Contents

Send Us Your Comments ................................................................................................................... vii

Preface ................................................................................................................................................ ix
  Audience ........................................................................................................................................ x
  Organization ................................................................................................................................. x
  Related Documentation ............................................................................................................... xi
  Conventions ................................................................................................................................. xii
  Documentation Accessibility ...................................................................................................... xvii

What’s New in Network, Directory, and Security Features for Oracle9i ...................................... xix
  Oracle Public Key Infrastructure ................................................................................................. xx
  Active Directory Integration ...................................................................................................... xx
  Oracle Wallets ............................................................................................................................ xx
  Using Oracle9i on Windows 2000 ............................................................................................ xx
  Desupported and Deprecated Features .................................................................................... xxi

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 ...................................................................... 1-6
  Automatically Enabling Operating System Authentication During Installation ................ 1-8
2 Administering External Users and Roles

How to Administer External Users and Roles ................................................................. 2-2
Using Oracle Administration Assistant for Windows NT .................................................. 2-2
  Adding a Computer and Saving Your Configuration ...................................................... 2-5
  Granting Administrator and Operator Privileges for All Databases on a Computer .... 2-6
  Connecting to a Database ............................................................................................... 2-9
  Viewing Database Authentication Parameter Settings ................................................. 2-13
  Creating a Nonprivileged Database User (External User) .............................................. 2-14
  Creating a Local Database Role .................................................................................... 2-18
  Creating an External Role .............................................................................................. 2-20
  Granting Administrator and Operator Privileges for a Single Database ..................... 2-24
Manually Administering External Users and Roles .......................................................... 2-27
  Creating a Nonprivileged Database User (External User) ............................................ 2-28
  Granting Administrator and Operator Privileges for Databases .................................. 2-34
  Creating an External Role .............................................................................................. 2-38

3 Administering Enterprise Users and Roles

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

4 Using Oracle9i Directory Server Features with Active Directory

LDAP and Active Directory Overview ............................................................................. 4-2
  LDAP and a Directory Server ....................................................................................... 4-2
  Oracle Internet Directory ............................................................................................. 4-2
  Active Directory ........................................................................................................ 4-2
Oracle9i Directory Server Features ............................................................................... 4-3
  Directory Naming ....................................................................................................... 4-3
  Enterprise User Security ............................................................................................ 4-3
Integration with Active Directory .................................................................................. 4-5
  Automatic Discovery of Directory Servers ................................................................ 4-5
  Integration with Microsoft Tools ................................................................................ 4-6
  User Interface Extensions for Oracle Net Directory Naming ..................................... 4-7
  Enhancement of Directory Object Type Descriptions ............................................... 4-7
  Integration with Windows Login Credentials ......................................................... 4-8
Oracle Directory Objects in Active Directory ................................................................. 4-9

Requirements for Using Oracle9i with Active Directory .............................................. 4-11
  Oracle Schema Creation Requirements ................................................................. 4-12
  Oracle Context Creation Requirements .............................................................. 4-13
  Directory Naming Requirements ....................................................................... 4-13
  Enterprise User Security Requirements ........................................................... 4-15

Oracle9i Installation and Configuration with Active Directory ................................... 4-16
  Installation Tasks .................................................................................................... 4-16
  Post-Installation Configuration Tasks ................................................................. 4-16

Testing Connectivity .................................................................................................. 4-16
  Testing Connectivity from Client Computers ...................................................... 4-16
  Testing Connectivity from Microsoft Tools .......................................................... 4-17

Access Control List Management for Oracle Directory Objects .................................. 4-20
  Accessing the Security Groups ............................................................................. 4-21
  Adding or Removing Users .................................................................................... 4-23
  Changing User Permissions ................................................................................... 4-24

Creating Enterprise Domains ...................................................................................... 4-25

5  Storing Oracle Wallets in the Windows Registry

Storing Private Keys and Trustpoints ........................................................................... 5-2
Storing the User’s Profile .......................................................................................... 5-2
Storing Oracle Wallets in the Windows Registry ........................................................ 5-2
  Oracle Wallet Manager .......................................................................................... 5-3
Oracle Enterprise Login Assistant .......................................................................... 5-3
Wallet Resource Locator .......................................................................................... 5-4

6  Windows 2000 PKI Integration

Oracle Public Key Infrastructure ............................................................................... 6-2
Windows Public Key Infrastructure .......................................................................... 6-2
  Microsoft Certificate Stores .................................................................................. 6-2
  Microsoft Certificate Services ............................................................................... 6-3
  Wallet Resource Locator ........................................................................................ 6-3
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

  TCP/IP Support for Windows 95 ................................................................................ A-5

Glossary

Index
Send Us Your Comments

Part No. A90165-01

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:

- E-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. Contact information for Oracle Support Services is available at this Web site:

http://www.oracle.com/support/
This guide is your primary source of introductory, post-installation, configuration, and administration information for using Oracle9i network, directory, and security features for Windows operating systems.

This chapter contains these topics:

- **Audience**
- **Organization**
- **Related Documentation**
- **Conventions**
- **Documentation Accessibility**
Audience

This guide is necessary for anyone configuring or administering Oracle9i network, directory, and security features for Windows operating systems.

Organization

This guide is organized as follows:

**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, "Using Oracle9i Directory Server Features with Active Directory"**
This chapter describes the use of Oracle9i Directory Server Features with Active Directory.

**Chapter 5, "Storing Oracle Wallets in the Windows Registry"**
This chapter describes the storing and retrieving of Oracle Wallets in the Windows registry.

**Chapter 6, "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
- Oracle9i Database Error Messages

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://technet.oracle.com/membership/index.htm

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://technet.oracle.com/docs/index.htm
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.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.</td>
<td>The C datatypes such as <strong>ub4</strong>, <strong>sword</strong>, or <strong>OCINumber</strong> are valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you specify this clause, you create an index-organized table.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Italic typeface indicates book titles, emphasis, syntax clauses, or placeholders.</td>
<td><em>Oracle9i Database Concepts</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can specify the <em>parallel_clause</em>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Run <code>old_release.SQL</code> where <code>old_release</code> refers to the release you installed prior to upgrading.</td>
</tr>
<tr>
<td><strong>UPPERCASE monospace</strong></td>
<td>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.</td>
<td>You can specify this clause only for a <code>NUMBER</code> column.</td>
</tr>
<tr>
<td>(fixed-width font)</td>
<td></td>
<td>You can back up the database using the <code>BACKUP</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Query the <code>TABLE_NAME</code> column in the <code>USER_TABLES</code> data dictionary view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the <code>ROLLBACK_SEGMENTS</code> parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>DBMS_STATS.GENERATE_STATS</code> procedure.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>lowercase monospace (fixed-width font)</td>
<td>Lowercase monospace typeface indicates executables 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.</td>
<td>Enter sqlplus to open SQL*Plus.</td>
</tr>
<tr>
<td>{}</td>
<td>Braces enclose two or more items, one of which is required. Do not enter the braces.</td>
<td>{ENABLE</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td>[COMPRESS</td>
</tr>
<tr>
<td>...</td>
<td>Horizontal ellipsis points indicate either:</td>
<td>CREATE TABLE ... AS subquery;</td>
</tr>
<tr>
<td>-</td>
<td>That we have omitted parts of the code that are not directly related to the example</td>
<td>SELECT col1, col2, ..., coln FROM employees;</td>
</tr>
<tr>
<td>.</td>
<td>Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.</td>
<td>. . . .</td>
</tr>
</tbody>
</table>
The following table describes conventions for Windows operating systems and provides examples of their use.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Start &gt;</td>
<td>How to start a program. For example, to start Oracle Database Configuration Assistant, you must click the Start button on the taskbar and then choose Programs &gt; Oracle - HOME_NAME &gt; Configuration and Migration Tools &gt; Database Configuration Assistant.</td>
<td>Choose Start &gt; Programs &gt; Oracle - HOME_NAME &gt; Configuration and Migration Tools &gt; Database Configuration Assistant</td>
</tr>
<tr>
<td>File and Directory Names</td>
<td>File/directory names are not case sensitive. The special characters <code>&lt;</code>, <code>&gt;</code>, <code>;</code>, <code>,</code>, <code>/</code>, `</td>
<td><code>, and </code>-<code>are not allowed. The special character</code>` is treated as an element separator, even when it appears in quotes. If the file name begins with <code>\</code>, Windows assumes it uses the Universal Naming Convention.</td>
</tr>
<tr>
<td>Convention</td>
<td>Meaning</td>
<td>Example</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>C:&gt;</td>
<td>Represents the Windows command prompt of the current hard disk drive. The escape character in a command prompt is &quot;^&quot;. Your prompt reflects the subdirectory in which you are working. Referred to as the command prompt in this manual.</td>
<td>C:\oracle\oradata&gt;</td>
</tr>
<tr>
<td>HOME_NAME</td>
<td>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.</td>
<td>C:&gt; net start OracleHOME_NAME TNSListener</td>
</tr>
<tr>
<td></td>
<td>The backslash special character () is sometimes required as an escape character for the double quote (&quot;) special character at the Windows command prompt. Parentheses and the single quote special character (') do not require an escape character. See your Windows operating system documentation for more information on escape and special characters.</td>
<td>C:&gt; exp scott/tiger TABLES=emp QUERY=&quot;WHERE job='SALESMAN' and sal&lt;1600&quot;</td>
</tr>
<tr>
<td></td>
<td>C:&gt; imp SYSTEM/password FROMUSER=scott TABLES=(emp, dept)</td>
<td></td>
</tr>
</tbody>
</table>
In releases prior to Oracle8i release 8.1.3, when you installed Oracle components, all subdirectories were located under a top level `ORACLE_HOME` directory that by default was:

- `C:\orant` for Windows NT
- `C:\orawin95` for Windows 95
- `C:\orawin98` for Windows 98

or whatever you called your Oracle home.

This release complies with Optimal Flexible Architecture (OFA) guidelines. All subdirectories are not under a top level `ORACLE_HOME` directory. There is a top level directory called `ORACLE_BASE` that by default is `C:\oracle`. If you install Oracle9i Release 1 (9.0.1) on a computer with no other Oracle software installed, the default setting for the first Oracle home directory is `C:\oracle\ora90`. The Oracle home directory is located directly under `ORACLE_BASE`.

All directory path examples in this guide follow OFA conventions.

See Oracle9i Database Getting Started for Windows for additional information on OFA compliances and for information on installing Oracle products in non-OFA compliant directories.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ORACLE_HOME</code> and <code>ORACLE_BASE</code></td>
<td>In releases prior to Oracle8i release 8.1.3, when you installed Oracle components, all subdirectories were located under a top level <code>ORACLE_HOME</code> directory that by default was:</td>
<td>Go to the <code>ORACLE_BASE\ORACLE_HOME\rdbms\admin</code> directory.</td>
</tr>
</tbody>
</table>
Oracle’s goal is to make our products, services, and supporting documentation accessible to the disabled community with good usability. 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 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/

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.
What’s New in Network, Directory, and Security Features for Oracle9i

This section describes the new Oracle9i network, directory, and security features for Windows operating systems.

- Oracle Public Key Infrastructure
- Active Directory Integration
- Oracle Wallets
- Using Oracle9i on Windows 2000
- Desupported and Deprecated Features
Oracle Public Key Infrastructure

Oracle Public Key Infrastructure (PKI) is used by the Oracle Enterprise Security Manager, Lightweight Directory Access Protocol (LDAP)-enabled Enterprise Manager, Oracle’s Secure Socket Layer (SSL) authentication, and Oracle9i database.

Public Key Infrastructure is information security technology using public key cryptography. Public key cryptography involves encrypting and decrypting of information using a shared (public) and private key pair. Data that the private key encrypts, the public key decrypts, and data that the public key encrypts, the private key decrypts. Public key cryptography is the basis of PKI.

Using Oracle Advanced Security, Oracle offers a comprehensive set of tools in Oracle9i utilizing PKI technology.

Active Directory Integration

Active Directory enables users to access network resources with a single login. Active Directory is the LDAP-compliant directory server included with Windows 2000. Active Directory centrally stores all Windows 2000 information, including users, groups, and policies.

Oracle Wallets

Oracle Wallets in Oracle9i can be stored and retrieved from the Windows registry. Oracle Wallets store the private keys and trust points, and hold the digital certificates used in public key applications for authentication and encryption. The Oracle Wallet Manager tool creates and manages Oracle Wallets. Oracle Public Key applications use the decrypted Oracle Wallet for authentication and encryption.

Using Oracle9i on Windows 2000

There are some differences between using Oracle9i on Windows 2000 and Windows NT 4.0.

See Also: Oracle9i Database Getting Started for Windows
Desupported and Deprecated Features

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

CONNECT/AS SYSDBA
CONNECT username/password AS SYSDBA

Oracle Net Services (Net8) Desupported Features
The following Oracle Net Services (formerly Net8) features are not supported in Oracle9i:

- NDS External Naming and NDS Authentication
- protocol.ora file
- SPX protocol
- Identix and SecurID authentication methods
- Net8 OPEN
- TRCROUTE
- SPAWN command in the Listener Control utility
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**
- **Automatically Enabling Operating System Authentication During Installation**
Windows Native Authentication Overview

The Oracle9i database can use Windows user login credentials to authenticate database users. The 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 the 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 the Secure Socket 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 the authentication is set to NTS, on a standalone Windows 2000 or Windows NT 4.0 computer, ensure that the 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, 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, the Oracle9i database determines the protocol to use, completely transparent to the user. The only Oracle requirement is to ensure that `SQLNET.AUTHENTICATION_SERVICES` parameter contains `ntss` in the `ORACLE_BASE\ORACLE_HOME\network\admin\sqlnet.ora` file on both the client and database server (this is the default setting for both after installation). For Oracle8 8.0 releases, you must manually set this value.

An Oracle9i database network typically includes client computers and database servers. The 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 the Oracle software and Windows operating system releases required to enable Kerberos as the default authentication protocol:

<table>
<thead>
<tr>
<th>For The...</th>
<th>This Windows Software is Required...</th>
<th>This Oracle Software is Required...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Computer</td>
<td>■ Windows NT 4.0</td>
<td>■ Oracle8i Client or later</td>
</tr>
<tr>
<td></td>
<td>■ Windows 2000</td>
<td></td>
</tr>
<tr>
<td>Database Computer</td>
<td>■ Windows NT 4.0</td>
<td>■ Oracle8i database or later</td>
</tr>
<tr>
<td></td>
<td>■ Windows 2000</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>■ Windows 2000</td>
<td>■ None</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User authentication</td>
<td>The process by which the database uses the user’s Windows login credentials to authenticate the user.</td>
<td>Oracle9i Database Administrator’s Guide</td>
</tr>
<tr>
<td>Role authorization</td>
<td>The process of granting an assigned set of roles to authenticated users.</td>
<td>Oracle9i Database Administrator’s Guide</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication of external users</td>
<td>Users are authenticated by the database using the user’s Windows login credentials that enable them to access the Oracle database without being prompted for additional login credentials.</td>
</tr>
<tr>
<td>Authorization of external roles</td>
<td>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. The init.ora parameter OS_ROLES is set to false by default. You must set OS_ROLES to true to authorize external roles.</td>
</tr>
</tbody>
</table>

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 the `OSAUTH_X509_NAME` registry parameter to `true` on the computer on which the 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 the 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 the `OSAUTH_X509_NAME` registry parameter.

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>
<thead>
<tr>
<th>Use...</th>
<th>When...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise users and roles</td>
<td>You have many users connecting to multiple databases.</td>
</tr>
<tr>
<td></td>
<td>Enterprise users have the same identity across multiple databases.</td>
</tr>
<tr>
<td></td>
<td>Enterprise users require the use of a directory server.</td>
</tr>
<tr>
<td></td>
<td>Use enterprise roles in environments where enterprise users assigned to</td>
</tr>
<tr>
<td></td>
<td>these roles are located in many geographic regions and must access</td>
</tr>
<tr>
<td></td>
<td>multiple databases. Each enterprise role can be assigned to more than</td>
</tr>
<tr>
<td></td>
<td>one enterprise user in the directory. If you do not use enterprise roles,</td>
</tr>
<tr>
<td></td>
<td>then you have to assign database roles manually to each database user.</td>
</tr>
<tr>
<td></td>
<td>Enterprise roles require the use of a directory server.</td>
</tr>
<tr>
<td>External users and roles</td>
<td>You have a smaller number of users accessing a limited number of</td>
</tr>
<tr>
<td></td>
<td>databases. External users must be created individually in each database,</td>
</tr>
<tr>
<td></td>
<td>and do not require the use of a directory server.</td>
</tr>
<tr>
<td></td>
<td>External roles must also be created individually in each database, and do</td>
</tr>
<tr>
<td></td>
<td>not require the use of a directory server. External roles are authorized</td>
</tr>
<tr>
<td></td>
<td>using group membership of the users in the local groups on the system.</td>
</tr>
</tbody>
</table>
Oracle9i Integration with Active Directory

This integration enables you to take advantage of the user authentication and role authorization. Note that these enhancements are only available if you are running in a Windows 2000 domain. Perform the following tasks to integrate Oracle components with Active Directory.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Task 1: Install and Configure Components</td>
</tr>
<tr>
<td>2.</td>
<td>Task 2: Set the OSAUTH_X509_NAME Registry Parameter</td>
</tr>
<tr>
<td>3.</td>
<td>Task 3: Start and Use Oracle Enterprise Security Manager</td>
</tr>
</tbody>
</table>

Task 1: Install and Configure Components

Read Chapter 4, “Using Oracle9i Directory Server Features with Active Directory” and the Oracle9i Database installation guide for Windows for information on pre-installation and configuration issues.

Task 2: Set the OSAUTH_X509_NAME Registry Parameter

Set the OSAUTH_X509_NAME registry parameter to enable client users to access the Oracle9i database as X.509-compliant enterprise users. This parameter is required only if you want to use enterprise users and roles.

<table>
<thead>
<tr>
<th>Set This Parameter On...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Oracle9i database computer running in a Windows 2000 domain</td>
<td>When set to true, this parameter enables a client username to be identified as an X.509-compliant enterprise username when connecting to an Oracle9i database through Active Directory. A user’s role authorization is done using Active Directory. When set to false (the default setting), the client user is identified as an external user and a user’s role authorization is done using the Oracle9i database data dictionary.</td>
</tr>
</tbody>
</table>

To set the OSAUTH_X509_NAME registry parameter:

1. Go to the computer on which the Oracle9i database is installed.
2. Choose Start > Run.
3. Enter regedit32 in the Open field, and choose OK.
   The registry editor window appears.
4. Go to HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME ID.
   where ID is the Oracle home that you want to edit.
5. If the 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. Choose Enter.

7. Set the value to `true` in the String field.

8. Choose OK.

9. Choose Exit from the Registry menu.
   The registry editor exits.

**Task 3: Start and Use Oracle Enterprise Security Manager**

Use Oracle Enterprise Security Manager to create and manage enterprise users, roles, and domains, and assign enterprise users and groups to enterprise roles.

Oracle Enterprise Security Manager is included as an integrated application with Oracle Enterprise Manager. The subsequent procedures describe Windows-unique features for using Oracle Enterprise Security Manager in a Windows 2000 domain.

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

To use Oracle Enterprise Security Manager:


2. Use the online help and instructions in Oracle Advanced Security Administrator’s Guide to use this tool.

3. Review the following issues for using Active Directory.
   
   - The administrator using Oracle Enterprise Security Manager must be a member of the security group `OracleDBSecurityAdmin`. By default, the administrator who created the Oracle Context (that is, configured the 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 manually add additional users, see "Access Control List Management for Oracle Directory Objects" on page 4-20 for information.
Automatically Enabling Operating System Authentication During Installation

Select Login from the Directory Server main menu to access a dialog box for selecting the authentication protocol appropriate to your environment:

<table>
<thead>
<tr>
<th>Select...</th>
<th>If...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT Native</td>
<td>Running an Oracle9i database on a Windows NT 4.0 or Windows 2000 computer in a Windows 2000 domain with Active Directory.</td>
</tr>
<tr>
<td>Simple Authentication</td>
<td>The other available selections do not work. Simple authentication can be used with either Oracle Internet Directory or Active Directory, but is also less secure.</td>
</tr>
</tbody>
</table>

Automatically Enabling Operating System Authentication During Installation

When you install the Oracle9i database, your Windows username is automatically added to a Windows NT local group called ORA_DBA. The ORA_DBA local group is:

- Automatically created when the Oracle9i database is installed.
- A special Windows NT local group whose members automatically receive the SYSDBA privilege.

This enables you to:

- Connect to any local Oracle9i databases without a password by issuing commands such as the following:
  ```
  CONNECT / AS SYSDBA
  ```
- Connect to remote Oracle9i databases without a password by issuing a command such as the following:
  ```
  CONNECT /@net_service_name AS SYSDBA
  ```
  where `net_service_name` is the net service name of the Oracle9i database to which to connect.
- Perform local or remote 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, provided you have Administrator privileges
This chapter describes the administration of external users and roles.

This chapter contains these topics:

- How to Administer External Users and Roles
- Using Oracle Administration Assistant for Windows NT
- Manually Administering External Users and Roles
How to Administer External Users and Roles

There are two methods for administering external users and roles:

- Using Oracle Administration Assistant for Windows NT
- Manually Administering External Users and Roles

---

**Note:** Both methods can also administer external users and roles in Windows 2000 domains, but cannot be used to administer enterprise users and roles. See "Administering Enterprise Users and Roles" on page 3-1 for more information on tools available for administrating enterprise users and roles.

---

Using Oracle Administration Assistant for Windows NT

Oracle Administration Assistant for Windows NT runs from the Microsoft Management Console and enables you to configure the following Oracle database users and roles to be authenticated by the Windows operating system:

- Configure regular Windows NT domain users and global groups as external users to access the Oracle database without a password.
- Configure Windows NT database administrators (with the `SYSDBA` privilege) to access the Oracle database without a password.
- Configure Windows NT database operators (with the `SYSOPER` privilege) to access the Oracle database without a password.
- Create and grant local and external database roles to Windows NT domain users and global groups.

Oracle Administration Assistant for Windows NT eliminates the need to 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 the `CREATE USER username IDENTIFIED EXTERNALLY` syntax.
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 and Operator Privileges for All Databases on a Computer
- Connecting to a Database
- Viewing Database Authentication Parameter Settings
- Creating a Nonprivileged Database User (External User)
- Creating a Local Database Role
- Creating an External Role
- Granting Administrator and Operator Privileges for a Single Database

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

- Install the Microsoft Windows NT 4.0 Option Pack, which includes the Microsoft Management Console
- Download the Microsoft Management Console from the Microsoft Web site:
  
  http://www.microsoft.com
Note: 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 the database with the domain name as the prefix. Therefore, if you are managing Oracle7.x or later databases remotely, you must set the registry value `OSAUTH_PREFIX_DOMAIN` in `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME\HOMEID` to `true` on the remote computer. 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, for example, 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 in the 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.
   The Microsoft Management Console starts.

2. Double-click Oracle Managed Objects.
   The Computer icon appears.

3. Right-click Computers.

   The Add Computer dialog box appears.

5. Specify the domain and hostname of the computer on which your Oracle database is installed.

6. Choose 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:

<table>
<thead>
<tr>
<th>This Node...</th>
<th>Enables You To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Database Administrators - Computer</td>
<td>Create an operating system-authenticated database administrator (with SYSDBA privileges) for all database instances on the computer.</td>
</tr>
<tr>
<td>OS Database Operators - Computer</td>
<td>Create an operating system-authenticated database operator (with SYSOPER privileges) for all database instances on the computer.</td>
</tr>
</tbody>
</table>

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.

10. See “Granting Administrator and Operator Privileges for All Databases on a Computer” on page 2-6.

**Granting Administrator and Operator Privileges for All Databases on a Computer**

You can grant database administrator (SYSDBA) and database operator (SYSOPER) privileges to DBAs for all databases on a computer.

To grant privileges 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. Make an appropriate selection:

<table>
<thead>
<tr>
<th>If You Want to Grant...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database administrator</td>
<td>1. Right-click OS Database Administrators - Computer.</td>
</tr>
<tr>
<td>(SYSDBA) privileges</td>
<td>2. See section “Granting Administrator Privileges for All Databases on a Computer” on page 2-7</td>
</tr>
<tr>
<td>Database operator</td>
<td>1. Right-click OS Database Operators - Computer.</td>
</tr>
<tr>
<td>(SYSOPER) privileges</td>
<td>2. See section “Granting Operator Privileges For All Databases on a Computer” on page 2-8</td>
</tr>
</tbody>
</table>
Granting Administrator Privileges for All Databases on a Computer

To grant administrator (SYSDBA) privileges for all databases on a computer:

1. Choose Add/Remove.

   The OS Database Administrators - Computer for hostname dialog box appears:

   2. Select the domain of the user to which to grant SYSDBA privileges from the Domain drop-down list box.

   3. Select the user.

   4. Choose Add.

      The user now appears in the OS Database Administrators - Computer window.

   5. Choose OK.
Granting Operator Privileges For All Databases on a Computer

To grant operator (SYSOPER) privileges for all databases on a computer:

1. Choose Add/Remove.

The OS Database Operators - Computer for `hostname` dialog box appears:

2. Select the domain of the user to which to grant SYSOPER privileges from the Domain drop-down list box.

3. Select the user.

4. Choose Add.

The user now appears in the OS Database Operators - Computer window.

5. Choose OK.
Connecting to a Database

Once you connect to a database, you can perform additional authentication tasks:

- Viewing Database Authentication Parameter Settings
- Creating a Nonprivileged Database User (External User)
- Creating a Local Database Role
- Creating an External Role
- Granting Administrator and Operator Privileges for a Single Database

To connect to a database:

1. Right-click the database instance to access (for example, ORCL) in the Microsoft Management Console scope pane:
To enable Secure Sockets Layer (SSL) when connecting to an Oracle database, do not use the default user account in the Windows NT Services dialog box when starting the Oracle service and the listener service. Start these services in the same user account as the wallet created in Oracle Wallet Manager. If the Oracle service and the listener service are started in the default user accounts, 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

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.

<table>
<thead>
<tr>
<th>This Node...</th>
<th>Enables You To...</th>
<th>For More Information...</th>
</tr>
</thead>
<tbody>
<tr>
<td>External OS Users</td>
<td>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 (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) privileges.</td>
<td>See “Creating a Nonprivileged Database User (External User)” on page 2-14</td>
</tr>
<tr>
<td>Local Roles</td>
<td>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.</td>
<td>See “Creating a Local Database Role” on page 2-18</td>
</tr>
<tr>
<td>External OS Roles</td>
<td>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.</td>
<td>See “Creating an External Role” on page 2-20</td>
</tr>
</tbody>
</table>
Troubleshooting Connection Problems

When connecting to a local computer, Oracle Administration Assistant for Windows NT first tries to connect as a SYSDBA to the database using the Bequeath networking protocol. When connecting to a remote computer, Oracle Administration Assistant for Windows NT tries to connect using Windows native authentication as a SYSDBA to the database using the TCP/IP networking protocol (port 1521 or the deprecated 1526). If it is unsuccessful, the dialog boxes shown in Table 2–1 appear and prompt you to enter information to connect to the database:

<table>
<thead>
<tr>
<th>This Node...</th>
<th>Enables You To...</th>
<th>For More Information...</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Database Administrators</td>
<td>Authenticate a Windows NT user with SYSDBA privileges for a specific instance on a computer.</td>
<td>See &quot;Granting Administrator and Operator Privileges for a Single Database&quot; on page 2-24</td>
</tr>
<tr>
<td>OS Database Operators</td>
<td>Authenticate a Windows NT user with SYSOPER privileges for a specific instance on a computer.</td>
<td>See &quot;Granting Administrator and Operator Privileges for a Single Database&quot; on page 2-24</td>
</tr>
</tbody>
</table>
### Table 2–1 Resolving Database Connection Problems

<table>
<thead>
<tr>
<th>This Dialog Box Appears...</th>
<th>Because...</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 box again, configure your domain user to be a database administrator authenticated by the Windows NT operating system.</td>
<td></td>
</tr>
</tbody>
</table>

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 change to the TCP/IP protocol and make sure the Oracle Net Services listener is for the database 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.
Viewing Database Authentication Parameter Settings

To view database authentication parameter settings:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS_AUTHENT_PREFIX</td>
<td>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 (&quot;&quot;&quot;) during Oracle9i database creation. Create Oracle users in the database without the prefix OPS$, which was needed for Oracle7 and Oracle8 release 8.0.x. Therefore, a Windows domain username of frank is authenticated as username frank. You can set this parameter to an appropriate value. For example, if you set this parameter to xyz, the Windows NT domain user frank is authenticated as user xyzfrank.</td>
</tr>
<tr>
<td>OS_ROLES</td>
<td>OS_ROLES is an init.ora file parameter that, if set to true, enables the Windows NT operating system to manage the authorization of external roles for database users. 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 the granting and revoking of roles for database users. See section &quot;Understanding the OS_ROLES Parameter&quot; on page 2-13 for more information.</td>
</tr>
</tbody>
</table>

Understanding the OS_ROLES Parameter

OS_ROLES is a parameter in the init.ora file that, if set to true, enables the Windows NT operating system to manage the authorization of external roles for database users. 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 the 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, 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, and 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 the roles through Windows NT. See "Creating a Local Database Role" on page 2-18 and "Creating an External Role" on page 2-20 for more information.

**Creating a Nonprivileged Database User (External User)**

You can create a nonprivileged database user (external user).

To create a nonprivileged database user:

1. Follow the steps in "Connecting to a Database" on page 2-9 to connect to a database.
2. Right-click External OS Users.
3. Choose Create.
The Create External OS User Wizard starts:

4. 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. Choose Add.

The user now appears in the New External OS Users window.

**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.
7. Choose Next.

8. 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. Double-click the tablespace to assign a tablespace quota in the Tablespace Quota window. This assigns profile and tablespace information to the users, and grants database roles.

10. Choose Next.
11. Select the database roles to grant to the new external users.

12. Choose the Grant button.


14. Right-click the external user for which you want to view information and select Properties.

   The assigned properties appear.
Creating a Local Database Role

You can create a local database role.

To create a local database role:

1. Follow the steps in "Connecting to a Database" on page 2-9 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.

The Create Local Role wizard appears:

4. Enter a local role name to use. A local role is a role that is managed by the Oracle database.

5. Select None if you want a user to use this local role without being required to enter a password.

6. Select Password if you want the 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.

7. Enter the password to use with this role.
8. Confirm the password by entering it a second time.

9. Choose Next.

10. Select appropriate system privileges to assign to the local role.

11. Choose 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.

12. If you want to grant the Admin Option to this role, click the value in the Admin Option column to display a drop-down list box. This enables you to select Yes.

13. Choose Next.
14. Select appropriate roles to assign to the local role. Both local roles and external roles appear in this list.

15. Choose 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.


Creating an External Role

You can create external roles.

To create an external role:

1. Follow the steps in "Connecting to a Database" on page 2-9 to connect to a database.

2. Right-click External OS Roles for the database for which to create an external role.

3. Choose Create.
4. Enter an external role name to use. An external role is a role that is managed by the Windows operating system.

5. Choose Next.
6. Select appropriate system privileges 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 the Admin Option to this role, choose the value in the Admin Option column to display a drop-down list box. This enables you to select Yes.
10. Choose Next.
11. Select appropriate roles to assign to the external role.

12. Choose Grant to grant the selected roles to the external role. Both local roles and external roles appear in this list.

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

Granting Administrator and Operator Privileges for a Single Database

You can grant database administrator (SYSDBA) and database operator (SYSOPER) privileges to database administrators for a single database on a computer.

To grant privileges for a single database:

1. Follow the steps in "Connecting to a Database" on page 2-9 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. Make an appropriate selection:

<table>
<thead>
<tr>
<th>If You Want to Grant...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| Database administrator (SYSDBA) privileges | 1. Right-click OS Database Administrators.  
2. Follow the steps 1-4 above. |
| Database operator (SYSOPER) privileges | 1. Right-click OS Database Operators.  
2. See section “Granting Operator Privileges for a Single Database” on page 2-26 |
Granting Administrator Privileges for a Single Database

To grant administrator (SYSDBA) privileges for a single database:

1. Choose Add/Remove.

   The OS Database Administrators for instance dialog box (MARK in this example) appears:

   ![Image of OS Database Administrators dialog box]

2. Select the domain of the user to which to grant SYSDBA privileges from the NT Domain Users and Groups drop-down list box.

3. Select the user. The user now appears in the OS Database Administrators window.

4. Choose OK.
Granting Operator Privileges for a Single Database

To grant operator (SYSOPER) privileges for a single database:

1. Choose Add/Remove.

   The OS Database Operators for instance dialog box (mark in this example) appears:

   ![OS Database Operators for MARK dialog box](image)

   - NT Domain Users and Groups
     - Name: Domain
     - Description:
     - Add
     - Remove

2. Select the domain of the user to which to grant SYSOPER privileges from the NT Domain Users and Groups drop-down list box.

3. Select the user.

4. Choose Add.

   The user now appears in the OS Database Operators window.

5. Choose OK.
Manually Administering External Users and Roles

Manual configuration involves using Oracle command line tools, editing the registry, and creating local groups in Windows NT User Manager. This enables you to:

- Configure nonprivileged Windows NT users (external users) to access the Oracle database without a password.
- Configure Windows NT database administrators (with the SYSDBA privilege) to access the Oracle database without a password.
- Configure Windows NT database operators (with the SYSOPER privilege) to access the Oracle database without a password.
- Create and grant local and external database roles to Windows NT domain users and global groups.

This section describes:

- Creating a Nonprivileged Database User (External User)
- Granting Administrator and Operator Privileges for Databases
- Creating an External Role

**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.
Creating a Nonprivileged Database User (External User)

This section describes how to authenticate nonprivileged database users (nondatabase administrators) using Windows NT so that a password is not required when accessing the database. See Table 2–2. When you use Windows NT to authenticate nonprivileged database users, your database relies solely on Windows NT to restrict access to database usernames. In the steps below, the following Windows NT usernames are authenticated:

<table>
<thead>
<tr>
<th>Username</th>
<th>This User...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local user frank</td>
<td>Logs into their local Windows NT client computer to access an Oracle9i database. The database 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.</td>
</tr>
<tr>
<td>Domain user frank on domain sales</td>
<td>Logs into a domain (sales in the steps below) 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.</td>
</tr>
</tbody>
</table>

The local and domain username frank and the domain sales are used in the steps. Substitute the appropriate local and domain username and domain name for your environment.

Follow the subsequent steps to connect without a password as a nonprivileged database user:

- Task 1: Perform Authentication Tasks on the Oracle9i Database Server
- Task 2: Perform Authentication Tasks on the Client Computer

**Task 1: Perform Authentication Tasks on the Oracle9i Database Server**

To perform authentication tasks on an Oracle9i database server:

1. Add the OS_AUTHENT_PREFIX parameter 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 the Oracle usernames in the database when a connection request is attempted. Using the OS_AUTHENT_PREFIX parameter with Windows native authentication methods is the
recommended method for performing secure, trusted client connections to your server.

2. Set `OS_AUTHENT_PREFIX` to an appropriate value. Values are case insensitive. For example:

<table>
<thead>
<tr>
<th>Set <code>OS_AUTHENT_PREFIX</code> to...</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>xyz</code></td>
<td><code>xyz</code> is prefixed to the beginning of the Windows NT username (for example, <code>xyzfrank</code> for local user <code>frank</code> or <code>xyzsales\frank</code> for domain user <code>frank</code> on domain <code>sales</code>).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> <code>xyz</code> is only an example of an acceptable parameter value. Use a value appropriate to your environment.</td>
</tr>
<tr>
<td><code>''</code></td>
<td>This is recommended, as it eliminates the need for any prefix to the Windows NT usernames (for example, <code>frank</code> for local user <code>frank</code> or <code>sales\frank</code> for domain user <code>frank</code> on domain <code>sales</code>).</td>
</tr>
<tr>
<td>Not included in <code>init.ora</code> file</td>
<td>The value defaults to <code>OPS$</code> (for example, <code>OPS$FRANK</code> for local user <code>frank</code> or <code>OPS$sales\frank</code> for domain user <code>frank</code> on domain <code>sales</code>).</td>
</tr>
</tbody>
</table>

The parameter value `xyz` is used in the subsequent steps. Substitute `xyz` with the value you set for `OS_AUTHENT_PREFIX`.

3. Use User Manager to create a Windows NT local or domain username for `frank` (if the appropriate name does not currently exist). See your Windows NT documentation or your network administrator if you do not know how to do this.

4. Follow these substeps to create a new registry parameter *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 the registry editor from the MS-DOS command prompt:
   
   ```
   C:\> regedit 32
   ```

   b. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME ID`, where `ID` is the Oracle home directory you want to edit.

   c. Choose the Add Value option in the Edit menu.
The Add Value dialog box appears:

![Add Value dialog box](image)

**d.** Enter `OSAUTH_PREFIX_DOMAIN` in the Value Name field.

**e.** Choose `REG_EXPAND_SZ` from the Data Type drop-down list box.

**f.** Choose OK.

The String Editor dialog box appears:

![String Editor dialog box](image)

**g.** Enter `true` in the String field to enable authentication at the domain level.

`true` enables the server to differentiate between multiple `frank` usernames, whether they are local user `frank`, domain user `frank` on `sales`, or domain user `frank` on another domain in your network. 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.** Choose OK.

The Registry Editor adds the parameter.

**i.** Choose Exit from the registry menu.

The String Editor exits.

5. **Ensure that the `SQLNET.AUTHENTICATION_SERVICES` parameter in the `sqlnet.ora` file 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 an operating system-authenticated user by entering the following:

<table>
<thead>
<tr>
<th>If Authenticating a...</th>
<th>Then Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local username</td>
<td><code>SQL&gt; CREATE USER xyzfrank IDENTIFIED EXTERNALLY;</code></td>
</tr>
<tr>
<td>Domain username</td>
<td><code>SQL&gt; CREATE USER &quot;XYZSALES\FRANK&quot; IDENTIFIED EXTERNALLY;</code></td>
</tr>
</tbody>
</table>

   Where: Is the...
   | xyz                      | Value set for the `OS_AUTHENT_PREFIX` initialization parameter. |
   | frank                    | Windows NT local username. |
   | SALES\FRANK             | Domain name and Windows NT domain username. The double quotes are required and the entire syntax must be in uppercase. |

9. Grant the Windows NT local user `frank` or domain user `frank` appropriate database roles:

<table>
<thead>
<tr>
<th>If Authenticating a...</th>
<th>Then Enter...</th>
</tr>
</thead>
</table>
   | Local username         | `SQL> GRANT RESOURCE TO xyzfrank;`  
   |                        | `SQL> GRANT CONNECT TO xyzfrank;` |
   | Domain username        | `SQL> GRANT RESOURCE TO "XYZSALES\FRANK";`  
   |                        | `SQL> GRANT CONNECT TO "XYZSALES\FRANK";` |

1 Enter the syntax for domain users in uppercase and with double quotes around the domain username.

10. Connect to the database with the `SYSDBA` name:
    `SQL> CONNECT /AS SYSDBA`
11. Shut down the database:
   SQL> SHUTDOWN

12. Restart the database:
   SQL> STARTUP

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

**Task 2: Perform Authentication Tasks on the Client Computer**

To perform 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 the SQLNET.AUTHENTICATION_SERVICES parameter in the sqlnet.ora file 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 the Oracle9i database.

   The 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 the Oracle9i database as local or domain user \textit{frank} by viewing the roles assigned in step 5 of “Task 2: Perform Authentication Tasks on the Client Computer”.

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

which outputs for local user \textit{frank}:

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>GRANTED_ROLE</th>
<th>ADM</th>
<th>DEF</th>
<th>OS_</th>
</tr>
</thead>
<tbody>
<tr>
<td>XYZFRANK</td>
<td>CONNECT</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>XYZFRANK</td>
<td>RESOURCE</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

2 rows selected.

or, for domain user \textit{frank}:

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>GRANTED_ROLE</th>
<th>ADM</th>
<th>DEF</th>
<th>OS_</th>
</tr>
</thead>
<tbody>
<tr>
<td>XYZSALES\FRANK</td>
<td>CONNECT</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>XYZSALES\FRANK</td>
<td>RESOURCE</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

2 rows selected.

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

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

\textbf{Note:} Automatic authorization is supported for all Oracle Net protocols.
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. This enables database administrators to issue the following commands from a client computer and connect to the 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 client must belong to one of the following four Windows NT local groups on the server. See Table 2–3.

**Table 2–3 Windows NT Local Groups**

<table>
<thead>
<tr>
<th>Local Group</th>
<th>This Local Group Includes All...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA_OPER</td>
<td>SYSOPER database privileges; applicable for all databases on a computer.</td>
</tr>
<tr>
<td>ORA_DBA ¹</td>
<td>SYSDBA database privileges; applicable for all databases on a computer.</td>
</tr>
<tr>
<td>ORA_SID_DBA</td>
<td>SYSDBA database privileges; applicable only for a single database on a computer (identified by the SID).</td>
</tr>
<tr>
<td>ORA_SID_OPER</td>
<td>SYSOPER database privileges; applicable only for a single database on a computer (identified by the SID).</td>
</tr>
</tbody>
</table>

¹ ORA_DBA is automatically created during installation. See section "Automatically Enabling Operating System Authentication During Installation" on page 1-8 for information.

The SYSOPER and SYSDBA privileges are mapped to the following Windows NT local groups. See Table 2–4.

**Table 2–4 SYSOPER and SYSDBA Privileges**

<table>
<thead>
<tr>
<th>This Privilege...</th>
<th>Maps to the Local Group...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSOPER</td>
<td>ORA_SID_OPER, ORA_OPER</td>
</tr>
<tr>
<td>SYSDBA</td>
<td>ORA_SID_DBA, ORA_DBA, ORA_SID_OPER, ORA_OPER</td>
</tr>
</tbody>
</table>
Follow these steps to connect as SYSOPER or SYSDBA without a password:

- Task 1: Perform Authentication Tasks on the Oracle9i Database Server
- Task 2: Perform Authentication Tasks on the Client Computer

**Task 1: Perform Authentication Tasks on the Oracle9i Database Server**

To perform 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 box appears.
3. Enter the appropriate Windows NT local group name in the Group Name field. For this example, the SID entered is ORCL.
4. Choose Add.
The Add Users and Groups dialog box appears:

5. Select an appropriate Windows NT user from the Names field and choose Add.
6. Choose OK.

Your selection is added to the Members field of the New Local Group dialog box:
7. Choose OK.
8. Exit User Manager.
9. Ensure that the `SQLNET.AUTHENTICATION_SERVICES` parameter in the `sqlnet.ora` file contains `nts`.
10. Start the registry edit from the command prompt: `C:\>regedt32`
11. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME.ID`.
12. Set the parameter `OSAUTH_PREFIX_DOMAIN` to `true` where `ID` is the Oracle home that you want to edit.

**Task 2: Perform Authentication Tasks on the Client Computer**

To perform 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 the `SQLNET.AUTHENTICATION_SERVICES` parameter in the `sqlnet.ora` file 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 the Oracle9i database:

   ```sql
   > SET INSTANCE net_service_name
   
   where `net_service_name` is the Oracle Net network service name for the Oracle9i database.
   ```
6. Connect as SYSOPER or SYSDBA based on the local group you specified in step 3 of "Task 1: Perform Authentication Tasks on the Oracle9i Database Server":

<table>
<thead>
<tr>
<th>If The Local Group Is...</th>
<th>Then Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA_DBA or ORA_SID_DBA</td>
<td>SQL&gt; CONNECT / AS SYSOPER or SQL&gt; CONNECT / AS SYSDBA</td>
</tr>
<tr>
<td>ORA_OPER or ORA_SID_OPER</td>
<td>SQL&gt; CONNECT / AS SYSOPER</td>
</tr>
</tbody>
</table>

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

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. For example see Table 2–5:

<table>
<thead>
<tr>
<th>Table 2–5 External Roles and Oracle Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>If You...</td>
</tr>
<tr>
<td>1. Enable external roles.</td>
</tr>
<tr>
<td>2. Log onto a Windows NT domain with your domain username; for example, sales\frank, where sales is the domain name and frank is the domain username.</td>
</tr>
<tr>
<td>3. Connect to the Oracle9i database as Oracle database user scott.</td>
</tr>
</tbody>
</table>

Follow the subsequent tasks to grant external roles with Windows NT:

- **Task 1: Perform Authentication Tasks on the Oracle9i Database Server**
- **Task 2: Perform Authentication Tasks on the Client Computer**

**Task 1: Perform Authentication Tasks on the Oracle9i Database Server**

To perform authentication tasks on the Oracle9i database server:

1. Add the `OS_ROLES` initialization parameter to the `init.ora` file.
2. Set `OS_ROLES` to `true`.
   The default setting for this parameter is `false`.
3. Ensure that the `SQLNET.AUTHENTICATION_SERVICES` parameter in the `sqlnet.ora` file 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:
   ```
   SQL> CREATE ROLE DBSALES3 IDENTIFIED EXTERNALLY;
   ```
   where `DBSALES3` is the name of the role for these steps. Substitute a role name appropriate to your database environment.
7. Grant Oracle roles to `DBSALES3` that 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 with the `SYSDBA` name:
   ```
   SQL> CONNECT / AS SYSDBA
   ```
9. Shut down the database:
   ```
   SQL> SHUTDOWN
   ```
10. Restart the database:
    ```
    SQL> STARTUP
    ```
11. Open the Windows NT User Manager.

12. Choose New Local Group from the User menu.

The New Local Group dialog box 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` Indicates the database instance.
   - `rolename` Identifies the database role granted to users of a database session.
   - `D` Optional character indicating that this database role is to be the default role of the database user. If specified, this character must be preceded by an underscore.
   - `A` Optional character indicating that this database role includes the ADMIN OPTION. This enables the user to grant the role to other roles only. If specified, this character must be preceded by an underscore.

   For this example, `ORA_orcl_dbsales3_D` is entered.

The Add Users and Groups dialog box appears:

15. Select the appropriate Windows NT local or domain username and choose Add.
16. Choose OK.

Your selection is added to the Members field of the New Local Group dialog box:
You can convert additional database roles to several possible Windows NT groups, as shown in the following table. Then, users connecting to the ORCL instance in this example and authenticated by Windows NT as members of these Windows NT local groups have the privileges associated with dbsales3 and dbsales4 by default (because of the _D option). DBSALES1 and dbsales2 are available for use by the user if they first connect as members of dbsales3 or dbsales4 and use the SET ROLE command. If a user tries to connect with dbsales1 or dbsales2 without first connecting with a default role, they are unable to connect. Additionally, users can grant dbsales2 and dbsales4 to other roles.

<table>
<thead>
<tr>
<th>Database Roles</th>
<th>Windows NT Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbsales1</td>
<td>ORA_ORCL_dbsales1</td>
</tr>
<tr>
<td>dbsales2</td>
<td>ORA_ORCL_dbsales2_a</td>
</tr>
<tr>
<td>dbsales3</td>
<td>ORA_ORCL_dbsales3_d</td>
</tr>
<tr>
<td>dbsales4</td>
<td>ORA_ORCL_dbsales4_da</td>
</tr>
</tbody>
</table>

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

17. Choose OK.
18. Exit User Manager.

**Task 2: Perform Authentication Tasks on the Client Computer**

To perform 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 the `SQLNET.AUTHENTICATION_SERVICES` parameter in the `sqlnet.ora` file 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 that you created in Step 3.

6. Connect to the Oracle9i database:
   SQL> CONNECT scott/tiger AS SYSDBA

You are connected to the Windows NT server over net service with the Oracle username scott/tiger. The roles applied to the Oracle username scott consist of all roles defined for the Windows NT username that were mapped to the database roles above (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 the generic names for the 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. The Windows NT-specific names for OSDBA and OSOPER are described in "Granting Administrator and Operator Privileges for Databases" on page 2-34. See Oracle9i Database Administrator’s Guide for more information on OSDBA and OSOPER.
Manually Administering External 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 the Oracle Enterprise Manager Console. See the 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 external users and roles in Windows 2000 domains, but you cannot use Oracle Enterprise Security Manager to perform this administration. See “How to Administer External Users and Roles” on page 2-2 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 do not need their own schemas in the database; they typically need to access only application schemas in a database. This is especially critical in an Internet environment, where a number of users access the same application and there is no need to create schemas for each of these users.

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.

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

Enterprise user authentication is enabled, if you:

- Set the OSAUTH_X509_NAME registry parameter to true. (See "Oracle9i Integration with Active Directory" on page 1-6 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 the Oracle Enterprise Security Manager to map enterprise users to the shared schema.

The Kerberos authentication protocol is used if the Windows and Oracle releases match those listed in the table in "Windows Authentication Protocols" on page 1-2. Otherwise, NTLM is used.
Enterprise Role Authorization

Enterprise Users are assigned one or more enterprise roles. Authorization of enterprise roles 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 is a role that must be created individually in each Oracle9i database.

For example, an enterprise user can be assigned the enterprise role HR, which contains the global role HR user in the human resources database, and the global role employee in the corporate information database. If a user changes jobs, his enterprise role assignment is only changed in the directory, altering his privileges in multiple databases throughout the enterprise. Also, an administrator can add capabilities to enterprise roles or remove privileges from the enterprise role without having to update each users’ 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.

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

Users can belong to Windows 2000 global 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 the OS.Roles initialization file parameter to true (the method for enabling external role authorization).
Using Oracle9i Directory Server Features with Active Directory

This chapter describes the use of Oracle9i Directory Server Features with Active Directory.

This chapter contains these topics:

- 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
LDAP and Active Directory Overview

This section provides an overview of the following topics:

- LDAP and a Directory Server
- Oracle Internet Directory
- Active Directory

LDAP and a Directory Server

The Lightweight Directory Access Protocol (LDAP) is a standard, extensible directory access protocol that enables directory clients and servers to interact using a common language. LDAP is a lightweight implementation of the X.500 Directory Access Protocol (DAP). LDAP runs directly over TCP/IP.

Oracle Internet Directory

Oracle Internet Directory provides data management tools, such as Oracle Directory Manager and command line tools, for manipulating large amounts of LDAP data. Oracle Internet Directory implements three levels of user authentication, namely, anonymous, password-based, and certificate-based using Secure Socket Layer (SSL) for authenticated access and data privacy.

Active Directory

Active Directory is the LDAP-compliant directory server included with Windows 2000. Active Directory stores all Windows 2000 information, including users, groups, and policies. Active Directory also stores information about network resources such as databases, and makes this information available to application users and network administrators. Active Directory enables users to access network resources with a single login. The scope of Active Directory can range from storing all the resources of a small computer network to storing all the resources of several wide areas networks (WANs). When using Oracle features that support Active Directory using LDAP, ensure that the Active Directory computer can be successfully reached using all of the TCP/IP hostname forms possible to reach the domain controller. For example, if the hostname of the domain controller is server1 in the domain acme.com, then you can ping that computer using:

server1.acme.com acme.com and server1

Active Directory often issues referrals back to itself in one or more of these forms, depending upon the operation being performed. If all of the forms cannot be used to reach the Active Directory computer, then some LDAP operations may fail.
Oracle9i Directory Server Features

Two features are provided which make use of a directory server. These features are briefly described in the following sections:

- Directory Naming
- Enterprise User Security

Both features have been enabled to work with Microsoft’s Active Directory.

Directory Naming

This feature enables clients to connect to the database server making use of information stored centrally in an LDAP-compliant directory server such as Active Directory. For example, net service names previously stored in the tnsnames.ora file can now be stored in Active Directory.

Note: Database service and net service name entries stored in an Oracle Names Server can be migrated to a directory server using the Oracle Names Server Control utility. See Oracle9i Net Services Administrator’s Guide for more information.

Enterprise User Security

This feature enables you to create and store Oracle9i database information as directory objects in an LDAP-compliant directory server. An administrator can create and store enterprise users and roles for the Oracle9i database in the directory, which helps centralize the administration of users and roles across multiple databases.

This chapter frequently references enterprise user security terms and concepts. Read the following documentation in Table 4-1 for descriptions of terms and concepts that an administrator and client user must understand before using an Oracle9i database with Active Directory. You must license Oracle Advanced Security to use Active Directory to manage enterprise roles.
### Table 4-1 Descriptions of Terms and Concepts

<table>
<thead>
<tr>
<th>See...</th>
<th>Which Describes...</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Managing Enterprise User Security&quot; in Oracle Advanced Security...</td>
<td>■ Enterprise user security and management</td>
</tr>
<tr>
<td>Administrator’s Guide</td>
<td>■ Descriptions of enterprise users, roles, domains, and concepts</td>
</tr>
<tr>
<td></td>
<td>■ Location for enterprise user security entries in a directory server</td>
</tr>
<tr>
<td></td>
<td>■ Installing and configuring enterprise user security</td>
</tr>
<tr>
<td>&quot;Using Oracle Enterprise Security Manager&quot; in Oracle Advanced Security</td>
<td>■ Creating and managing enterprise users, roles, and domains</td>
</tr>
<tr>
<td>Administrator’s Guide</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Oracle Enterprise Security Manager cannot create or delete Windows 2000, Windows NT, Windows 95, or Windows 98 operating system usernames. Instead, Oracle Enterprise Security Manager creates a contact name in Active Directory. You cannot log in with a contact name; it is just defined for external purposes. You can then assign roles to this "user."

**Note:** Enterprise domains are directory constructs consisting of Oracle9i databases and enterprise users and roles. Enterprise domains are different from Windows 2000 domains, which are a collection of computers that share a common directory database.
Integration with Active Directory

In addition to Oracle Net directory naming and enterprise user security integration with a directory server, the following features have been specifically integrated into Active Directory:

- Automatic Discovery of Directory Servers
- Integration with Microsoft Tools
- User Interface Extensions for Oracle Net Directory Naming
- Enhancement of Directory Object Type Descriptions
- Integration with Windows Login Credentials
- Oracle Directory Objects in Active Directory

Automatic Discovery of Directory Servers

Oracle Net Configuration Assistant enables you to configure client computer and Oracle9i database server access to a directory server. When Oracle Net Configuration Assistant starts at the end of Oracle9i database installation or is manually started after installation, it prompts you to specify a directory server type to use. When you select Active Directory as the directory server type, Oracle Net Configuration Assistant automatically:

- Discovers the Active Directory server location
- Configures access to the Active Directory server
- Creates the Oracle context (also known as your domain)

If the Active Directory server through which client connections are accessing an Oracle9i database is shut down, another Active Directory server is automatically discovered and begins providing connection information; this prevents any downtime for client connections.

**Note:** You must be running the Oracle client and database software in a Windows 2000 domain to take advantage of the automatic directory server discovery features of Oracle Net Configuration Assistant. This is regardless of the Oracle client and database releases you are using.
If you are not running in a Windows 2000 domain, Oracle Net Configuration Assistant does not automatically discover your directory server, and instead prompts you for additional information, such as the Active Directory location.

When using the Oracle Net Configuration Assistant to complete directory usage configuration against Active Directory, Oracle schema creation can fail due to Active Directory display not being populated with all 24 default languages. Before running the Oracle Net Configuration Assistant to complete directory access configuration, verify that display specifiers for all 24 languages are populated by entering the following at the command prompt:

```
ldapde -p OneLevel -d cn=DisplaySpecifiers,cn=Configuration, domain context -f temp file
```

where:

- `domain context` is the domain context for this Active Directory server. For example `dc=acme,dc=com`
- `temp file` is a file where you want to put the output.

If the command reports that less than 24 entries were found, you can still use the Oracle Net Configuration Assistant. However, it will report that Oracle schema creation failed when all that failed was that display specifiers for some languages were not created.

### Integration with Microsoft Tools

Oracle9i database services, net service names, and enterprise role entries in Active Directory display in the Microsoft Windows 2000 tools in Table 4-2:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>This Enables You To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Explorer</td>
<td>A user tool that displays the hierarchical structure of files, directories, and local and network drives on your computer.</td>
<td>Display and test Oracle9i database service and net service name objects</td>
</tr>
<tr>
<td>Active Directory Users and Computers</td>
<td>An administrative tool installed on Windows servers configured as domain controllers. This tool enables you to add, modify, delete, and organize Windows 2000 accounts and groups, and publish resources in your organization’s directory.</td>
<td>Display and test Oracle9i database service and net service name objects and manage access control</td>
</tr>
</tbody>
</table>
See Also:
- "Testing Connectivity from Microsoft Tools" on page 4-17
- "Access Control List Management for Oracle Directory Objects" on page 4-20

User Interface Extensions for Oracle Net Directory Naming

The property menus of Oracle9i database service and net service name objects in Windows Explorer and Active Directory Users and Computers have been enhanced. This enables you to test for object connectivity to the Oracle9i database and perform database administration. When you right-click these Oracle directory objects, a menu presents you with two options for testing connectivity shown in Table 4–3:

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>Starts an application that tests that the username, password, and net service name you initially entered can connect to the Oracle9i database.</td>
</tr>
<tr>
<td>Connect with SQL*Plus</td>
<td>Starts SQL*Plus, which enables you to perform database administration, run scripts, and so on.</td>
</tr>
</tbody>
</table>

See Also:  "Testing Connectivity from Microsoft Tools" on page 4-17 for more information

Enhancement of Directory Object Type Descriptions

Oracle directory object type descriptions in Active Directory have been enhanced to make them easier to understand. For example, in Figure 4–1 is the description for OracleDefaultDomain’s type in the Type column of the right window pane.
Integration with Windows Login Credentials

This feature enables the Oracle client and database to use the credentials of the currently logged on Windows user for authentication and authorization.

The Oracle9i database and configuration tools can use the currently logged on Windows user’s login credentials to automatically connect to Active Directory without having to re-enter their login credentials. This enables:

- Oracle9i clients and databases to securely connect to Active Directory and retrieve net service name, enterprise user, and enterprise role information
- Configuration tools such as Oracle Enterprise Security Manager, Oracle Net Configuration Assistant, and Oracle Database Configuration Assistant to connect automatically to Active Directory and configure the Oracle9i database and net service name objects

Figure 4–1 Directory Object Type Descriptions in Active Directory
Oracle Directory Objects in Active Directory

Figure 4–2 shows when the Oracle9i database and Oracle Net Services are installed and configured to access Active Directory, Oracle directory objects appear in Active Directory Users and Computers:

Figure 4–2  Oracle Directory Objects in Active Directory Users and Computers
Table 4–4 describes these Oracle directory objects:

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>The domain (also known as the administrative context) in which you created your Oracle Context. The administrative context contains various Oracle entries to support directory naming and enterprise user security. Oracle Net Configuration Assistant automatically discovers this information during Oracle9i database integration with Active Directory.</td>
</tr>
<tr>
<td>Oracle Context</td>
<td>The top-level Oracle entry in the Active Directory tree that can contain Oracle9i database service and net service name object information. All Oracle software information is placed in this folder.</td>
</tr>
<tr>
<td>orcl</td>
<td>The Oracle9i database service name (for this example, orcl is the name).</td>
</tr>
<tr>
<td>Products</td>
<td>A folder for Oracle product information.</td>
</tr>
<tr>
<td>OracleDBSecurity</td>
<td>A folder for database security information.</td>
</tr>
<tr>
<td>OracleDefaultDomain</td>
<td>The default enterprise domain created. You can create additional enterprise domains with Oracle Enterprise Security Manager.</td>
</tr>
<tr>
<td>sales</td>
<td>The net service name object (for this example, sales is the name).</td>
</tr>
<tr>
<td>Users</td>
<td>The folder for the three Oracle security groups. See section “Access Control List Management for Oracle Directory Objects” on page 4-20 for more information. Enterprise users and roles created with Oracle Enterprise Security Manager also appear in this folder.</td>
</tr>
</tbody>
</table>
Requirements for Using Oracle9i with Active Directory

Table 4-5 lists the requirements that you must complete depend upon the Oracle features you want to use:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Oracle Schema Creation Requirements&quot; on page 4-12</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>&quot;Oracle Context Creation Requirements&quot; on page 4-13</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>&quot;Directory Naming Requirements&quot; on page 4-13</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>&quot;Enterprise User Security Requirements&quot; on page 4-15</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: The Oracle schema and Oracle Context can both be created by running Oracle Net Configuration Assistant.

Note: You must be running your Oracle clients and database server in a Windows 2000 domain. This is regardless of the Oracle client and Oracle database server releases you are running.

If you are using Active Directory with Oracle on Windows 2000 or Windows NT, then ping the DNS domain name of your Windows 2000 domain. If this does not work, perform either of the following tasks:

- Set your Windows 2000 primary domain controller's IP address as your DNS.
  
  For example, if your Windows 2000 domain is sales, the DNS domain name for this domain is sales.acme.com. The IP address is of the form 001.002.003.0.

- Add the DNS domain name of your Windows 2000 domain and your domain controller's IP address to your hosts or lmhosts file.

  On the Windows 2000 computer, either 001.002.003.0 can be set as the DNS, or 001.002.003.0 sales.acme.com can be added to the hosts or lmhosts file.

If you are using Active Directory with Oracle on Windows 2000 or Windows NT, then ping the DNS domain name of your Windows 2000 domain. If this does not work, perform either of the following tasks:

- Set your Windows 2000 primary domain controller's IP address as your DNS.
  
  For example, if your Windows 2000 domain is sales, the DNS domain name for this domain is sales.acme.com. The IP address is of the form 001.002.003.0.

- Add the DNS domain name of your Windows 2000 domain and your domain controller's IP address to your hosts or lmhosts file.

  On the Windows 2000 computer, either 001.002.003.0 can be set as the DNS, or 001.002.003.0 sales.acme.com can be added to the hosts or lmhosts file.
If this step is not performed, then errors such as the following are returned when using Active Directory:

_Cannot Chase Referrals_

On Windows NT and Windows 2000, the Oracle database service runs in the security context of the LocalSystem or a specific local or domain user. When using Oracle8i release 8.1.7 with Active Directory, if the database service runs in the security context of LocalSystem, manually add the computer name in which the database service is running. This enables you to access control entries on the OracleDBSecurity container object in the Active Directory with read permissions on the OracleDBSecurity container object. For example, if the database service OracleServiceORCL is running in the security context of LocalSystem in the computer mypc1, then add mypc1 with READ permissions ON OracleDBSecurity object to the access control entries on the OracleDBSecurity container object.

**Oracle Schema Creation Requirements**

Complete the following Oracle schema creation requirements to use the net directory naming and enterprise user security features with Active Directory. A schema is a set of rules for Oracle Net Services and Oracle9i database entries and their attributes stored in Active Directory.

- You can create only one Oracle schema for each _forest_.
- Perform schema creation on a Windows 2000 domain controller.
- The Windows 2000 domain controller must be the operations master that allows schema updates. See your Microsoft Windows operating system documentation for instructions.
- Log in as a member of the Schema Administrator group to create the schema. Domain administrators by default are in the Schema Administrator group.
- Use Oracle Net Configuration Assistant to create the Oracle schema. You can create your schema during or after installation. The schema can be created by running Oracle Net Configuration Assistant on the Oracle9i database.

_See Also:_ Oracle9i Net Services Administrator’s Guide for configuration procedures and Oracle9i Database installation guide for Windows for a configuration overview
Oracle Context Creation Requirements

You must complete the following Oracle Context creation requirements to use the net directory naming and enterprise user security features with Active Directory. The Oracle Context is the top-level Oracle entry in the Active Directory tree that contains Oracle9i database service and Oracle Net service name object information.

- You can create only one Oracle Context for each Windows 2000 domain (administrative context).
- You must have the right to create domain objects in order to create the Oracle Context in Active Directory with Oracle Net Configuration Assistant. If you are a domain administrator, you automatically have these rights.
- Use Oracle Net Configuration Assistant to create your Oracle Context. You can create the Oracle Context during Oracle9i Database Custom install or after installation.

See Also: See Oracle9i Database installation guide for Windows for installation procedures and Oracle9i Net Services Administrator’s Guide for configuration procedures

Directory Naming Requirements

Ensure that you first satisfy the requirements described in:

- "Oracle Schema Creation Requirements” on page 4-12
- "Oracle Context Creation Requirements” on page 4-13
Table 4–6 describes the minimum Microsoft and Oracle software releases that must be installed to use directory naming with Active Directory:

**Table 4–6 Minimal Directory Naming Requirements**

<table>
<thead>
<tr>
<th>For...</th>
<th>Required Microsoft Software</th>
<th>Required Oracle Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Computers from which to manage the Oracle9i enterprise users, roles and domains</td>
<td>- Windows 2000&lt;br&gt;- Windows NT 4.0 with Active Directory Service Interfaces (ADSI)&lt;br&gt;- Windows 95 or 98 with the Distributed Systems Client upgrade&lt;br&gt;- Must be in the Windows 2000 domain</td>
<td>Oracle8i Client release 8.1.6 or later</td>
</tr>
<tr>
<td>Database Server</td>
<td>- Windows NT 4.0 with ADSI&lt;br&gt;- The computer running the database server should be in the Windows 2000 domain&lt;br&gt;- Windows 2000</td>
<td>Oracle8i database release 8.1.6 or later is required for registering the database service as an object in Active Directory.</td>
</tr>
</tbody>
</table>
Enterprise User Security Requirements

Ensure that you first satisfy the requirements described in:

- "Oracle Schema Creation Requirements" on page 4-12
- "Oracle Context Creation Requirements" on page 4-13

Table 4–7 describes the Microsoft and Oracle software releases required to use enterprise user security with Active Directory:

<table>
<thead>
<tr>
<th>For...</th>
<th>Microsoft Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server</td>
<td>Windows NT 4.0 with ADSI</td>
</tr>
<tr>
<td></td>
<td>Oracle8i database release 8.1.6 or later is required for registering the database service as an object in Active Directory.</td>
</tr>
<tr>
<td></td>
<td>The computer running the database server should be in the Windows 2000 domain</td>
</tr>
<tr>
<td></td>
<td>Windows 2000</td>
</tr>
</tbody>
</table>

| Remote computer | The host computer has to be in the Windows 2000 domain |
|                | Windows NT 4.0 with ADSI or Windows 2000                |
|                | Oracle Enterprise Manager Console release 2.1, which includes: |
|                | - Oracle Enterprise Security Manager                     |
|                | - Oracle Net Services                                    |

Note: Oracle Enterprise Security Manager is required if you want to create and manage enterprise users, roles, and domains. If Oracle Enterprise Security Manager uses Native Authentication to connect to Active Directory, the host computer should be in a Windows 2000 domain and the user should be logged into the host computer as a Windows 2000 domain user.
Oracle9i Installation and Configuration with Active Directory

This section provides an overview of installation and configuration information. This section contains these topics:

- Installation Tasks
- Post-Installation Configuration Tasks

Installation Tasks

See the Oracle9i Database installation guide for Windows for Oracle9i installation instructions.

Post-Installation Configuration Tasks

You must set the OSAUTH_X509_NAME registry parameter to true to use enterprise user security in the Oracle Windows Native Authentication Adapter. See "Task 2: Set the OSAUTH_X509_NAME Registry Parameter".

Testing Connectivity

This section describes how to connect to an Oracle9i database through Active Directory. This section contains these topics:

- Testing Connectivity from Client Computers
- Testing Connectivity from Microsoft Tools

Testing Connectivity from Client Computers

When using Oracle Net directory naming client computers connect to a database by specifying the database or net service name entry that appears in the Oracle Context. For example, if the database entry under the Oracle Context in Active Directory was orcl, a user connects through SQL*Plus to the Oracle9i database as shown in Table 4-8:

<table>
<thead>
<tr>
<th>If the Client and Oracle9i database are in...</th>
<th>The Client Specifies The Following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The same domain</td>
<td>SQL&gt; CONNECT scott/tiger@orcl</td>
</tr>
<tr>
<td>Different domains</td>
<td>SQL&gt; CONNECT scott/tiger@orcl.domain</td>
</tr>
<tr>
<td></td>
<td>where domain is the domain in which the Oracle9i database is located.</td>
</tr>
</tbody>
</table>
The connect strings in this table follow DNS-style conventions. While Active Directory also supports connections using X.500 naming conventions, DNS-style conventions are the recommended method because of ease of use. DNS-style conventions enable client users to access an Oracle9i database through a directory server by entering minimal connection information; this is the case even when the client computer and Oracle9i database are in separate domains. X.500 names are longer; this is especially the case when the client and Oracle9i database are located in different domains (also known as administrative contexts).

To learn more about X.500 naming conventions, see "Configuration Management Concepts", of Oracle9i Net Services Administrator’s Guide for information.

Testing Connectivity from Microsoft Tools

Oracle directory objects in Active Directory are integrated with Microsoft tools such as:

- Windows Explorer
- Active Directory Users and Computers

You can perform the following tasks from within these Microsoft tools:

- Connect with SQL*Plus to an Oracle9i database
- Test Oracle9i database connectivity

**Note:** All clients accessing an Oracle9i database through Active Directory require read access on all net service name objects in the Oracle Context and must be able to authenticate anonymously with Active Directory. Oracle Net Configuration Assistant automatically sets this up.
## Accessing Connectivity Tools

To access connectivity tools:

1. Start the Microsoft tool with which you want to connect:

<table>
<thead>
<tr>
<th>With...</th>
<th>Choose...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Explorer</td>
<td>1. Start &gt; Programs &gt; Accessories &gt; Windows Explorer</td>
</tr>
<tr>
<td></td>
<td>2. Expand My Network Places.</td>
</tr>
<tr>
<td></td>
<td>3. Expand Entire Network.</td>
</tr>
<tr>
<td>Active Directory Users and</td>
<td>1. Start &gt; Programs &gt; Administrative Tools &gt; Active Directory Users and</td>
</tr>
<tr>
<td>Computers</td>
<td>Computers.</td>
</tr>
</tbody>
</table>

2. Expand the domain in which your Oracle Context is located.

3. Go to your Oracle Context.

4. Right-click a database service or Oracle Net Service name object.

A menu appears with several options:

![Screenshot of Active Directory Users and Computers window](image)
5. Make an appropriate selection:

<table>
<thead>
<tr>
<th>If You Want To...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test connectivity</td>
<td>1. Choose Test.</td>
</tr>
<tr>
<td></td>
<td>2. Go to section &quot;Testing Connectivity&quot;</td>
</tr>
<tr>
<td>Connect with SQL*Plus</td>
<td>1. Choose Connect with SQL*Plus.</td>
</tr>
<tr>
<td></td>
<td>2. Go to section &quot;Connecting With SQL*Plus&quot;</td>
</tr>
</tbody>
</table>

**Testing Connectivity**

A status message appears describing the status of your connection attempt:

**Connecting With SQL*Plus**

The Oracle SQL*Plus Login dialog box appears:

Enter your username and password. A status message appears describing the status of your connection attempt.
Access Control List Management for Oracle Directory Objects

Access Control Lists provide Active Directory security by specifying:

- The user that can access the object attributes in the object
- Authentication method to access the entry
- Access rights, or what the user can do with the object (read/write) attributes in the object

Three security groups shown in Table 4–9 are automatically created when the Oracle Context is created in Active Directory. The user configuring access (and thus creating the Oracle Context) is automatically added to each:

Table 4–9 Oracle Context Security Groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OracleDBSecurityAdmin</td>
<td>Group for the creator of the Oracle Context. Users in this group can also:</td>
</tr>
<tr>
<td></td>
<td>- Manage the group membership for all three security groups</td>
</tr>
<tr>
<td></td>
<td>- Manage any object in the Oracle Context</td>
</tr>
<tr>
<td></td>
<td>- Use Oracle Enterprise Security Manager to create enterprise domains</td>
</tr>
<tr>
<td>OracleDBCreator</td>
<td>Group for the creator of the Oracle9i database. Users in this group can:</td>
</tr>
<tr>
<td></td>
<td>- This group creates new Oracle9i database objects in the Oracle Context</td>
</tr>
<tr>
<td></td>
<td>- Modify the Oracle9i database objects that they create</td>
</tr>
<tr>
<td></td>
<td>- Read, but not modify, the membership for this group</td>
</tr>
<tr>
<td></td>
<td>The domain administrator is automatically a member of this group.</td>
</tr>
<tr>
<td>OracleNetAdmins</td>
<td>Users in this group can:</td>
</tr>
<tr>
<td></td>
<td>- Create, modify, and read Oracle Net Services objects and attributes</td>
</tr>
<tr>
<td></td>
<td>- Read the group membership of this group</td>
</tr>
</tbody>
</table>
Accessing the Security Groups

Active Directory Users and Computers enables you to add or remove users or change permission settings in the three security groups. See Table 4–10.

<table>
<thead>
<tr>
<th>If You Want to...</th>
<th>Use...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove users in OracleNetAdmins</td>
<td>Active Directory Users and Computers</td>
</tr>
<tr>
<td>Add or remove users in</td>
<td></td>
</tr>
<tr>
<td>OracleDBSecurityAdmin or</td>
<td></td>
</tr>
<tr>
<td>OracleDBCcreator</td>
<td></td>
</tr>
</tbody>
</table>


**Note:** Use Active Directory Users and Computers to perform the procedures described in this section. Windows Explorer does not provide the functionality.

To add or remove users or change permission settings:

2. Choose Advanced Features from the View main menu.
   This enables you to view and edit information that is normally hidden.
3. Expand the domain (administrative context) in which your Oracle Context is located.
4. Expand Users.
The three security groups appear in the right window pane:

5. Right-click the Oracle security group that you want to view or modify. A menu appears with several options.
7. Make an appropriate selection:

<table>
<thead>
<tr>
<th>If You Want To...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove users</td>
<td>1. Choose the Members tab.</td>
</tr>
<tr>
<td></td>
<td>2. Go to section &quot;Adding or Removing Users&quot; on page 4-23.</td>
</tr>
<tr>
<td></td>
<td>2. Go to section &quot;Changing User Permissions&quot; on page 4-24.</td>
</tr>
</tbody>
</table>
Adding or Removing Users

To add or remove users:


   The Properties dialog box for the group you selected appears (in this example, OracleDBSecurityAdmins):

   ![OracleDBSecurityAdmins Properties dialog box]

2. Make an appropriate selection:

<table>
<thead>
<tr>
<th>To...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Users</td>
<td>1. Choose Add.</td>
</tr>
<tr>
<td></td>
<td>The Select Users, Contacts, Computers, or Groups dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>2. Select appropriate users or groups, and choose Add.</td>
</tr>
<tr>
<td></td>
<td>Your selections appear in the Select Users, Contacts, Computers, or</td>
</tr>
<tr>
<td></td>
<td>Groups dialog box.</td>
</tr>
<tr>
<td></td>
<td>3. Choose OK.</td>
</tr>
<tr>
<td>Remove Users</td>
<td>1. Select a user to remove.</td>
</tr>
<tr>
<td></td>
<td>2. Choose Remove.</td>
</tr>
<tr>
<td></td>
<td>The user is removed.</td>
</tr>
<tr>
<td></td>
<td>3. Choose OK.</td>
</tr>
</tbody>
</table>
Changing User Permissions

To change user permissions:

   The Properties dialog box for the group you selected appears.
2. Choose Advanced.
3. Choose View/Edit.
   The Permission Entry dialog box for the security group you selected appears:
4. View or make appropriate changes to group permissions.

5. Choose OK.

Creating Enterprise Domains

A default enterprise domain, OracleDefaultDomain, is created in your Oracle Context. If you do not want to use this domain or want to create another domain, use Oracle Enterprise Security Manager to create additional enterprise domains. These domains are added under the OracleDBSecurity folder.
This chapter describes the storing and retrieving of Oracle Wallets in the Windows registry.

This chapter contains these topics:

- Storing Private Keys and Trustpoints
- Storing the User’s Profile
- Storing Oracle Wallets in the Windows Registry
- Oracle Enterprise Login Assistant
- Wallet Resource Locator
Storing Private Keys and Trustpoints

Oracle Wallets store the private keys and trustpoints, and holds the digital certificates used in public key applications for authentication and encryption. The Oracle Wallet Manager tool 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. Using Oracle Enterprise Login Assistant, the user can log on once for each session and until the user logs out, all applications use the same obfuscated wallet to authenticate. On Windows 95, Windows 98, Windows NT, Windows 2000, the encrypted and obfuscated Oracle Wallets can be stored in the file system or the user profile area in the Windows registry. Oracle Wallet Manager, Oracle Enterprise Login Assistant and their related functionality are features of Oracle Advanced Security, a separately licensable option to the Oracle9i database.

Storing the User’s Profile

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

Storing Oracle Wallets in the Windows Registry

On Windows operating systems, Oracle Wallets are located in the user profile area \HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS in the registry. 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.

The WALLET_LOCATION parameter in the sqlnet.ora file specifies whether Oracle Wallets are stored in the file system or in the registry. It also specifies the location of the encrypted or obfuscated Oracle Wallet.

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

\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\SALESAPP is

WALLET_LOCATION =
  (SOURCE= (METHOD=REG) (METHOD_DATA= (KEY=SALESAPP)))
The encrypted or obfuscated Oracle Wallet is stored in the registry under `\HKEY_CURRENT_USER\SOFTWARE\ORACLE\ORACLE\WALLETS\SALESAPP\EWALLET.P12` or `\HKEY_CURRENT_USER\SOFTWARE\ORACLE\ORACLE_WALLETS\SALESAPP\CWALLET.SSO`, respectively.

**Oracle Wallet Manager**

The Oracle Wallet Manager tool creates and manages Oracle Wallets. To use the Windows registry for Oracle Wallets, the Use Windows System registry check box needs to be selected. If Windows System Registry is selected, when the tool opens a wallet or saves a new wallet, it shows a list of existing keys under:

`\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS`

The user can select one of the existing locations, or enter the name for a new location (registry key). For example, if the new key is `key1`, then the tool creates a registry key:

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

and the encrypted wallet is stored at the registry value:

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

and the obfuscated wallet is stored at the registry value:

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

If the user does not select the Use Windows System registry check box, then the tool displays all the available drives and directories on the local computer. The user can select one of the existing directories or can 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 the Oracle Enterprise Login Assistant is launched, the tool looks for the encrypted or obfuscated Oracle Wallet and stores the obfuscated wallet in the default file system location: `%USERPROFILE%\ORACLE\WALLETS`. If an obfuscated wallet is found, the tool returns a message stating that autologin has been enabled. Otherwise, the tool displays a message stating that autologin has not been enabled. If Login from the Oracle Enterprise Login Assistant is selected, the tool looks for the encrypted wallet in the default file system location, prompts the user for the wallet password, and creates an obfuscated wallet in the default location. Oracle Enterprise Login Assistant then displays a message that autologin has been enabled. Otherwise, if Login from the tool is selected and no encrypted wallet is found in the default location, the tool displays a message stating that no wallet is
found in the default location. If Logout from the tool is selected, the obfuscated wallet is removed from the default location. If the user exits the tool, without selecting Logout, then the obfuscated wallet is left in the default location.

In Oracle9i, Windows when the Oracle Enterprise Login Assistant is launched, the tool looks for the obfuscated wallet in the registry location:

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

If an obfuscated wallet is found and Logout is selected, the tool removes this obfuscated wallet from the registry, the tool looks in the file system location `%USERPROFILE%\ORACLE\WALLETS` for an obfuscated wallet. If an obfuscated wallet is found and Logout is selected, the tool removes this obfuscated wallet from the file system. If an obfuscated wallet is not found in the registry or the file system default locations, then the tool displays a message stating that autologin is not enabled.

If Login from the Oracle Enterprise Login Assistant is selected, the tool looks for the encrypted wallet in the registry location:

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

If an encrypted wallet is found in this location, the user is prompted for the wallet password and the tool creates the obfuscated wallet in the same registry location. At the next Logout in the same session of the tool, the obfuscated wallet is removed from the registry. If Login is selected from the Oracle Enterprise Login Assistant and no encrypted wallet is found in the registry, the tool then looks for the encrypted wallet in the local computer’s file system under `%USERPROFILE%\ORACLE\WALLETS`. If an encrypted wallet is found in this location, the user is prompted for the wallet password and an obfuscated wallet is created in the same default file system location. At the next Logout in the same session of the tool, the obfuscated wallet is removed from the file system. If Login is selected and no encrypted wallet is found in the default location (in the registry or file system) then the tool displays a message stating that no Oracle Wallet was found in the default location.

**Wallet Resource Locator**

The parameter `WALLET_LOCATION` in the `sqlnet.ora` file 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 the `WALLET_LOCATION` parameter in the `sqlnet.ora` file, Oracle PKI applications first look for the obfuscated wallet in the registry key:

```
\HKEY_CURRENT_USER\SOFTWARE\ORACLE\WALLETS\DEFAULT
```
If it is not found, Oracle PKI applications look for the obfuscated wallet in the computer’s local file system under %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.
This chapter describes the 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 the 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 - Stores the digital certificates trustpoints and private keys used in public key applications for encryption, 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 the decrypted, obfuscated Oracle Wallets.

Windows Public Key Infrastructure

The Microsoft Certificate Store integration works only with the certificates that use Microsoft Enhanced Cryptographic Provider. You need to install the Windows High Encryption Pack to get this Cryptographic Provider and select Microsoft Enhanced Cryptographic Provider when creating these certificates. 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 certificates and their associated properties. Windows 2000 stores certificates and certificate revocation lists in logical and physical stores. Logical stores contain pointers to the public key objects in the physical stores. Logical stores enable public key objects to be shared between users, computers, and services without requiring the storage of duplicates of the objects for each user, computer, or service. With physical stores, public key objects are stored in the registry of the local computer or, for some user certificates, in Active Directory. Some of the standard system certificate stores defined by Microsoft are:

- 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 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:

- The Server Engine - handles all certificate requests. The engine interacts with modules at each processing stage to ensure that the proper action is taken based on the state of the request.
- The Intermediary - receives requests for new certificate from clients and then submits them to the 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**

The Wallet Resource Locator (WRL) specifies that the WALLET_LOCATION parameter in the sqlnet.ora file identifies a particular PKI.

The user can choose between using Oracle Wallet or Microsoft Certificate Store by setting the WALLET_LOCATION parameter in sqlnet.ora.

To use the credentials from Microsoft Certificate Store:

- The WALLET_LOCATION parameter in sqlnet.ora is set to:
  
  WALLET_LOCATION = (SOURCE = (METHOD=MCS))

- The Oracle application uses Oracle’s TCP/IP with SSL protocol (TCPS) to connect to the Oracle Server.

- The SSL protocol uses the X.509 certificates and trustpoints from the user’s Microsoft Certificate Store for SSL authentication.
This appendix describes Oracle Net Services configuration for Windows. For more specific 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
- Named Pipes Protocol for Windows 95

See Also: Oracle Net Services integration with Active Directory for Windows 2000 in Chapter 4, “Using Oracle9i Directory Server Features with Active Directory”
Understanding Oracle Net Services Registry Parameter and Subkeys

The registry contains the 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:

- Oracle_HOME_NAME\ClientCache
- Oracle_HOME_NAME\CMAdmin
- Oracle_HOME_NAME\CMan
- Oracle_HOME_NAME\TNSListener

Each service subkey contains the parameters shown in Table A–1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayName</td>
<td>Specifies the service name.</td>
</tr>
<tr>
<td>ImagePath</td>
<td>Specifies the fully qualified path name of the executable invoked by the service and any command line arguments passed to the executable at runtime.</td>
</tr>
<tr>
<td>ObjectName</td>
<td>Specifies the logon user account and computer to which the service should log on.</td>
</tr>
</tbody>
</table>
If the same IP address and port are used for different listeners, then instead of the second and the consecutive listeners failing to bind as expected, it allows them to go ahead and listen on this IP address and port. This results 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, Windows 98, and Windows 95:

- **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 the **LOCAL** parameter to connect to the database without specifying a connect identifier in the connect string. The value for the **LOCAL** parameter is the net service name in the `tnsnames.ora` file located in the `ORACLE_BASE\ORACLE_HOME\network\admin` directory.

For example, if the **LOCAL** parameter is specified as `finance`, you connect to a database from SQL*Plus with the following command:

```sql
SQL> CONNECT scott/tiger AS finance
```

Oracle Net Services 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 the **TNS_ADMIN** parameter to change the directory name for configuration files from the default location. 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 the USE_SHARED_SOCKET parameter to true to enable the 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 Oracle 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 the variable USE_SHARED_SOCKET for both Oracle homes.

Advanced Network Configuration

The following sections describe advanced configuration procedures specifically for Oracle Net Services on the 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 the OracleHOME_NAME TNSListener service 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 the OracleHOME_NAME TNSListener service.
   
   The Services dialog box appears.

3. Choose the This Account option button. Then, choose the "..." option button 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. Choose OK.
The Services dialog box appears with the user ID displayed in the This Account text box.
6. Type your password in the Password text box.
7. Retype the same logon password in the Confirm Password text box.
8. Choose OK.

**Named Pipes Protocol for Windows 95**

If you use the Named Pipes protocol for Windows 95 to connect to Oracle9i for Windows NT, client applications may run very slowly due to a known problem in Microsoft's implementation of Windows 95 NWLinkDirect-Hosting.

To work around this problem, you may do any of the following:
- Use other protocols (for example, TCP/IP) for connecting from an Oracle client
- Remove the protocol NWLink from Windows 95 if you do not need to access NetWare Servers
- Disable the Direct-Hosting feature on Windows 95

**TCP/IP Support for Windows 95**

Oracle TCP/IP support for Windows 95/98 uses Windows Sockets 2 interfaces. Therefore, you must install Windows Socket 2 Update for Windows 95 before installing Oracle9i. Download it from the following Microsoft Web site:

http://www.microsoft.com/windows95/downloads

Windows Socket 2 Update for Windows 95 can also be installed by double-clicking on the file WS2SETUP.EXE located in the \WINSOCK2 directory at the root of your distribution media.
**Active Directory Service Interfaces (ADSI)**

A client-side product based on the 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.

**authentication**

The process of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to granting access to resources in a system. A recipient of an authenticated message can be certain of the message’s origin (its sender). Authentication is presumed to preclude the possibility that another party has impersonated the sender.

**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. The set of privileges available to an authenticated entity.
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 the certificate authority’s private key.

Common Object Request Broker Architecture (CORBA)
A standard that enables distributed objects to communicate with each other, independent of programming language, operating system, and location.

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 the database name, the names and locations of associated databases and online redo log files, the timestamp of the database creation, the 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.

digital certificate
An ITU X.509 v3 standard data structure that securely binds 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.

downgrade
To transform an installed version of an Oracle database from a later release back into an earlier release.

Dynamic Link Library (DLL)
An executable file that a Windows application can load when needed.

encryption
The process of disguising a message rendering it unreadable to any but the intended recipient.

Enterprise Java Beans
A server-side component model for Java.

external role
Roles created and managed by the Windows NT and Windows 20000 operating systems. Once an external role is created, you can grant or revoke that role to a database user. You must set the 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 routine
A function written in a third-generation language (3GL), such as C, and callable from within PL/SQL or SQL as if it were a PL/SQL function or procedure.
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) privileges.

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.

Globalization Support
The Oracle architecture that ensures that database utilities, error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

HOME ID
Represents a unique registry subkey for each Oracle home directory in which you install products. A new HOME ID is created and incremented each time you install products to a different Oracle home directory on one computer. Each HOME ID 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.

initialization parameter file
An ASCII text file that contains information needed to initialize a database and instance. The init.ora file resides in \ORACLE_BASE\admin\DB_NAME\pfile directory 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 the type of computer), Oracle allocates a memory area called the System Global Area (SGA) and starts one or more Oracle processes. This combination of the SGA and the Oracle processes is
called an instance. The memory and processes of an instance manage the associated database's data efficiently and serve the one or more users of the database.

**Internet Inter-ORB Protocol (IIOP)**
A standard that enables Object Request Brokers (ORBs) from different vendors to communicate with each other using TCP/IP.

**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 the Oracle Internet Directory.

**listener**
A process that resides on the server whose responsibility is to listen for incoming client connection requests and manage the traffic to the server.

Every time a client requests a network session with a server, a listener receives the actual request. If the client information matches the listener information, then the listener grants a connection to the server.

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

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

**local role**
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 both Windows NT (for external roles) and the Oracle database (for local roles) to grant roles 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.
**Microsoft Transaction Server**
A COM-based transaction processing system that runs on an Internet or network server.

**migrate**
To transform an installed version of an Oracle database from a major release to another major release, for example, from Oracle8 to Oracle9i.

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

**multiple Oracle homes**
The capability of having more than one Oracle home on a computer.

**net service name**
The 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, database alias, or service name.

**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.

**NT global groups**
Contains users with access to computers and resources throughout the current domain and within any other domains that trust it. Global groups only contain global domain user accounts as their members.

**Object Request Broker (ORB)**
A software component that serves as the middle ware between distributed objects. The distributed objects must comply with the Common Object Request Broker Architecture (CORBA) standard.

**Optimal Flexible Architecture (OFA)**
A set of file naming and placement guidelines for Oracle software and databases.
Oracle Call Interface (OCI)

An application programming interface that enables you to manipulate data and schemas in an Oracle database. You compile and link an Oracle Call Interface program in the same way that you compile and link a nondatabase application. There is no need for a separate preprocessing or precompilation step.


The information in this guide applies to the Oracle9i Enterprise Edition, Oracle9i Standard Edition, and Oracle9i Personal Edition database types. Unless otherwise noted, the features and functionality described in this guide are common to all three database types.

ORACLE_BASE

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

If you install an OFA-compliant database using Oracle Universal Installer defaults, ORACLE_BASE is X:\ORACLE where X is any hard drive (for example, C:\ORACLE).

ORACLE_HOME

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

If you install an OFA-compliant database, using Oracle Universal Installer defaults, Oracle home (known as \ORACLE_HOME in this guide) is located beneath X:\ORACLE_BASE. It contains subdirectories for Oracle software executables and network files.

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 foundation layer**
A networking communication layer that is responsible for establishing and maintaining the connection between the client application and server, as well as exchanging messages between them.

**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 the Oracle Net, listener, Oracle Connection Manager, Oracle Net Configuration Assistant, and Oracle Net Manager.

**Oracle Protocol Support**
A software layer responsible for mapping Transparent Network Substrate (TNS) functionality to industry-standard protocols used in the client/server connection.

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

**Oracle9i JVM**
Oracle9i includes Oracle9i JVM, the integrated Java Virtual Machine. Oracle9i JVM provides Java2 support (JDK1.2), a CORBA 2.0 Object Request Broker, an embedded JDBC driver, a SQLJ translator, and an Enterprise Java Beans transaction server.

**PL/SQL**
Oracle Corporation’s procedural language extension to SQL.
PL/SQL enables you to mix SQL statements with procedural constructs. You can define and execute PL/SQL program units such as procedures, functions, and packages.

**precompiler**
A programming tool that enables you to embed SQL statements in a high-level source program.

**private key**
In public-key cryptography, this key is the secret key. It is primarily used for decryption but is also used for encryption with digital signatures.
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 infrastructure
Information security technology utilizing the principles of public key cryptography. Public key cryptography involves encrypting and decrypting information using a shared public and private key pair. 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.

redo log buffer
A circular buffer in the System Global Area (SGA) that contains information about changes made to the database.

redo log file
A file that contains a record of all changes made to data in the database buffer cache. If an instance failure occurs, the redo log files are used to recover the modified data that was in memory.
registry
A Windows repository that stores configuration information for a computer.

remote computer
A computer on a network other than the local computer.

remote database
A database on a remote computer from the local client computer.

replication
The process of copying and maintaining database objects in multiple databases that make up a distributed database system.

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 Windows NT 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).

snap-in
An administrative tool that runs within Microsoft Management Console.

starter database
A preconfigured, ready-to-use database that requires minimal user input to create.
**SYSDBA**
A special database administration role that contains all system privileges with the ADMIN OPTION, and the 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 the 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 descriptors in a tnsnames.ora file, and in the definition of the network listener in a listener.ora file.

**SYSTEM username**
One of two standard DBA usernames automatically created with each database. (The other username is **SYS**.) SYSTEM is created with an initial password of MANAGER. The SYSTEM username 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 mapped to net service names. The file may be maintained centrally or locally, for use by all or individual clients.

The tnsnames.ora file typically resides in `ORACLE_BASE\ORACLE_HOME\network\admin` on Windows NT.

**trust point**
A trust point or trusted certificate is a third party identity that is qualified with a level of trust. The trusted certificate is used when an identity is being validated as the entity it claims to be. The 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.

**upgrade**
To transform an installed version of an Oracle database major release into another major release of the same version. Compare with "migrate".

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

**view**
A selective presentation of the structure of, and data in, one or more tables (or other views).
Index

A

Access Control Lists
accessing security groups, 4-21
adding or removing users in security groups, 4-23
available security groups, 4-20
changing user permissions in security groups, 4-24
Active Directory
accessing security groups, 4-21
adding or removing users in security groups, 4-23
automatic discovery of directory servers, 4-5
changing permissions in security groups, 4-24
connecting to a database, 4-16, 4-17
creating security domains, 4-25
defined, 4-2
enhancement of directory object type descriptions, 4-7
how Oracle directory objects appear, 4-9
integration with directory servers, 4-5
integration with Microsoft tools, 4-6
integration with Windows login credentials, 4-8
managing Access Control Lists, 4-20
managing security groups directory server managing Access Control Lists, 4-20
procedures for installing Oracle into, 4-16
requirements for creating an Oracle Context, 4-13
requirements for creating an Oracle schema, 4-12
requirements for creating enterprise user security, 4-15
requirements for creating Oracle Net directory naming, 4-13
requirements for using Oracle, 4-11
testing connectivity from client computers, 4-16
testing connectivity with Microsoft tools, 4-17
testing connectivity with SQL*Plus, 4-7, 4-19
testing database connectivity, 4-7, 4-19
user interface extensions, 4-7
Active Directory Users and Computers
accessing directory server objects, 4-18
integration with Oracle objects in Active Directory, 4-6
testing database connectivity from, 4-19
Administering, 2-1, 3-1
authentication automatically enabling during installation, 1-8
creating an operating system-authenticated user, 2-31
enhancements, 1-4
overview, 1-2
setting the OS_AUTHENT_PREFIX initialization parameter, 2-29
setting the OSAUTH_PREFIX_DOMAIN registry parameter, 2-29
using Windows native authentication methods, 1-2
when to use enterprise users, 1-5
when to use external users, 1-5
Authentication Adapters
using, A-4
authentication parameter settings viewing, 2-13
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
contact name, 4-4
CREATE USER command, 2-31

D
database administrator privileges
granting for a single database on a computer with
Oracle Administration Assistant for
Windows NT, 2-24, 2-25
granting for all databases on a computer with
Oracle Administration Assistant for
Windows NT, 2-6, 2-7
manually granting for all databases on a
computer, 2-34
database operator privileges
granting for a single database on a computer with
Oracle Administration Assistant for
Windows NT, 2-24, 2-26
granting for all databases on a computer with
Oracle Administration Assistant for
Windows NT, 2-6, 2-8
manually granting for all databases on a
computer, 2-34
database privileges
in Windows NT local groups, 2-34, 2-40, 2-42
directory servers
automatic discovery of directory servers, 4-5
creating security domains, 4-25
enhancement of directory object type
descriptions, 4-7
features integrated with Oracle9i, 4-3
how Oracle directory objects display in Active
Directory, 4-9
installation tasks, 4-16
integration with Active Directory, 4-5
integration with Microsoft tools, 4-6
integration with Windows login credentials, 4-8
overview, 4-2
requirements for creating an Oracle Context in
Active Directory, 4-13
requirements for creating an Oracle schema in
Active Directory, 4-12
requirements for creating enterprise user security
in Active Directory, 4-15
requirements for creating Oracle Net directory
naming in Active Directory, 4-13
requirements for using Oracle with Active
Directory, 4-11
user interface extensions, 4-7
DisplayName parameter, A-2
DNS-style naming convention, 4-16

E
time domains
different from Windows domains, 4-4
viewing in Active Directory, 4-10
time roles
authorizing in Windows 2000 domains, 3-3
environments in which to use, 1-5
viewing in Active Directory, 4-10
time user security
creation requirements, 4-15
time users
environments in which to use, 1-5
viewing in Active Directory, 4-10
time OS roles
defined, 2-10
time roles
administering, 2-2
administering manually on Windows NT, 2-27
administering with Oracle Administration Assistant for Windows NT, 2-2
creating with Oracle Administration Assistant for Windows NT, 2-20
defined, 2-10
environments in which to use, 1-5
external users
administering, 2-2
administering manually on Windows NT, 2-27
administering with Oracle Administration Assistant for Windows NT, 2-2
creating manually, 2-28
creating with Oracle Administration Assistant for Windows NT, 2-14
environments in which to use, 1-5

F
Features
new, xix

G
generic documentation references
OS_AUTHENT_PREFIX initialization parameter, 2-13
OSDBA group, 2-43
OSOPER group, 2-43
Windows NT-specific authentication methods, 1-2
Windows NT-specific local groups use, 2-34
Windows NT-specific OS_AUTHENT_PREFIX case insensitivity, 2-29
Windows NT-specific role syntax, 2-42

I
ImagePath parameter, A-2
initialization parameters
OS_AUTHENT_PREFIX, 2-29
OS_ROLES, 1-4, 2-13, 2-39, 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, 2-34, 2-40, 2-42
LOCAL networking parameter, A-3
local roles
defined, 2-10

M
Microsoft Certificate Services, 6-3
Microsoft Certificate Stores, 6-2
Microsoft Management Console requirements, 2-3
running Oracle Administration Assistant for Windows NT from, 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
new
Features, xix
nonprivileged database user
creating manually, 2-28
creating with Oracle Administration Assistant for Windows NT, 2-14
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
creating an authenticated user
creating, 2-31
Index-4

setting the OS_AUTHENT_PREFIX initialization parameter, 2-29
setting the OSAUTH_PREFIX_DOMAIN registry parameter, 2-29
operating systems
  authentication overview, 1-2
OPSS, 2-29
ORA_DBA local group
  adding users to, 1-8, 2-34
ORA_OPER local group
  adding users to, 2-34
ORA_SID_DBA local group
  adding users to, 2-34
ORA_SID_OPER local group
  adding users to, 2-34
Oracle Administration Assistant for Windows NT
  adding a computer to the navigation tree, 2-5
  connecting to a database, 2-9
  creating a local database role, 2-18
  creating a nonprivileged database user, 2-14
  creating an external role, 2-20
  granting administrator privileges for a single database on a computer, 2-25
  granting administrator privileges for all databases on a computer, 2-7
  granting operator privileges for a single database on a computer, 2-26
  granting operator privileges for all databases on a computer, 2-8
  managing Oracle 7.x and Oracle 8.0.x computers, 2-4
  managing remote computers, 2-4
  saving a navigation tree configuration, 2-5
  setting the OS_AUTHENT_PREFIX initialization parameter, 2-13
  setting the OS_ROLES initialization parameter, 2-13
  troubleshooting database connection issues, 2-11
  using, 2-2
  viewing database authentication parameter settings, 2-13
Oracle Context
  creating with Oracle Net Configuration Assistant, 4-13
  creation requirements, 4-13
defined, 4-10
Oracle Database Configuration Assistant
  registering a database object in a directory server, 4-8
Oracle Enterprise Security Manager
  creating security domains, 4-25
  using, 1-7
  using simple authentication, 1-8
  using with Windows native authentication, 1-8
Oracle Names
  Named Pipes Protocol Adapter, A-4
Oracle Net Configuration Assistant
  automatically discovering directory server information, 4-10
  configuring Oracle software with a directory server, 4-5, 4-8
  creating the Oracle Context, 4-13
  creating the Oracle schema, 4-11
Oracle Net directory naming
  connecting to a database through a directory server, 4-16
  creation requirements, 4-13
  testing connectivity from client computers, 4-17
  testing connectivity with Microsoft tools, 4-17
Oracle Public Key Infrastructure, 6-2
Oracle schema
  creating with Oracle Net Configuration Assistant, 4-11
  creation requirements, 4-12
Oracle Wallet Manager, 5-3
Oracle Wallets, 5-2
  Storing in the Windows Registry, 5-2
  storing private keys and trustpoints, 5-2
Oracle9i, 2-18
Oracle9i Database Administrator’s Guide, 2-18
OracleDBCreator security group
defined, 4-20
OracleDBSecurityAdmin security group
defined, 4-20
OracleDefaultDomain
directory server security domain, 4-25
OracleHOME_NAMEClientCache key, A-2
OracleHOME_NAMEMAdminService key, A-2
OracleHOME_NAMEManService key, A-2
OracleHOME_NAMETNSListener key, A-2
OracleHOME_NAMETNSListener service, A-4
OracleNetAdmins security group
  defined, 4-20
OS database administrators
  defined, 2-11
OS database operators
  defined, 2-11
OS_AUTHENT_PREFIX initialization parameter, 2-13, 2-28, 2-29
OS_ROLES initialization parameter, 2-13
OS_ROLES parameter
  not required in Windows 2000 domains, 3-3
  using with external roles, 1-4, 2-13, 2-39
OSAUTH_PREFIX_DOMAIN registry parameter, 2-4, 2-29, 2-30
OSAUTH_X509_NAME registry parameter, 3-2
OSDBA group, 2-43
OSOPER group, 2-43

P

passwords
  connecting without a password with
    SYSDBA, 1-8
privileges
  in Windows NT local groups, 2-34, 2-40, 2-42

R

registry
  DisplayName, A-2
  ImagePath, A-2
  ObjectName, A-2
  OracleHOME_NAMEClientCache key, A-2
  OracleHOME_NAMEMCMAadminService key, A-2
  OracleHOME_NAMEMCManService key, A-2
  OracleHOME_NAMETNSListener key, A-2
registry parameters
  OSAUTH_PREFIX_DOMAIN, 2-30
remote computers
  managing with Oracle Administration Assistant for Windows NT, 2-4
requirements
  for creating an Oracle Context in Active Directory, 4-13
  for creating an Oracle schema in Active Directory, 4-12
  for creating enterprise user security in Active Directory, 4-15
  for creating Oracle Net directory naming in Active Directory, 4-13
  for using Oracle with Active Directory, 4-11
role authorization
  description, 1-4
  in Windows 2000 domains, 3-3
roles
  authorization method enhancements, 1-4
  authorized in Windows 2000 domains, 3-3
  creating a local database role with Oracle Administration Assistant for Windows NT, 2-18
  creating an external role with Oracle Administration Assistant for Windows NT, 2-20
  when to use enterprise roles, 1-5
  when to use external roles, 1-5

S

security groups
  accessing, 4-21
  adding or removing users, 4-23
  changing user permissions, 4-24
  SET INSTANCE command, 2-37, 2-43
  simple authentication
    using with Oracle Enterprise Security Manager, 1-8
SQL*Plus
  connecting to a database through Active Directory, 4-7, 4-19
sqlnet.ora file
  location of, 2-37, 2-39
  setting to enable Windows native authentication, 2-37, 2-39
storing private keys and trustpoints
  Oracle Wallets, 5-2
SYSDBA privileges
  connecting based on your NT local group, 2-38
connecting without a password, 1-8
granting for a single database on a computer with Oracle Administration Assistant for Windows NT, 2-24, 2-25
granting for all databases on a computer with Oracle Administration Assistant for Windows NT, 2-6, 2-7
manually granting for all databases on a computer, 2-34
mapping to a local group, 2-34
SYSOPER privileges
  connecting based on your NT local group, 2-38
  granting for a single database on a computer with Oracle Administration Assistant for Windows NT, 2-24, 2-26
  granting for all databases on a computer with Oracle Administration Assistant for Windows NT, 2-6, 2-8
  manually granting for all databases on a computer, 2-34
  mapping to a local group, 2-34
Oracle Administration Assistant for Windows NT, 2-2
required domains for Oracle clients and server to use directory server features, 4-11
role authorization, 3-3
Windows authentication protocols
default protocol used, 1-3
with Windows 2000, 1-2
with Windows NT 4.0, 1-2
Windows Explorer
  accessing directory server objects, 4-18
  integration with Oracle objects in Active Directory, 4-6
  testing database connectivity from, 4-19
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, 2-37, 2-39
  user and role requirements, 1-4
  user authentication enhancements, 1-4
  using with Oracle Enterprise Security Manager, 1-8
Windows NT 4.0 domains
  administering external users and roles manually, 2-27
  administering external users and roles with Oracle Administration Assistant for Windows NT, 2-2
  basic features, 1-4
  Windows NT local groups
    with database privileges, 1-8, 2-34, 2-40, 2-42
Windows 2000 domains
  administering external users and roles with

T
TNS_ADMIN networking parameter, A-3
troubleshooting
  Oracle Administration Assistant for Windows NT connection issues, 2-11

U
USE_SHARED_SOCKET networking parameter, A-4
user authentication
description, 1-4
users
  authentication enhancement methods, 1-4
  when to use enterprise users, 1-5
  when to use external users, 1-5

W
Wallet Resource Locator, 6-3
Windows 2000 domains
  administering external users and roles with
Windows NT 4.0 domains
  administering external users and roles with
Windows NT local groups
  with database privileges, 1-8, 2-34, 2-40, 2-42

X
X.500 naming convention, 4-16