed in the Control Panel, is set to start automatically.

Oracle Corporation normally recommends that you only have a single net listener service running on a Windows NT computer at any one time. This single listener can support multiple databases. If you need to have two different net listener services running on a Windows NT computer at the same time, make sure that they are configured to listen on different TCP/IP port numbers.

If the same IP address and port are used for different listeners, you might expect that the second and subsequent listeners would fail to bind. Instead, Windows NT allows them all to listen on the same IP address and port, resulting in unexpected behavior of the listeners. This is a suspected Windows NT operating system problem with TCP/IP and has been reported to Microsoft.

Understanding Optional Configuration Parameters

You can use the following parameters on Windows NT and Windows 98:

- LOCAL
- TNS_ADMIN
- USE_SHARED_SOCKET

Oracle Net Service first checks for the parameters as environment variables, and uses the values defined. If environment variables are not defined, it searches for these parameters in the registry.

LOCAL

You can use parameter LOCAL to connect to Oracle9i database without specifying a connect identifier in the connect string. The value of parameter LOCAL is any connect identifier, such as a net service name. For example, if parameter LOCAL is specified as *finance*, you can connect to a database from SQL*Plus with:

```
SQL> CONNECT scott/tiger
```

rather than

```
SQL> CONNECT scott/tiger@finance
```

Oracle Net checks if LOCAL is defined as an environment variable or as a parameter in the registry, and uses *finance* as the service name. If it exists, Oracle Net connects.

TNS_ADMIN

You can add parameter TNS_ADMIN to change the directory path of Oracle Net Services configuration files from the default location of *ORACLE_HOME\network\admin*. For example, if you set TNS_ADMIN to *ORACLE_BASE\ORACLE_HOME\test\admin*, the configuration files are used from *ORACLE_BASE\ORACLE_HOME\test\admin*.

USE_SHARED_SOCKET

You can set parameter `USE_SHARED_SOCKET` to `true` to enable use of shared sockets. If this parameter is set to `true`, the network listener passes the socket descriptor for client connections to the database thread. As a result, the client does not need to establish a new connection to the database thread and database connection time improves. Also, all database connections share the port number used by the network listener, which can be useful if you are setting up third-party proxy servers.

This parameter only works in dedicated server mode in a TCP/IP environment. If this parameter is set, you cannot use the 9.0 listener to spawn Oracle7 release 7.x databases. To spawn a dedicated server for an Oracle database not associated with the same Oracle home as the listener and have shared socket enabled, you must also set parameter `USE_SHARED_SOCKET` for both Oracle homes.

Advanced Network Configuration

The following sections describe advanced configuration procedures specifically for Oracle Net Services on Windows operating systems.

Configuring Authentication Method

Oracle Net Services provides authentication methods for Windows operating systems using Windows Native Authentication.

Configuring Security for Named Pipes Protocol

The network listener service may be unable to open the Named Pipe created by Oracle Names unless service `OracleHOME_NAME*TN*Listener` has a valid user ID and password associated with it.

To set up the network listener permissions:

1. From the Control Panel window, double-click Services.
The Services window appears.
2. Double-click service `OracleHOME_NAME*TN*Listener`.
The Services dialog box appears.
3. Choose option This Account. Then choose option "... " next to it.
The Add User dialog box appears.

4. Select your logon ID (user ID) from the Names list and choose Add.
The user ID appears in the Add Name text box.
5. Click OK.
The Services dialog box appears with the user ID displayed in text box This Account.
6. Type your password in the Password text box.
7. Retype the same logon password in the Confirm Password text box.
8. Click OK.

Glossary

Active Directory Service Interfaces (ADSI)

A client-side product based on Component Object Model (COM). ADSI defines a directory service model and a set of COM interfaces that enable Windows 2000, Windows NT, Windows 98, and Windows 95 client applications to access several network directory services, including Active Directory. ADSI allow applications to communicate with Active Directory.

alert file

A file that contains important information and error messages that are generated during database operations.

authenticate

To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite for allowing access to resources in a system.

authorization

Permission given to a user, program, or **process** to access an object or set of objects. In Oracle, authorization is done through the **role** mechanism. A single person or a group of people can be granted a role or a group of roles. A role, in turn, can be granted other roles.

certificate authority

A certificate authority (CA) is a trusted third party that certifies the identity of other entities such as users, databases, administrators, clients, and servers. The certificate authority verifies the user's identity and grants a certificate, signing it with one of the certificate authority's **private keys**.

connect descriptor

A specially formatted description of the destination for a network connection. A connect descriptor contains destination **service** and network route information. The destination service is indicated by using its service name for Oracle9i or Oracle8i databases or its Oracle **system identifier (SID)** for Oracle8 release 8.0 databases. The network route provides, at a minimum, the location of the **listener** through use of a network address.

connect identifier

A **net service name** or service name, that maps to a **connect descriptor**. Users initiate a connect request by passing a **username** and password along with a connect identifier in a **connect string** for the **service** to which they wish to connect, for example:

```
CONNECT username/password@connect_identifier
```

connect string

Information the user passes to a **service** to connect, such as **username**, password and **net service name**. For example:

```
CONNECT username/password@net_service_name
```

control file

A file that records the physical structure of a database and contains database name, names and locations of associated databases and online redo log files, timestamp of database creation, current log sequence number, and checkpoint information.

credentials

A **username**, password, or certificate used to gain access to the database.

data dictionary

A set of read-only tables that provide information about a database.

database alias

See **net service name**.

decryption

Process of converting contents of a message that has gone through **encryption** (ciphertext) back into its original readable format (plaintext).

digital certificates

ITU X.509 v3 standard data structures that securely bind an identity to a **public key**. A certificate is created when an entity's public key is signed by a trusted identity, a **certificate authority**. The certificate ensures that the entity's information is correct and that the public key actually belongs to that entity.

digital signature

Digital signatures are created when a **public key** algorithm is used to sign messages with senders' **private keys**. A digital signature assures that a document is authentic, has not been forged by another entity, has not been altered, and cannot be repudiated by the sender.

encryption

Process of disguising a message, rendering it unreadable to any but the intended recipient.

enterprise domains

Directory constructs consisting of Oracle9i databases and enterprise users and roles. Enterprise domains are different from Windows 2000 domains, which are collections of computers that share a common directory database.

enterprise role

A directory structure which contains global roles on multiple databases, and which can be granted to an **enterprise user**.

enterprise user

A user that has a unique identity across an enterprise. An enterprise user connects to individual databases through a **schema** and is assigned an **enterprise role** that determines the user's access privileges on databases.

external role

Roles created and managed by Windows NT and Windows 2000 operating systems. Once an external role is created, you can grant or revoke that **role** to a database user. You must set **init.ora** parameter `OS_ROLES` to `true` and restart your Oracle database before you can create an external role. You cannot use both Windows operating systems and the Oracle database to grant roles concurrently.

external user

A user authenticated by the Windows 2000 or Windows NT operating system who can access the Oracle database without being prompted for a password. External

users are typically regular database users (non-database administrators) to which you assign standard database roles (such as `CONNECT` and `RESOURCE`), but do not want to assign **`SYSDBA`** (database administrator) or **`SYSOPER`** (database operator) **privilege**.

forest

A group of one or more Active Directory trees that trust each other. All trees in a forest share a common **schema**, configuration, and global catalog. When a forest contains multiple trees, the trees do not form a contiguous namespace. All trees in a given forest trust each other through transitive bidirectional trust relationships.

global groups

See **Windows NT global groups**.

global role

A role whose privileges are contained within a single database, but which is managed in a directory.

HOMEID

Represents a unique **registry** subkey for each Oracle home directory in which you install products. A new `HOMEID` is created and incremented each time you install products to a different Oracle home directory on one computer. Each `HOMEID` contains its own configuration parameter settings for installed Oracle products.

HOME_NAME

Represents the name of an **ORACLE_HOME**. All Oracle homes have a unique `HOME_NAME`.

init.ora

See **initialization parameter file**.

initialization parameter file

An ASCII text file that contains information needed to initialize a database and **instance**. File `init.ora` resides in directory `\ORACLE_BASE\admin\DB_NAME\pfile` on Windows operating systems.

instance

Every running Oracle database is associated with an Oracle instance. When a database is started on a database server (regardless of computer type), Oracle allocates a memory area called **System Global Area (SGA)** and starts an Oracle

process. This combination of SGA and an Oracle process is called an instance. The memory and the process of an instance manage the associated database's data efficiently and serve the one or more database users.

LDAP

See [Lightweight Directory Access Protocol \(LDAP\)](#).

Lightweight Directory Access Protocol (LDAP)

A standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate. LDAP is a framework of design conventions supporting industry-standard directory products, such as Oracle Internet Directory.

listener

A **process** that resides on the server whose responsibility is to listen for incoming client connection requests and manage traffic to the server. Every time a client requests a network session with a server, a listener receives the actual request. If client information matches listener information, then the listener grants a connection to the server.

listener.ora

A configuration file for the **listener** that identifies listener name, protocol addresses for accepting connection requests, and the services for which it is listening.

File `listener.ora` typically resides in `ORACLE_BASE\ORACLE_HOME\network\admin` on Windows operating systems.

local groups

See [Windows NT local groups](#).

local roles

Roles created and managed by the database. Once a local role is created, you can grant or revoke that **role** to a database user. You cannot use Windows NT (for **external role** management) and the Oracle database (for local role management) concurrently.

Microsoft Management Console

An application that serves as a host for administrative tools called snap-ins. By itself, Microsoft Management Console does not provide any functionality.

mount

To associate a database with an **instance** that has been started.

multiple Oracle homes

Capability of having more than one Oracle home on a computer.

net service name

Name used by clients to identify a database server. A net service name is mapped to a port number and protocol. Also known as a **connect string**, or **database alias**.

network listener

A listener on a server that listens for connection requests for one or more databases on one or more protocols. See **listener**.

network service

In an Oracle application network, a service performs tasks for its service consumers. For example, an Oracle Names server provides name resolution services for clients.

obfuscated

Obfuscated information is scrambled into a non-readable form. De-scrambling is extremely difficult if the algorithm used for scrambling is not known.

ORACLE_BASE

Oracle base, known as *ORACLE_BASE* in this guide, is the root of the Oracle directory tree.

ORACLE_HOME

Corresponds to the environment in which Oracle products run. This environment includes location of installed product files, PATH variable pointing to products' binary files, **registry** entries, net service names, and program groups.

Oracle Net

A component of **Oracle Net Services** that enables a network session from a client application to an Oracle database server. Once a network session is established, Oracle Net acts as a data courier for the client application and the database server. It is responsible for establishing and maintaining the connection between the client application and database server, as well as exchanging messages between them. Oracle Net is able to perform these jobs because it is located on each computer in the network.

Oracle Net Services

A suite of networking components that provide enterprise-wide connectivity solutions in distributed, heterogeneous computing environments. Oracle Net Services are comprised of **Oracle Net, listener**, Oracle Connection Manager, Oracle Net Configuration Assistant, and Oracle Net Manager.

Oracle service

A **service** that is associated with an Oracle component.

private keys

In **public key cryptography**, these are the secret keys. They are used primarily for **decryption** but also for **encryption** with a **digital signature**.

privilege

A right to execute a particular type of SQL statement or to access another user's object.

process

A mechanism in an operating system that can run an executable. (Some operating systems use the term job or task.) A process normally has its own private memory area in which it runs. On Windows NT, a process is created when a program runs (such as Oracle or Microsoft Word). In addition to an executable program, all processes consist of at least one **thread**. The Oracle master process contains hundreds of threads.

public key

In **public key cryptography**, this key is made public to all. It is primarily used for **encryption** but can also be used for verifying signatures.

public key cryptography

Public key cryptography involves information **encryption** and **decryption** using a shared **public key** paired with **private keys**. Provides for secure, private communications within a public network.

quota

A limit on a resource, such as a limit on the amount of database storage used by a database user. A database administrator can set **tablespace** quotas for each Oracle **username**.

recovery

To restore a physical backup is to reconstruct it and make it available to the Oracle server. To recover a restored backup is to update it using redo records (that is, records of changes made to the database after the backup was taken). Recovering a backup involves two distinct operations: rolling forward the backup to a more current time by applying redo data, and rolling back all changes made in uncommitted transactions to their original state.

registry

A Windows repository that stores configuration information for a computer.

remote computer

A computer on a network other than the local computer.

role

A named group of related privileges. You can grant a role to users or other roles.

schema

A named collection of objects, such as tables, [views](#), clusters, procedures, and packages, associated with a particular user.

service

An executable [process](#) installed in the [registry](#) and administered by Windows NT. Once a service is created and started, it can run even when no user is logged on to the computer.

service name

See [net service name](#).

SID

See [system identifier \(SID\)](#).

SYSDBA

A special database administration [role](#) that contains all system privileges with ADMIN OPTION, and [SYSOPER](#) system [privilege](#). SYSDBA also permits CREATE DATABASE actions and time-based [recovery](#).

SYSOPER

A special database administration **role** that permits a database administrator to perform `STARTUP`, `SHUTDOWN`, `ALTER DATABASE OPEN/MOUNT`, `ALTER DATABASE BACKUP`, `ARCHIVE LOG`, and `RECOVER`, and includes `RESTRICTED SESSION` **privilege**.

System Global Area (SGA)

A group of shared memory structures that contain data and control information for an Oracle **instance**.

system identifier (SID)

A unique name for an Oracle **instance**. To switch between Oracle databases, users must specify the desired SID. The SID is included in the `CONNECT DATA` parts of the **connect descriptor** in a `tnsnames.ora` file, and in the definition of the **network listener** in a `listener.ora` file.

SYSTEM

A standard DBA **username** automatically created with each database. `SYSTEM` is created with an initial password of `MANAGER`. Username `SYSTEM` is the preferred username for DBAs to use for database maintenance.

tablespace

A database is divided into one or more logical storage units called tablespaces. Tablespaces are divided into logical units of storage called segments, which are further divided into extents.

thread

An individual path of execution within a **process**. Threads are objects within a process that execute program instructions. Threads allow concurrent operations within a process so that a process can execute different parts of its program simultaneously on different processors. A thread is the most fundamental component that can be scheduled on Windows NT.

tnsnames.ora

A file that contains connect descriptors; each **connect descriptor** is mapped to a **net service name**. The file may be maintained centrally or locally, for use by all or individual clients. This file typically resides in `ORACLE_BASE\ORACLE_HOME\network\admin` on Windows NT.

trust points

Trust points or trusted certificates are third party identities that are qualified with a level of trust. A trusted certificate is used when an identity is being validated as the entity it claims to be. Certificate authorities you trust are called trusted certificates. If there are several levels of trusted certificates, a trusted certificate at a lower level in the certificate chain does not need to have all its higher level certificates reverified.

universal groups

Universal groups are available in Windows 2000, but not in Windows NT. They can contain other groups, including other universal groups, **local groups**, and **global groups**.

username

A name that can connect to and access objects in a database.

views

Selective presentations of one or more tables (or other views), showing both their structure and their data.

Windows NT global groups

Groups that can be granted permissions and rights in their own domain, member servers and workstations of their domain, and in trusted domains. They can also become members of **Windows NT local groups** in all these places. But global groups can contain user accounts only from their own domains.

Windows NT local groups

Groups that can be granted permissions and rights only for its own computer or, if part of a domain, to the domain controllers of that domain. Local groups can, however, contain user accounts and **Windows NT global groups** from both their own domain and from trusted domains.

Index

A

- authentication
 - automatically enabling during installation, 1-8
 - enhancements, 1-4
 - OSAUTH_PREFIX_DOMAIN parameter, 2-31
 - overview, 1-2
 - using Windows native methods, 1-2
 - viewing parameter settings, 2-12
 - when to use enterprise users, 1-5
 - when to use external users, 1-5
- Authentication Adapters
 - using, A-4
- authentication protocols
 - default protocol used, 1-3
 - with Windows 2000, 1-2
 - with Windows NT 4.0, 1-2
- authorization
 - when to use enterprise roles, 1-5
 - when to use external roles, 1-5

C

- configuration parameters
 - LOCAL, A-3
 - TNS_ADMIN, A-3
 - USE_SHARED_SOCKET, A-4
- configuring
 - Authentication Adapters, A-4
 - Named Pipes Protocol Adapter, A-4
- CONNECT /AS SYSDBA
 - connecting without a password, 1-8
- connecting
 - LOCAL parameter, A-3

D

- database administrator privileges
 - for a single database on a computer, 2-26
 - for all databases on a computer, 2-5, 2-7
- database operator privileges
 - for a single database on a computer, 2-28
 - for all databases on a computer, 2-5, 2-7
- database privileges
 - in Windows NT local groups, 2-42, 2-44
- DisplayName parameter, A-2

E

- enterprise roles
 - authorizing in Windows 2000 domains, 3-2, 3-3
 - environments in which to use, 1-5
- enterprise users
 - environments in which to use, 1-5
- external OS user
 - creating, 2-13, 2-30
- external roles
 - administering, 2-2, 2-30
 - creating, 2-22
 - environments in which to use, 1-5
- external users
 - administering, 2-2, 2-30
 - creating, 2-13, 2-30
 - environments in which to use, 1-5

I

- ImagePath parameter, A-2
- initialization parameters

OS_ROLES, 1-4, 3-3

K

Kerberos, 3-2
default use of, 1-3
features, 1-2

L

local database role
creating with Oracle Administration Assistant for
Windows NT, 2-18
local groups
with database privileges, 2-42, 2-44
LOCAL networking parameter, A-3

M

Microsoft Certificate Services, 5-3
Microsoft Certificate Stores, 5-3
Microsoft Management Console
requirements, 2-3

N

Named Pipes Protocol Adapter
with an Oracle Names Server, A-4
networking parameters
LOCAL, A-3
TNS_ADMIN, A-3
USE_SHARED_SOCKET, A-4
NTLM, 3-2
default use of, 1-3
features, 1-2
NTS. *See* Windows native authentication

O

ObjectName parameter, A-2
operating system authentication
automatically enabling during installation, 1-8
connecting as SYSDBA without a password, 1-8
OSAUTH_PREFIX_DOMAIN parameter, 2-31
operating systems
authentication overview, 1-2

ORA_DBA local group
adding users to, 1-8
Oracle Administration Assistant for Windows NT
adding a computer to the navigation tree, 2-4
connecting to a database, 2-8
creating a local database role, 2-18
creating an external OS user, 2-13
creating an external role, 2-22
database connection issues, 2-10
granting administrator privileges, 2-26
granting operator privileges, 2-28
managing remote computers, 2-3
saving a navigation tree configuration, 2-4
setting OS_AUTHENT_PREFIX, 2-12
using, 2-2
viewing authentication settings, 2-12
Oracle Enterprise Security Manager
using, 1-7
Oracle Names
Named Pipes Protocol Adapter, A-4
Oracle public key infrastructure, 5-2
Oracle Wallet Manager, 4-3
Oracle Wallets, 4-2
storing in the registry, 4-2
storing private keys and trust points, 4-2
Oracle9i Database Administrator's Guide, 2-19
OracleHOME_NAMEClientCache, A-2
OracleHOME_NAMEECMAAdminService, A-2
OracleHOME_NAMEECManService, A-2
OracleHOME_NAMETNSListener, A-2
OracleHOME_NAMETNSListener service, A-4
OS_AUTHENT_PREFIX parameter
case insensitivity, 2-31
defined, 2-12
using, 2-31
OS_ROLES parameter
defined, 2-12
not required in Windows 2000 domains, 3-3
using with external roles, 1-4
OSAUTH_PREFIX_DOMAIN, 2-31
OSAUTH_PREFIX_DOMAIN parameter, 2-3, 2-31
OSAUTH_X509_NAME parameter, 3-2

P

parameters

- DisplayName, A-2
- ImagePath, A-2
- LOCAL, A-3
- ObjectName, A-2
- OS_AUTHENT_PREFIX, 2-12
- OS_ROLES, 2-12
- OSAUTH_PREFIX_DOMAIN, 2-3, 2-31
- OSAUTH_X509_NAME, 3-2
- TNS_ADMIN, A-3
- USE_SHARED_SOCKET, A-4

passwords

- not needed with SYSDBA, 1-8

privileges

- in Windows NT local groups, 2-42, 2-44

R

registry

- DisplayName, A-2
- ImagePath, A-2
- ObjectName, A-2
- OracleHOME_NAMEClientCache, A-2
- OracleHOME_NAMECMAdminService, A-2
- OracleHOME_NAMECMANService, A-2
- OracleHOME_NAMETNSListener, A-2
- OSAUTH_PREFIX_DOMAIN, 2-31

remote computers

- managing with Oracle Administration Assistant for Windows NT, 2-3

role authorization

- description, 1-4
- in Windows 2000 domains, 3-2
- method enhancements, 1-4

roles

- authorized in Windows 2000 domains, 3-3
- creating, 2-22
- creating a local database role with Oracle Administration Assistant for Windows NT, 2-18
- when to use enterprise roles, 1-5
- when to use external roles, 1-5

S

SET INSTANCE command, 2-40, 2-45

sqlnet.ora file

- and Windows native authentication, 2-39, 2-41
- location of, 2-39, 2-41

storing private keys and trust points

- Oracle Wallets, 4-2

SYSDBA privileges

- connecting without a password, 1-8
- for a single database on a computer, 2-26
- for all databases on a computer, 2-5, 2-7

SYSOPER privileges

- for a single database on a computer, 2-28
- for all databases on a computer, 2-5, 2-7

T

TNS_ADMIN networking parameter, A-3

U

USE_SHARED_SOCKET networking

- parameter, A-4

user authentication

- description, 1-4
- enhancement methods, 1-4
- when to use enterprise users, 1-5
- when to use external users, 1-5

W

Wallet Resource Locator, 5-4

Windows 2000 domains

- administering external users and roles with Oracle Administration Assistant for Windows NT, 2-2
- role authorization, 3-2

Windows authentication protocols

- default protocol used, 1-3
- with Windows 2000, 1-2
- with Windows NT 4.0, 1-2

Windows native authentication

- benefits, 1-2
- enhancements, 1-4
- installation of, 1-2

- methods and use of, 1-2
- overview, 1-2
- role authorization enhancements, 1-4
- setting the sqlnet.ora file, 2-39, 2-41
- user and role requirements, 1-4
- user authentication enhancements, 1-4

Windows NT 4.0 domains

- administering external users and roles
 - manually, 2-30
- basic features, 1-4

Windows NT local groups

- with database privileges, 1-8, 2-42, 2-44

Windows NT-specific

- role syntax, 2-44