

Oracle® Collaboration Suite

Administrator's Guide

10g Release 1 (10.1.1) for Windows or UNIX

B14476-02

September 2005

Copyright © 2003, 2005, Oracle. All rights reserved.

Primary Author: Joshua Stanley

Contributing Author: Laureen Asato, Marla Azriel, John Bassett, Ruth Baylis, Robin Clark, Ellen Desmond, Raymond Gallardo, Don Gosselin, Helen Grembowicz, Barbara Heninger, Roza Leyderman, Madhubala Mahabaleshwar, Andrew Mitchell, Richard Strohm

Contributor: Louise Avila, Tridip Bhattacharya, Attila Bodis, Marco Carrer, Marcus Chan, Will Chin, Wayne Cho, Charles Colt, Tanya Correia, Jason Davis, Ray Dutcher, Neil Evans, Natasha Fattedad, Prateek Gangwal, Meeta Gupta, Richard Hall, Cindee Kibbe, Rui Konno, Peter LaQuerre, Joseph Onorato, Deborah Owens, Julia Pond, Thomas Van Raalte, Mary Beth Roeser, Sudip Roy, Pavi Sandhu, Harry Schaefer, Richard Smith, Deborah Steiner, James Stevens, Meera Viswanathan, Derek Wichmann, David Wood, Adrian Yau

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

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065

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

Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	xxix
Audience.....	xxix
Documentation Accessibility	xxix
Related Documents	xxx
Conventions	xxxix
 What's New in Oracle Collaboration Suite Administration?	xxxiii
 Part I Getting Started	
 1 Getting Started After Installing Oracle Collaboration Suite	
Getting Started with Oracle Collaboration Suite	1-1
Set Up Operating System User Accounts	1-1
Getting Started with Oracle Content Services	1-3
Choosing Deployment Options for Oracle Content Services	1-3
Signing In to Oracle Content Services for the First Time	1-3
Creating Additional Sites.....	1-3
Designating an Administrator E-mail Address for Site Quota Notifications	1-3
Setting a Business Administrator Account for Oracle Real-Time Collaboration.....	1-4
Setting an Administrator Account for Oracle Mail and Oracle Discussions.....	1-4
Enabling Enterprise Manager Accessibility Mode	1-5
Using the Oracle Collaboration Suite Welcome Page.....	1-5
Verifying the Current Configuration	1-7
Checking Oracle Collaboration Suite Port Numbers	1-7
Verifying Portal Configuration	1-9
Verifying Oracle Discussions Configuration	1-9
Verifying Oracle Mail Configuration	1-9
Verifying Oracle Content Services Configuration.....	1-9
Verifying Oracle Calendar Configuration	1-10
Verifying Oracle Real-Time Collaboration Configuration.....	1-10
Verifying Oracle Voicemail & Fax Configuration	1-11
Configuring Oracle Voicemail & Fax.....	1-11
Verifying Oracle Mobile Collaboration Configuration.....	1-12
Verifying Oracle Workspaces Configuration.....	1-12

Setting Up the End-User Documentation Portal	1-12

2 Starting and Stopping Oracle Collaboration Suite

Overview of Starting and Stopping Oracle Collaboration Suite.....	2-2
Starting and Stopping Oracle Collaboration Suite Tiers	2-3
Starting the Infrastructure Tier	2-4
Starting the Infrastructure Using Oracle Enterprise Manager Grid Control 10g	2-5
Stopping the Infrastructure Tier	2-6
Starting an Applications Tier.....	2-7
Starting Applications Tiers Using Oracle Enterprise Manager Grid Control 10g	2-10
Stopping an Applications Tier	2-10
Starting and Stopping Oracle Collaboration Suite Database Instances.....	2-11
Starting and Stopping Individual Components.....	2-12
Starting and Stopping Using the Oracle Collaboration Suite Control	2-13
Starting and Stopping Using opmnctl.....	2-13
Starting and Stopping Oracle Calendar	2-14
Starting and Stopping Oracle Content Services.....	2-15
Starting and Stopping Oracle Content Services Node Processes on a Single Applications Tier	2-15
Starting and Stopping Oracle Content Services Node Processes Across Multiple Applications Tiers	2-15
Starting and Stopping Oracle Content Services Sub-Processes	2-16
Starting and Stopping Oracle Discussions	2-16
Starting and Stopping Oracle Mail	2-17
Starting and Stopping Oracle Mobile Collaboration	2-17
Starting and Stopping Oracle Real-Time Collaboration Components	2-18
Starting and Stopping Oracle Collaboration Suite Search	2-19
Starting and Stopping Oracle Voicemail & Fax	2-19
Starting and Stopping Oracle Workspaces	2-19
Enabling and Disabling Components.....	2-20
Starting and Stopping: Special Topics	2-20
Using opmnctl Instead of Other Command-Line Tools to Start and Stop	2-20
Starting and Stopping Log Loader	2-21
Starting and Stopping in High Availability Environments	2-21
Shutting Down Oracle Collaboration Suite Database with the IMMEDIATE Option.....	2-22

Part II Managing Oracle Collaboration Suite

3 Oracle Collaboration Suite Management Tools

Oracle Collaboration Suite Administration Tools	3-1
Introduction to Oracle Collaboration Suite Control	3-1
Introduction to Grid Control	3-2
Introduction to the Database Control Console	3-2
Introduction to Oracle Directory Manager.....	3-2
Managing Oracle Collaboration Suite from the Command Line	3-3
Using Other Tools to Monitor the Built-In Performance Metrics	3-3
Using Oracle Collaboration Suite Control Console	3-4

Introducing the Oracle Collaboration Suite Control Console Home Pages	3-5
About the Underlying Technologies of Oracle Collaboration Suite Control	3-6
Using the Oracle Collaboration Suite Control Console Online Help	3-6
Getting Started with the Oracle Collaboration Suite Control Console	3-6
Using the Oracle Collaboration Suite Farm Home Page.....	3-7
Displaying the Oracle Collaboration Suite Control Console.....	3-7
Using the Oracle Collaboration Suite Control Console URL	3-8
Displaying the Oracle Collaboration Suite Control Console from the Welcome Page	3-8
Using the Oracle Collaboration Suite Home Page	3-9
Using an Oracle Collaboration Suite Component Home Page	3-10
Monitoring and Diagnosing with the Oracle Collaboration Suite Control Console.....	3-11
Reviewing the Oracle Collaboration Suite Component Topology	3-11
Reviewing General Information and Resource Usage	3-12
Reviewing the Resources of the Host Computer	3-13
Monitoring Oracle Collaboration Suite Components.....	3-14
Displaying the All Metrics Page	3-14
Monitoring J2EE Applications	3-15
Using Grid Control to Manage Oracle Collaboration Suite	3-16
About the Components of Grid Control.....	3-17
Installing the Grid Control Components.....	3-18
Logging In to the Grid Control Console	3-18
Overview of Grid Control Monitoring Tasks	3-19
Obtaining More Information about Grid Control	3-20
Using Oracle Directory Manager to Manage Oracle Collaboration Suite	3-20
Managing Oracle Collaboration Suite from the Command Line	3-21

4 Managing Oracle Collaboration Suite Users and Groups

Introduction to the Oracle Internet Directory Provisioning Console	4-1
Provisioning Process.....	4-4
User Enrollment in Applications	4-4
Provisioning Users in Oracle Calendar	4-4
Provisioning Users in Oracle Content Services	4-5
Provisioning Users in Oracle Mail.....	4-5
Provisioning and Managing Oracle Voicemail & Fax Users	4-5
Assigning Users Administrative Roles in Oracle Real-Time Collaboration	4-5
Getting Started with the Provisioning Console	4-6
Managing User Entries Using the Provisioning Console.....	4-7
Creating Individual User Entries.....	4-8
Managing User Entries in Bulk	4-11
Modifying User Entries	4-12
Assigning Privileges to Users.....	4-13
Changing the Password of a User.....	4-14
Unlocking User Accounts	4-15
Enabling and Disabling User Accounts	4-15
De-provisioning Users from Applications	4-15
De-provisioning Users from Oracle Voicemail & Fax.....	4-17

Deleting User Accounts and Data.....	4-17
Deleting a User Account	4-17
Removing User Data from Oracle Calendar	4-18
Removing User Data from Oracle Content Services.....	4-18
Removing User Data from Oracle Mail	4-18
Removing User Data from Oracle Real-Time Collaboration	4-18
Removing User Data from Oracle Voicemail & Fax	4-18
Oracle Collaboration Suite Application-Specific User Attributes.....	4-18
Managing Group Entries Using the Provisioning Console	4-22
Creating Group Entries	4-22
Modifying Group Entries.....	4-24
Deleting Group Entries.....	4-24
Assigning Privileges to Groups	4-24
Configuring User Account Creation Using the Provisioning Console.....	4-25
Managing Oracle Collaboration Suite Application-Specific Attribute Defaults.....	4-26
Configuring the Self-Service Console for User Management.....	4-26
Setting Default Provisioning Policies	4-28
Changing the Default Password Policies	4-32
Searching for Entries Using the Provisioning Console	4-36
Searching for User Entries	4-36
Searching for Group Entries	4-37
Managing Identity Management Realms Using the Provisioning Console.....	4-37
Configuring an Identity Management Realm	4-37
Viewing Configuration Settings for an Identity Management Realm.....	4-38
Modifying Configuration Settings for an Identity Management Realm.....	4-38
Configuring the Parent Distinguished Name for Entries in a Realm.....	4-38
Creating an Additional Identity Management Realm	4-39

5 Managing Oracle Collaboration Suite Applications

Administering Oracle Collaboration Suite Components using Component Administration Tools	5-1
Oracle Calendar Administration Tools	5-2
Oracle Calendar Command-Line Utilities.....	5-2
Oracle Calendar Administrator	5-2
Oracle Mail Administration Tools	5-2
The Oracle WebMail Client	5-3
Oracle Collaboration Suite Control Console.....	5-3
Grid Control Console	5-3
Oracle Mail Command-Line Utilities.....	5-3
Oracle Content Services Administration Tools.....	5-4
Oracle Content Services Administration Mode.....	5-4
Oracle Content Services Command-Line Tools.....	5-4
Oracle Real-Time Collaboration Administration Tools.....	5-4
Oracle Real-Time Collaboration Configuration Utility	5-4
Oracle Real-Time Collaboration Web Client for Administrators	5-4
Oracle Real-Time Collaboration Monitoring Interfaces	5-5
Oracle Real-Time Collaboration Configuration Tests	5-6

Oracle Voice Mail & Fax Administration Tools.....	5-6
Oracle Mobile Collaboration Administration Tools	5-7
Overview of Typical Administration Tasks for Oracle Collaboration Suite Components.....	5-7
Oracle Calendar Administration Tasks	5-8
Monitoring	5-8
Maintenance.....	5-8
Oracle Mail Administration Tasks.....	5-8
Oracle Content Services Administration Tasks	5-9
Oracle Real-Time Collaboration Administration Tasks	5-9
Oracle Voicemail & Fax Administration Tasks.....	5-10
Oracle Mobile Collaboration Administration Tasks.....	5-10
Managing Oracle Collaboration Suite Search	5-11
Monitoring Oracle Collaboration Suite Search.....	5-13
Configuring Oracle Collaboration Suite Search	5-13
Managing Oracle Contacts	5-15
Managing Oracle Contacts Default Categories.....	5-15
Managing Oracle Contacts Maximum Entries.....	5-17
Managing Oracle Discussions	5-18
Introduction to Oracle Discussions	5-19
Oracle Discussions Integration with Oracle Mail	5-19
Multiple Oracle Mail Storage Support.....	5-20
Applications Tier Association.....	5-20
Multiple E-mail Domains	5-20
Oracle Discussions Access Control.....	5-20
Managing Oracle Discussions roles	5-23
Oracle Discussions Administration Tasks.....	5-23
Oracle Discussions Global Administration.....	5-23
Oracle Discussions Category Administration	5-24
Oracle Discussions Forum Settings	5-25
Forum Access Control.....	5-26
Message Editing and Hiding Policies	5-26
Oracle Discussions Web User Interface Defaults	5-27
Locking Oracle Discussions Message Forums and Topics	5-27
Moving Oracle Discussions Topics Across Forums.....	5-27
Clipping Oracle Discussions Topics.....	5-28
Oracle Discussions Announcements.....	5-28
Oracle Discussions Forum E-mail Integration.....	5-28
Posting Messages to a Forum Using E-mail.....	5-28
Forwarding Messages Posted Using the Oracle Discussions Web UI to E-Mail.....	5-28
Forums and Distribution Lists Integration	5-29
Accessing Oracle Discussions with RSS	5-30
Accessing Oracle Discussions using E-mail.....	5-30
Oracle Discussions Message Indexing for Search	5-30
Managing the End-User Documentation Portal	5-30
About the End-User Documentation Portal.....	5-31
Customizing the End-User Documentation Portal	5-32
Editing End-User Documentation Portal Views.....	5-34

Hiding Sections	5-35
Showing Sections	5-35
Adding a New Section	5-35
Editing a Section.....	5-36
Deleting a Section.....	5-36
Using Static Version of End-User Documentation Portal	5-37
Directory Structure of End-User Documentation Portal.....	5-37
Contents of eudp	5-37
Contents of admin.....	5-38
Contents of content.....	5-38
Contents of temp	5-38
Contents of views.....	5-38
Editing Content in End-User Documentation Portal.....	5-39
Structure of HTML Pages	5-39
Managing Oracle Application Server Portal and Oracle Collaborative Portlets	5-40
Managing Oracle Application Server Portal	5-40
Configuring OracleAS Portal After Installation	5-42
Managing Oracle Collaborative Portlets.....	5-43
Changing the Host or Port on an Applications Tier hosting Oracle Collaborative Portlets....	5-43
Configuring Oracle Collaborative Portlets with Multiple Applications Tiers.....	5-44
Using SSL in Oracle Collaborative Portlets.....	5-45
Managing Oracle Web Access Client.....	5-45
Viewing Oracle Web Access Client Performance Metrics	5-47
Managing Oracle Web Access Client System Configuration	5-47
Managing Oracle Web Access Client Default Settings	5-52
Configuring Oracle Web Access Client for Non-Single Sign-On IMAP Mode.....	5-55
Corporate Directory Searches with Oracle Web Access Client	5-56
Using an Alternate Search Base for Entries Returned by Oracle Web Access Client.....	5-58
Placing Constraints on Directory Entries Returned by Oracle Web Access Client	5-58
Managing Oracle Workspaces.....	5-59
Introduction to Oracle Workspaces.....	5-60
Oracle Workspaces Access Control	5-61
Oracle Workspaces Management Tasks	5-64
Adding Applications to your Oracle Collaboration Suite Deployment.....	5-64

6 Managing Oracle Collaboration Suite Databases

Using the Oracle Enterprise Manager 10g Database Control Console	6-2
Database Management Features	6-2
Database Control Console Online Help.....	6-2
Database Control Console Navigational Features	6-2
Starting the Database Control Console.....	6-3
Starting dbconsole in Windows	6-3
Accessing the Database Control Console	6-4
Administering Database Users	6-5
Creating Database Users	6-6
Using a Shortcut to Create Database Users	6-8

Editing Database Users	6-8
Unlocking Database Accounts and Resetting Passwords.....	6-9
Granting Database Roles.....	6-9
Revoking Database Roles.....	6-9
Dropping Database Users	6-10
Granting Database Control Administrative Privileges	6-10
Setting Up Database Control Preferences	6-10
Defining Database Alert Blackout Time Periods	6-11
Setting Database Preferred Credentials	6-11
SQL Statements and Other Management Tools: SQL*Plus and iSQL*Plus	6-12
Starting SQL*Plus.....	6-12
Starting iSQL*Plus.....	6-13
Starting and Stopping the Oracle Collaboration Suite Database	6-13
Options for Starting Up Oracle Collaboration Suite Database.....	6-14
Starting Up a Database Using Grid Control	6-14
Starting Up a Database using the Database Control Console	6-14
Starting Up a Database Using SQL*Plus	6-15
Starting Up a Database Using Recovery Manager	6-15
Preparing to Start an Oracle Collaboration Suite Database Instance	6-15
Using SQL*Plus to Start Up an Oracle Collaboration Suite Database.....	6-15
Scenarios for Starting a Oracle Collaboration Suite Database Instance	6-17
Starting an Instance, and Mounting and Opening a Database	6-17
Starting an Instance Without Mounting a Database.....	6-17
Starting an Instance and Mounting a Database.....	6-18
Restricting Access to an Instance at Startup	6-18
Forcing an Instance to Start	6-19
Starting an Instance, Mounting a Database, and Starting Complete Media Recovery..	6-19
Automatic Database Startup at Operating System Start	6-19
Starting Remote Instances.....	6-19
Altering Oracle Collaboration Suite Database Availability	6-20
Mounting a Database to an Instance	6-20
Opening a Closed Database	6-20
Opening a Database in Read-Only Mode.....	6-20
Restricting Access to an Open Database.....	6-21
Options for Shutting Down an Oracle Collaboration Suite Database.....	6-21
Shutting Down a Database Using Grid Control.....	6-21
Shutting Down a Database using the Database Control Console.....	6-21
Shutting Down a Database Using Recovery Manager	6-22
Shutting Down a Database Using SQL*Plus.....	6-22
Shutting Down an Oracle Collaboration Suite Database with the NORMAL Clause	6-22
Shutting Down an Oracle Collaboration Suite Database with the IMMEDIATE Clause....	6-22
Shutting Down an Oracle Collaboration Suite Database with the TRANSACTIONAL Clause	6-23
Shutting Down an Oracle Collaboration Suite Database with the ABORT Clause.....	6-23
Viewing Listener Configuration	6-24
Starting up and Shutting Down the Listener	6-24
Managing Oracle Collaboration Suite Database Structures	6-24

Exploring the Storage Structure of Your Database	6-24
Control File	6-25
Redo Log Files	6-26
Multiplexing the Redo Log.....	6-26
Archive Log Files	6-27
Rollback Segments	6-27
Tablespaces	6-27
Tablespaces Page	6-28
Some Tablespaces in the Database	6-28
Temporary Tablespace Groups.....	6-29
Datafiles.....	6-29
Other Storage Structures	6-29
Initialization Parameter File	6-29
Password File	6-30
Backup Files.....	6-30
Common DBA Tasks for Managing Database Storage.....	6-30
Viewing Tablespaces in Your Database.....	6-30
Modifying a Tablespace	6-30
Dropping a Tablespace.....	6-31
Reclaiming Wasted Space	6-31
Using the Segment Advisor	6-31
Shrinking Database Objects.....	6-32
Managing Undo for Your Database	6-32
About Undo	6-33
Undo Tablespace Size and Retention Time.....	6-33
Automatic Undo Management	6-34
Undo Management with Database Control.....	6-34
Using Oracle Recommendations for Managing Undo	6-35
Extending the Undo Tablespace.....	6-35
Using the Undo Advisor.....	6-35
Setting New Threshold Undo Retention Time	6-36
Viewing and Modifying Initialization Parameters	6-36
Managing Memory Parameters	6-38
Modifying Memory Parameters.....	6-38
Managing the OracleAS Metadata Repository.....	6-38
Frequently Asked Questions About OracleAS Metadata Repository	6-39
Viewing OracleAS Metadata Repository Schema Passwords	6-41
Viewing OracleAS Metadata Repository Schema Passwords using Oracle Directory Manager 6-41	
Viewing OracleAS Metadata Repository Schema Passwords using ldapsearch.....	6-42
Changing OracleAS Metadata Repository Schema Passwords.....	6-42
Changing Schema Passwords using the Oracle Collaboration Suite Control.....	6-45
Changing Schema Passwords using SQL*Plus.....	6-45
Changing Schema Passwords in Oracle Internet Directory	6-46
Changing the Character Set of OracleAS Metadata Repository	6-46
Renaming and Relocating OracleAS Metadata Repository Datafiles	6-47
Changing Oracle Collaboration Suite Schema Passwords	6-49
Changing the Oracle Calendar Schema Password.....	6-50

Changing the Oracle Content Services Schema Password	6-50
Changing the Oracle Mail Schema Password	6-51
Changing the Oracle Real-Time Collaboration Schema Password.....	6-52
7 Managing Oracle Collaboration Suite Infrastructure	
Setting Up and Enabling Multiple Realms	7-1
How the Single Sign-On Server Enables Authentication to Multiple Realms	7-2
Locating Realms in Oracle Internet Directory	7-2
Validating Realm-Affiliated Users to Partner Applications	7-3
Configuring the Single Sign-On Server for Multiple Realms	7-4
Granting Administrative Privileges for Multiple Realms	7-7
Managing the Oracle Internet Directory Service Registry	7-7
Introduction to the Oracle Internet Directory Service Registry	7-7
URIs Recorded in the Oracle Internet Directory Service Registry	7-8
Using Oracle Directory Manager to Edit the Oracle Internet Directory Service Registry....	7-10
8 Managing Oracle Collaboration Suite Log Files	
Introduction to Oracle Collaboration Suite Logging	8-1
Understanding Log File Data and Naming.....	8-2
ODL Message Formatting and ODL Log File Naming	8-2
Using a Log Repository	8-2
Configuring Component Logging Options	8-3
Listing and Viewing Log Files with Oracle Collaboration Suite Control	8-3
Listing Log Files for Components.....	8-4
Listing Log Files from Oracle Collaboration Suite Components Pages	8-4
Using Log Files Advanced Search	8-5
Searching Diagnostic Messages in a Log Repository	8-6
Getting Started with Log Repository	8-6
Searching Log Repository with Simple Search	8-6
Searching Log Repository with Advanced Search	8-7
Viewing Repository Log Entry Details	8-8
Using Regular Expressions With Log Repository Search	8-9
Diagnosing Problems and Correlating Messages	8-9
Correlating Messages Across Log Files and Components.....	8-10
Diagnosing Component Problems.....	8-11
Using Oracle Collaboration Suite Log Loader	8-11
Starting and Stopping Log Loader	8-12
Enabling and Disabling Log Loader.....	8-12
Updating the Log Configuration	8-12
Setting Log Loader Properties.....	8-13
Understanding Log Loader Diagnostic Messages.....	8-14
Advanced Logging Topics	8-14
Using the printlogs Tool to View Log Messages	8-15
Understanding ODL Messages and ODL Log Files.....	8-15
ODL Message Contents.....	8-15
ODL Log File Naming.....	8-17

Understanding Log Loader Log File Format Conversion.....	8-18
Component Diagnostic Log File Registration.....	8-18
Configuring Components to Produce ODL Messages and ECIDs	8-19
Configuring Oracle HTTP Server to Produce ODL Messages	8-20
Configuring OC4J to Produce ODL Messages.....	8-20
Configuring OC4J to Produce ECIDs.....	8-20
Creating and Managing a Diagnostic Message Database Repository.....	8-21
Limitations and Configuration.....	8-23

9 Managing Microsoft Active Directory Integration

Concepts and Architecture of Microsoft Active Directory Integration	9-1
Components for Integrating with Microsoft Active Directory.....	9-2
How Oracle Directory Integration and Provisioning Maintains Synchronization.....	9-5
Oracle Internet Directory Schema Elements for Integration with Microsoft Active Directory	9-7
Directory Information Tree in an Integration with Microsoft Active Directory.....	9-7
About Realms in Oracle Internet Directory	9-7
Planning the Deployment.....	9-9
Example: Integration with a Single Microsoft Active Directory Domain Controller	9-10
Example: Integration with Multiple Microsoft Active Directory Domain Controllers .	9-11
Deployment Options for Integrating with Microsoft Active Directory	9-13
Deployments with Oracle Internet Directory as the Central Directory	9-13
Deployments with Microsoft Active Directory as the Central Directory	9-14
Configuration of Integration with Microsoft Active Directory	9-16
Configuring the Realm	9-16
Configuring Synchronization Profiles	9-17
About the Sample Synchronization Profiles	9-17
Creating Synchronization Profiles.....	9-18
Configuring the Connection Details for Microsoft Active Directory	9-18
Customizing Mapping Rules	9-19
Customizing the LDAP Schema	9-21
Customizing the Search Filter to Get Information from Microsoft Active Directory	9-22
Synchronizing Deletions from Microsoft Active Directory	9-23
Synchronizing Passwords.....	9-23
Customizing Access Control Lists	9-24
Customizing ACLs for Import Profiles.....	9-24
Customizing ACLs for Export Profiles	9-25
ACLs for Other Oracle Components.....	9-25
Configuring the Active Directory Connector for Synchronization in SSL Mode	9-26
Considerations for Synchronizing with a Multiple-Domain Microsoft Active Directory Environment	9-26
Configuring the Active Directory Connector Profiles	9-27
Preparing for Synchronization.....	9-28
Creating Synchronization Profiles with Express Configuration.....	9-29
Understanding Express Configuration.....	9-29
Running Express Configuration.....	9-30
Additional Synchronization Considerations	9-32

Customizing Attribute Mapping	9-33
Final Configuration Requirements	9-33
Customizing DN Mapping Rules	9-33
Synchronizing Multiple Domains	9-34
Performing Initial Bootstrapping	9-35
Granting Privileges to Non-Default Realms	9-35
Configuring Synchronization Profiles for SSL	9-35
Additional Considerations	9-35
Configuring the Active Directory External Authentication Plug-in	9-36
Installing Active Directory External Authentication Plug-ins	9-36
Enabling the Active Directory External Authentication Plug-ins	9-37
Testing the Active Directory External Authentication Plug-ins	9-37
Configuring Windows Native Authentication	9-38
System Requirements	9-38
Configuration Tasks	9-38
Fallback Authentication	9-42
Login Scenarios	9-43
Configuring Synchronization of Oracle Internet Directory Foreign Security Principal References with Microsoft Active Directory 9-44	
Tasks to Resolve Foreign Key References	9-44
Managing Integration with Microsoft Active Directory	9-47
Tasks After Configuring with Microsoft Active Directory	9-47
Typical Management of Integration with Microsoft Active Directory	9-47
Bootstrapping Data Between Directories	9-48
Managing the Active Directory External Authentication Plug-in	9-49
Deleting the Active Directory External Authentication Plug-in	9-49
Disabling the Active Directory External Authentication Plug-in	9-49
Re-Enabling the Active Directory External Authentication Plug-in	9-49
Switching to a Different Microsoft Active Directory Domain Controller in the Same Domain 9-50	

10 Monitoring and Tuning Oracle Collaboration Suite Performance

Performance Tuning Oracle Collaboration Suite	10-1
Tuning Oracle Calendar	10-1
Tuning Oracle Discussions	10-1
Oracle Internet Directory Connection Parameters	10-2
Database Connection Parameters	10-2
Oracle Discussions Caches	10-2
Oracle Discussions Logs	10-3
Tuning Oracle Mail	10-4
Overview of the Oracle Mail Architecture	10-4
Understanding the Breakdown of Costs	10-6
Recommended Database Connection Settings	10-7
Recommended LDAP Connection Settings	10-7
Oracle Mail Parameter Recommendations	10-7
Recommended Database Process Parameter Settings	10-9
Monitoring CPU Usage for Oracle WebMail	10-9

Monitoring JavaMail API Response Time for Oracle WebMail.....	10-9
Determining the Optimum Database Pool Size for Oracle WebMail.....	10-10
Oracle WebMail Parameter Recommendations	10-10
Tuning Oracle Content Services.....	10-12
Tuning Oracle Ultra Search	10-12
Tuning Oracle Application Server Portal	10-12
Tuning Oracle Real-Time Collaboration.....	10-12
Increasing Conference Server and Listening Processes	10-12
Increasing Messaging Connections	10-13
Increasing the Number of Open File Descriptors Used for Client Connections	10-13
Tuning Oracle Voicemail & Fax	10-14
Tuning Oracle Mobile Collaboration	10-14
Tuning Oracle Workspaces.....	10-15
Adjusting Oracle Workspaces Sizing.....	10-15
Database Connection Pool Size	10-15
LDAP Connection Pool Size.....	10-15
Discussions Service Connection Pool Size	10-16
Discussions Service on Behalf of Inbox Connection Pool Size.....	10-16
Adjusting Oracle Workspaces Performance	10-16
Database Connection Pool Wait Timeout	10-16
Database Connection Pool Inactivity Timeout.....	10-16
Calendar User Connection Pool	10-16
Calendar Connection Pool Blocking	10-17
Oracle Calendar Master Node Connection	10-17
JDBC Statement Caching	10-17
Workspaces Log Level	10-17
Investigating Oracle Workspaces Performance.....	10-17
Monitoring and Tuning the Oracle Collaboration Suite Database	10-19
Proactive Database Monitoring.....	10-19
Alerts.....	10-19
Performance Self-Diagnostics: Automatic Database Diagnostics Monitor	10-20
Monitoring General Database State and Workload	10-20
Managing Alerts.....	10-21
Viewing Metrics and Thresholds	10-21
Setting Metric Thresholds.....	10-23
Setting up Notification	10-25
Responding to Alerts.....	10-25
Clearing Alerts	10-26
Diagnosing Performance Problems	10-26
Viewing Performance Analysis.....	10-26
Responding to Performance Findings	10-26
Modifying Default ADDM Behavior	10-27
Running ADDM Manually	10-27
Using Advisors to Optimize Database Performance	10-28
About Performance Advisors.....	10-28
About the SQL Tuning Advisor.....	10-29
About the SQL Access Advisor.....	10-30

Using the Memory Advisor.....	10-30
11 Backing Up and Recovering Oracle Collaboration Suite	
Oracle Collaboration Suite Backup and Recovery Strategy	11-1
Basics of Backup and Recovery	11-1
Oracle Collaboration Suite Backup and Recovery Roadmap	11-2
Oracle Collaboration Suite Backup and Recovery Using Recovery Manager (RMAN) and Other Customized Scripts	11-3
Assumptions and Restrictions for all Oracle Collaboration Suite Backup and Recovery Operations	11-3
Understanding Database Backup and Recovery	11-3
Types of Database Backup	11-4
Types of Database Recovery	11-5
Oracle Database Backup Methodology	11-6
Enabling ARCHIVELOG Mode	11-6
Performing Cold Database Backups.....	11-8
Performing Online Database Backups	11-8
Part III Reconfiguring Oracle Collaboration Suite	
12 Changing Infrastructure Services	
Overview of Procedures for Changing Infrastructure Services	12-1
Changing the Oracle Internet Directory or HTTP (SSO) Ports on Identity Management.....	12-3
Changing Oracle Internet Directory from Dual Mode to SSL Mode.....	12-3
Moving Identity Management to a New Host.....	12-6
Sample Uses for this Procedure	12-6
Assumptions and Restrictions.....	12-6
Overview	12-7
Procedure	12-9
Strategy for Performing Failover with this Procedure	12-12
Changing the OracleAS Metadata Repository Used by an Applications Tier	12-13
Sample Uses for this Procedure	12-13
Assumptions and Restrictions.....	12-13
Overview	12-14
Procedure	12-17
About LDAP-based Replicas	12-25
What is an LDAP-based Replica?	12-25
How is the LDAP-based Replica Used for Changing Infrastructure Services?	12-26
Installing and Setting Up an LDAP-Based Replica.....	12-27
Things to Know Before You Start	12-27
Procedure	12-27
Applications Tier Application Reconfiguration	12-28
Oracle Calendar Re-association	12-28
Oracle Real-Time Collaboration Re-association	12-29

13 Managing High-Availability Environments

Adding and Removing RAC nodes	13-1
Overview of Node Addition Procedures.....	13-1
Step 1: Connecting New Nodes to the Cluster	13-2
Making Physical Connections	13-2
Installing Operating System	13-2
Creating Oracle Users.....	13-2
Checking the Installation	13-3
Step 2: Extending Clusterware and Oracle Software to New Nodes	13-3
Adding Nodes at the Vendor Clusterware Layer (UNIX Only)	13-3
Adding Nodes at the Oracle Clusterware Layer (UNIX and Windows).....	13-4
Step 3: Preparing Storage for RAC on New Nodes.....	13-6
Raw Device Storage Preparation for New Nodes.....	13-6
Step 4: Adding Nodes at the Oracle RAC Database Layer	13-8
Step 5: Adding Database Instances to New Nodes	13-10
Updating Path Environment Variables on New Nodes on Windows-Based Systems	13-12
Connecting to iSQL*Plus after Adding a Node on Windows-Based Platforms	13-12
Adding Nodes that Already Have Clusterware and Oracle Software to a Cluster	13-12
Adding a Node on a Shared Oracle Home	13-13
Deleting Instances from Real Application Clusters Databases	13-13
Deleting Nodes from Oracle Clusters on UNIX-Based Systems	13-14
ASM Instance Clean-Up Procedures for Node Deletion.....	13-15
Deleting Nodes from Oracle Clusters on Windows-Based Platforms	13-16
ASM Instance Cleanup Procedures after Node Deletion on Windows-Based Platforms	13-17
Adding or Deleting Nodes from Oracle Collaboration Suite Database.....	13-17
Step 1: Modify the RAC Database Connect String in Oracle Internet Directory	13-17
Step 2: Modify the Crawler's Connect String Through the Search Admin Application.....	13-18
Step 3: Bounce the Oracle Collaboration Suite Applications Tier Processes.....	13-18
Removing Nodes from Oracle Collaboration Suite Applications	13-19
Configuring Manual Cold Failover for Oracle Calendar Server	13-19
Starting and Stopping Oracle Collaboration Suite in a High-Availability Environment	13-19
Stopping Oracle Collaboration Suite.....	13-20
Starting Oracle Collaboration Suite	13-20

14 Changing Oracle Collaboration Suite Network Configurations

Introduction to Changing Oracle Collaboration Suite Ports	14-1
Viewing Port Numbers.....	14-2
Changing Applications Tier Ports.....	14-2
Changing Oracle Enterprise Manager Ports	14-3
Changing OC4J Ports.....	14-4
Changing the Oracle HTTP Server Listen Port.....	14-6
Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 on UNIX Systems	14-6
Using the portconfig Command to Change the Oracle HTTP Server Listen Port	14-6
Changing the OracleAS Web Cache Listen Port	14-10
Changing the OracleAS Web Cache Administration Port	14-16

Changing the OracleAS Web Cache Invalidation Port.....	14-17
Changing the OracleAS Web Cache Statistics Port.....	14-18
Changing the DCM Discovery Port.....	14-18
Changing the Java Object Cache Port	14-19
Changing the Log Loader Port.....	14-19
Changing OPMN Ports (ONS Local, Request, and Remote)	14-19
Changing the Oracle HTTP Server Diagnostic Port.....	14-20
Changing the Port Tunneling Port	14-21
Changing OracleAS Portal Ports.....	14-21
Changing Oracle Mobile Collaboration Ports.....	14-21
Specifying Ports for DMS-Monitored Services	14-21
Changing Infrastructure Ports	14-22
Changing the OracleAS Metadata Repository Net Listener Port	14-22
Changing the KEY value for an IPC Listener	14-26
Changing Oracle Internet Directory Ports.....	14-27
Changing the HTTP Server Port on Identity Management	14-30
Changing a Hostname, Domain Name, or IP Address.....	14-36
Changing the Hostname or Domain Name of an Applications Tier Installation.....	14-36
Changing the Hostname, Domain Name, or IP Address of an Infrastructure Installation	14-40
Changing the IP Address of an Infrastructure Tier.....	14-46
Special Topics for Changing Your Hostname or Domain Name	14-48
Setting the Log Level for chgiphost.....	14-48
Customizing the chgiphost Script	14-49
Changing your Hostname after Upgrading from Windows 2000 to Windows 2003 ..	14-50
Recovering from Errors When Changing Your Hostname.....	14-50

15 Customizing Oracle Collaboration Suite

Customizing Default Logos	15-1
Replacing the Default Logo on the Oracle Collaboration Suite Portal Home Page	15-1
Customizing the Oracle WebMail Logo	15-2
Customizing the Oracle Calendar Logo	15-2
Customizing the Oracle Web Conferencing Logo.....	15-3
Customizing the Oracle Mobile Collaboration & Voice Logo.....	15-4
Customizing Colors and Fonts	15-4
Changing the Default Colors and Fonts on the Oracle Collaboration Suite Portal Home Page	15-5
Customizing Oracle WebMail Colors and Fonts.....	15-5
Customizing Oracle Calendar Colors and Fonts.....	15-5
Customizing Oracle Web Conferencing Colors and Fonts	15-6
Customizing Oracle Mobile Collaboration & Voice Colors and Fonts	15-6
Changing the Look and Feel of the Provisioning Console.....	15-6
Customizing Oracle Content Services.....	15-7
Customizing Oracle Real-Time Collaboration	15-7
Customizing and Extending Oracle Web Access Client	15-7
General Notes on Customizing Oracle Web Access Client.....	15-8
Customizing Oracle Web Access Client Skins	15-8
Setup	15-8

Customizing.....	15-8
styles.css	15-8
Icon Images	15-9
Deployment	15-9
User Configuration	15-9
Customizing Oracle Web Access Client Menu Sets	15-9
Setup	15-9
Customizing.....	15-9
Exiting Menu Items	15-10
Custom Menu Items	15-10
Custom Font List for the Rich Text Editor	15-10
Deployment	15-11
User Configuration	15-11
Customizing Oracle Web Access Client Resource Bundles.....	15-11
Setup	15-11
Customizing.....	15-11
Deployment	15-12
User Configuration	15-12
Popping Up Oracle Web Access Client Windows	15-12
Extended Composer API	15-13
Populating a Compose Window Opened from the Main Window	15-14
Warnings	15-14
Sample Extension Code.....	15-15
Receiving Data using Custom Items in Context Menus.....	15-16

Part IV Appendixes

A Default Port Numbers and Ranges

Oracle Application Server Ports	A-1
J2EE and OracleAS Web Cache Ports.....	A-2
Portal and Oracle Mobile Collaboration Ports.....	A-3
Infrastructure Ports.....	A-4
OracleAS Integration InterConnect Ports	A-4
Oracle Enterprise Manager Grid Control 10g Ports	A-5
Oracle Calendar Ports	A-5
Oracle Content Services Ports.....	A-6
Oracle Real-Time Collaboration Ports	A-7
Oracle Voicemail & Fax Ports.....	A-7
Port Numbers (Sorted by Port Number)	A-8

B Default Locations of Component Log Files

Oracle Calendar Logs.....	B-1
Oracle Content Services Logs	B-1
Oracle Mail Logs.....	B-2
Oracle Mobile Collaboration Logs.....	B-2
Oracle Real-Time Collaboration Logs	B-3

Oracle Voicemail & Fax Logs	B-4

C User Provisioning Java API

Application Configuration	C-1
Application Registration and Provisioning Configuration.....	C-1
Application Registration	C-1
Provisioning Configuration.....	C-3
Application Identity Information	C-6
Application Identity Realm Information.....	C-6
Application Provisioning and Default Policy	C-6
Application User Data Location	C-7
Event Interface Configuration	C-7
Application User Attribute and Defaults Configuration.....	C-9
Application Provisioning Plug-in Configuration	C-10
Application Propagation Configuration	C-11
Application Event Propagation Run Time Status.....	C-12
Application Configuration Classes.....	C-13
User Management	C-13
UserFactoryBuilder and UserFactory.....	C-13
UserFactoryControl	C-14
Creating a User	C-14
Modifying a User.....	C-15
Deleting a User	C-15
Looking Up a User	C-15
Debugging	C-16
Sample Code	C-16
Java Plug-ins for User Provisioning	C-17
Plug-in Types and Their Purpose	C-17
Plug-in Requirements	C-18
Data Entry Plug-in	C-18
Pre-Data-Entry Plug-in	C-20
Post-Data-Entry Plug-in	C-21
Data Access Plug-in	C-21
Plug-in Return Status.....	C-22
Configuration Template	C-23
Sample Code	C-24

Glossary

Index

List of Examples

1-1	Sample portlist.ini Contents	1-7
8-1	Sample ODL Message Content	8-15
9-1	Example of Distinguished Name Mapping	9-19
9-2	Example of One-to-One Distinguished Name Mapping	9-20
9-3	Attribute-Level Mapping for the User Object.....	9-20
9-4	Attribute-Level Mapping for the Group Object	9-21
9-5	How Foreign Key References Are Resolved	9-44
12-1	Example ccf.sql File after Edits	12-22
12-2	Reassociating Calendar with a new Collaboration Suite Database	12-29
15-1	Sample Extension Code	15-15

List of Figures

1-1	Oracle Collaboration Suite Welcome Page.....	1-6
3-1	The Oracle Collaboration Suite Farm Home Page	3-7
3-2	Oracle Collaboration Suite home page	3-9
3-3	Topology Viewer.....	3-12
3-4	General Section of the Oracle Collaboration Suite Home Page	3-12
3-5	System Components Table on the Oracle Collaboration Suite Home Page.....	3-13
3-6	General Information and Load Statistics on the Host Home Page.....	3-14
3-7	Disk Space Usage Chart Available from the Host Home Page.....	3-14
3-8	Infrastructure All Metrics Page.....	3-15
3-9	List of Applications on the J2EE Applications Page	3-16
3-10	Grid Control Console Home Page.....	3-19
4-1	Interactions of Oracle Internet Directory Self-Service Console with Oracle Delegated Administration Services 4-3	
4-2	Oracle Internet Directory Provisioning Console	4-7
4-3	Provisioning Console Create User: General Window	4-8
4-4	Provisioning Console Create User: Application Provisioning Window	4-9
4-5	Provisioning Console Create User: Application Attributes Window	4-10
4-6	Provisioning Console Create User: Review Window	4-11
4-7	Provisioning ConsoleEdit User: Application Provisioning Window.....	4-16
4-8	Accessing Oracle Internet Directory with Oracle Directory Manager	4-33
4-9	Password Policy Management in Oracle Internet Directory	4-34
5-1	Oracle Real-Time Collaboration Tabs and Administrator Levels.....	5-5
5-2	Accessing Oracle Internet Directory with Oracle Directory Manager	5-16
5-3	The End-User Documentation Portal.....	5-32
5-4	End-User Documentation Portal Views page.....	5-33
5-5	End-User Documentation Portal Edit View page	5-34
5-6	End-User Documentation Portal - Editing a section.....	5-36
5-7	Oracle Collaboration Suite Control - Main OracleAS Portal Monitoring Page	5-41
5-8	Oracle Collaboration Suite Control - Oracle Web Access Client Control Page	5-46
5-9	Oracle Web Access Client Performance Metrics	5-47
5-10	Oracle Web Access Client System Configuration	5-51
5-11	Oracle Web Access Client Default Settings.....	5-54
6-1	Database Home Page Navigational Property Pages.....	6-2
6-2	Database Home Page Drill Down Link	6-3
6-3	Database Home Page Related Links	6-3
6-4	Database Home Page.....	6-5
6-5	Database Users Page.....	6-6
6-6	Create User General Page	6-7
6-7	Storage Options	6-25
6-8	Database Administration Page	6-37
7-1	The Big Picture: Single Sign-On in Multiple Realms	7-3
7-2	mod_osso Headers for Users with the Same Name.....	7-4
7-3	Accessing Oracle Internet Directory with Oracle Directory Manager	7-11
7-4	Displaying the Service Registry with Oracle Directory Manager.....	7-12
7-5	Oracle Calendar OCAL Virtual Services Object in the Service Registry	7-13
8-1	Oracle Collaboration Suite Control Console View Logs Search Results	8-4
8-2	Log Files Advanced Search Filter By Log File Attributes	8-5
8-3	Search Log Repository Page	8-7
8-4	Search Log Repository Advanced Search Filter By Log Entry Fields	8-8
8-5	Log Repository Log Entry Details Page.....	8-9
8-6	Log Loader Properties Page	8-13
9-1	Flow for Windows Native Authentication.....	9-5
9-2	The Default Identity Management Realm.....	9-8
9-3	Default DIT Structures in Oracle Internet Directory and Active Directory When Both	

	Directory Hosts Are Under the Domain us.MyCompany.com	9-10
9-4	Example of a Mapping Between Oracle Internet Directory and Multiple Domains in Microsoft Active Directory	9-11
9-5	Mapping Between Oracle Internet Directory and a Forest in Microsoft Active Directory	9-12
10-1	Oracle Mail Processes	10-5
10-2	All Metrics Page	10-22
10-3	Alerts Section of Database Home Page.....	10-23
10-4	Edit Thresholds Page.....	10-24
10-5	Performance Analysis	10-26
10-6	Create ADDM Task	10-28
10-7	Buffered Cache Size Advice	10-31
12-1	Oracle Collaboration Suite Control Console Infrastructure Page.....	12-2
12-2	Original Host (Master) and New Host (Replica).....	12-8
12-3	Changing from Original to New Identity Management	12-9
12-4	Original OracleAS Metadata Repository	12-14
12-5	Original OracleAS Metadata Repository and New OracleAS Metadata Repository...	12-15
12-6	Changing from the Original to the New OracleAS Metadata Repository.....	12-16
12-7	LDAP-based Replica Environment	12-26
C-1	The Directory Information Tree for Provisioning Configuration Data	C-5

List of Tables

1-1	Oracle Collaboration Suite Environment Variables for UNIX	1-2
1-2	Oracle Collaboration Suite Environment Variables for Windows	1-2
1-3	Expected Oracle Content Services Basic Functionality	1-10
1-4	Required Oracle Voicemail & Fax Services	1-11
3-1	Summary of the Oracle Collaboration Suite Control Underlying Technologies	3-6
4-1	User Privileges	4-13
4-2	Oracle Calendar User Attributes	4-19
4-3	Oracle Mail User Attributes	4-20
4-4	Oracle Voicemail & Fax User Attributes	4-21
4-5	Group Privileges	4-24
4-6	Oracle Collaboration Suite Application Provisioning Plug-in Implementation	4-29
4-7	Provisioning Subscription Tool Parameters	4-30
4-8	Fields in the Password Policies General Tab Page	4-34
4-9	Fields in the Password Policies Account Lockout Tab Page	4-36
4-10	Fields in the Password Policies IP Lockout Tab Page	4-36
4-11	Fields in the Password Policies Password Syntax Tab Page	4-36
5-1	Oracle Discussions Role Permissions	5-22
5-2	Forum Message Editing and Hiding Policies	5-26
5-3	Oracle Web Access Client System Configuration Parameters	5-48
5-4	Oracle Web Access Client Default Settings Parameters	5-52
5-5	Oracle Workspaces Workspace Management	5-61
5-6	Oracle Workspaces Membership Management	5-62
5-7	Oracle Workspaces Template Management	5-62
5-8	Oracle Workspaces Application Management	5-62
5-9	Oracle Content Services Access in Oracle Workspaces	5-62
5-10	Oracle Calendar Access in Oracle Workspaces	5-62
5-11	Oracle Discussions Access in Oracle Workspaces	5-63
5-12	Oracle Workspaces Support for Oracle Collaboration Suite Web Client Access	5-63
6-1	Tablespaces and Descriptions	6-28
6-2	Methods for Changing OracleAS Metadata Repository Schema Passwords	6-43
7-1	Parameters for enblhstg.csh and addsub.csh	7-6
7-2	URIs Recorded in the Oracle Internet Directory Service Registry	7-8
8-1	Oracle Collaboration Suite Components Supporting Message Correlation	8-10
8-2	ODL Format Message Header Fields	8-16
8-3	Component IDs For Diagnostic Log File Configuration	8-19
8-4	Oracle Application Server Components with Configuration Options for Supporting ODL..	8-20
9-1	Comparing the DirSync Approach to the USN-Changed Approach	9-6
9-2	Typical Requirements with Oracle Internet Directory as the Central Directory	9-14
9-3	Typical Requirements with Microsoft Active Directory as the Central Directory	9-15
9-4	Arguments for the Directory Integration and Provisioning Express Configuration Tool	9-31
9-5	Single Sign-On Login Options in Internet Explorer	9-43
10-1	Oracle Mail Processes	10-4
10-2	Parameter Recommendations for Oracle Mail	10-8
10-3	Database Process Parameter Recommendations for Oracle Mail	10-9
10-4	Parameter Recommendations for Oracle WebMail	10-10
10-5	Performance Advisors	10-29
10-6	Other Advisors	10-29
14-1	Changing Oracle Collaboration Suite Control Ports Using the emctl Command Line	14-4
14-2	Arguments for the portconfig Command	14-7
14-3	Supported Procedures for Hostname, Domain Name, and IP Address Changes	14-36
14-4	Prompts and Actions for chgiphost -mid	14-38

14-5	Prompts and Actions for chgiphost -idm	14-42
14-6	Log Levels Supported for chgiphost	14-49
15-1	Extended Composer API Parameters	15-13
15-2	dataKey Key Names	15-14
A-1	J2EE and Web Cache Ports	A-2
A-2	Portal and Oracle Mobile Collaboration Ports.....	A-3
A-3	Infrastructure Ports.....	A-4
A-4	OracleAS Integration InterConnect Ports.....	A-5
A-5	Oracle Enterprise Manager Grid Control 10g Ports.....	A-5
A-6	Oracle Calendar Server Ports	A-5
A-7	Oracle Content Services Ports	A-6
A-8	Oracle Real-Time Collaboration Ports	A-7
A-9	Oracle Voicemail & Fax Ports.....	A-7
A-10	Port Numbers (Sorted by Port Number)	A-8
B-1	Oracle Calendar Log Files.....	B-1
B-2	Oracle Content Services Log Files	B-1
B-3	Oracle Mail Log File Directories	B-2
B-4	Oracle Mobile Collaboration and Oracle Wireless Log Files.....	B-2
B-5	Oracle Real-Time Collaboration Log File Directories.....	B-3
B-6	Oracle Voicemail & Fax Log Files.....	B-4
C-1	Some Useful Privilege Groups	C-3
C-2	Interfaces and Their Configuration	C-7
C-3	Information Formats Supported by the PLSQL Interface.....	C-8
C-4	Properties Stored as Attributes in the Attribute Configuration Entry	C-10
C-5	Event propagation parameters.....	C-11

Preface

Oracle Collaboration Suite is an integrated suite of software applications designed to enable communication, messaging, and content sharing in an enterprise environment.

Audience

This manual is intended for administrators of Oracle Collaboration Suite. It describes how to perform all of the typical administrative tasks relating to maintenance, user service, provisioning, updating, monitoring performance, and ordinary modifications of Oracle Collaboration Suite and its various components. Where appropriate, this manual references Administrator's Guides for individual Oracle Collaboration Suite components.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility 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 more information, visit the Oracle Accessibility Program Web site at

<http://www.oracle.com/accessibility/>

Accessibility of Code Examples in Documentation

Screen readers 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, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see these Oracle resources:

Oracle Collaboration Suite

- *Oracle Collaboration Suite Release Notes for Solaris Operating System*
- *Oracle Collaboration Suite Release Notes for Microsoft Windows*
- *Oracle Collaboration Suite Release Notes for Linux*
- *Oracle Collaboration Suite Release Notes for hp-ux*
- *Oracle Collaboration Suite Release Notes for AIX Based Systems*
- *Oracle Collaboration Suite Deployment Guide*
- *Oracle Collaboration Suite Installation Guide for Microsoft Windows*
- *Oracle Collaboration Suite Installation Guide for Solaris Operating System*
- *Oracle Collaboration Suite Installation Guide for Linux*
- *Oracle Collaboration Suite Installation Guide for hp-ux*
- *Oracle Collaboration Suite Installation Guide for AIX Based Systems*
- *Oracle Collaboration Suite Oracle Voicemail & Fax and Oracle Web Conferencing Conversion Servers Installation and Upgrade Guide for Microsoft Windows*
- *Oracle Collaboration Suite Upgrade Guide*
- *Oracle Collaboration Suite Security Guide*
- *Oracle Collaboration Suite Migration and Coexistence Guide*
- *Oracle Calendar Administrator's Guide*
- *Oracle Content Services Administrator's Guide*
- *Oracle Content Services Application Administrator's Guide*
- *Oracle Mail Administrator's Guide*
- *Oracle Mobile Collaboration Administrator's Guide*
- *Oracle Real-Time Collaboration Administrator's Guide*
- *Oracle Voicemail & Fax Administrator's Guide*

Oracle Application Server

- *Oracle Application Server Concepts*
- *Oracle Application Server Administrator's Guide*
- *Oracle HTTP Server Administrator's Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Process Manager and Notification Server Administrator's Guide*
- *Oracle Application Server Single Sign-On Administrator's Guide*

- *Oracle Ultra Search Administrator's Guide*
- *Oracle Application Server Web Cache Administrator's Guide*
- *Oracle Application Server Wireless Administrator's Guide*
- *Oracle Application Server Portal Configuration Guide*
- *Oracle Identity Management Guide to Delegated Administration*
- *Oracle Identity Management Integration Guide*
- *Oracle Identity Management Application Developer's Guide*

Oracle Enterprise Manager

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Advanced Configuration*
- *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*

Oracle Database

- *Oracle Database Administrator's Guide*
- *Oracle Database 2 Day DBA*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Collaboration Suite Administration?

This preface introduces the new administrative features of Oracle Collaboration Suite 10g Release 1 (10.1.1). This information is mostly useful to users who have managed Oracle Collaboration Suite Release 1 (9.0.2 and 9.0.3) and Oracle Collaboration Suite Release 2 (9.0.4).

The new administrative features of Oracle Collaboration Suite 10g Release 1 (10.1.1) include:

New Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite Features

New features in [Oracle Enterprise Manager](#) Oracle Collaboration Suite Control include:

- **Topology view of the Oracle Collaboration Suite environment**

A visual representation of the environment is essential for administrators to understand component relationships, such as where applications are deployed across the OracleAS Farm or OracleAS Cluster. The Oracle Collaboration Suite Control Console satisfies this requirement by providing Topology Viewer. Topology Viewer provides a graphical, real-time view of Oracle Collaboration Suite processes managed by [Oracle Process Manager and Notification Server \(OPMN\)](#). From Topology Viewer, you can perform various tasks such as:

 - Viewing the status of the farm, cluster and member components
 - Starting, stopping or restarting processes
 - Monitoring performance across the Oracle Collaboration Suite environment
 - Drilling down to component home pages for details

See "[Reviewing the Oracle Collaboration Suite Component Topology](#)" on page 3-11.
- **Support for viewing and changing Infrastructure Services for Identity Management**

Using the Oracle Collaboration Suite Control, you can view, configure, and change the Infrastructure Services (Identity Management and OracleAS Metadata Repository) used by Oracle Collaboration Suite components. A wizard guides you through the steps of changing the OracleAS Metadata Repository configured for Identity Management. See [Chapter 12, "Changing Infrastructure Services"](#).
- **Views of all performance metrics and metric details**

For each component, you can view a list of performance metrics that Oracle Collaboration Suite Control is monitoring. For each performance metric being monitored, you can drill down to view a brief history of its performance. See ["Monitoring Oracle Collaboration Suite Components"](#) on page 3-14.

- Links to administration pages for all Oracle Collaboration Suite components
From the Oracle Collaboration Suite home page, you can navigate directly to home pages for each of the Oracle Collaboration Suite components that exist in your deployment.
- Complete integration of OracleAS Web Cache administration into Oracle Collaboration Suite Control
Now, you can fully manage and administer OracleAS Web Cache instances through Oracle Collaboration Suite Control, instead of using a separate tool (OracleAS Web Cache Manager). The *Oracle Application Server Web Cache Administrator's Guide* describes how to use Application Server Control to manage OracleAS Web Cache.
- Support for querying from a database log repository
Now, the log repository feature of Oracle Collaboration Suite Control supports using a database repository, not only a file-based repository, as the log repository. However, you cannot use Oracle Collaboration Suite Control to create the database log repository; you must manually create it. See ["Creating and Managing a Diagnostic Message Database Repository"](#) on page 8-21.
- Ability to change the port values of Application Server Control framework components
Now, you can change port numbers of Enterprise Manager components, such as Application Server Control and Oracle Management Agent, by using the `emctl` command-line utility. See {XREF old:} Section 4.3.1, Changing Oracle Enterprise Manager Ports

Oracle Internet Directory Provisioning Console

Oracle Collaboration Suite now includes a centralized user account management and provisioning tool, which allows you to provision users for all of your Oracle Collaboration Suite applications at once. You can manage passwords, set default attributes, grant administrative privileges, bulk-load users for quick provisioning of your entire user base, and manage de-provisioning and user account deletion, all from one centralized GUI.

See: [Chapter 4, "Managing Oracle Collaboration Suite Users and Groups"](#)

Oracle Database 10g and Database Control for the Oracle Collaboration Suite Database

When you install the Oracle Collaboration Suite Database, Oracle Collaboration Suite now installs a version of Oracle Database 10g to host the OracleAS Metadata Repository, Oracle Identity Management, and the Oracle Collaboration Suite application data. Oracle Database 10g includes Oracle Enterprise Manager 10g Database Control, which you can use to manage your new Oracle Collaboration Suite Database.

See: ["Using the Oracle Enterprise Manager 10g Database Control Console"](#) on page 6-2.

New Library Path Variables

The value of the LD_LIBRARY_PATH environment variable has changed, and a new environment variable, LD_LIBRARY_PATH_64 has been introduced with this release.

See: ["Set Up Operating System User Accounts"](#) on page 1-1.

Automation of Configuration Steps to Modify Ports

You can modify port values for Oracle Collaboration Suite components. When some component port values are changed, other components can be affected by those changes. In this release, you can run a command-line program to modify various port values. This command-line program performs additional steps that are required because of the port change, such as configuring OracleAS Web Cache to use a new Oracle HTTP Server port.

See: [Chapter 14, "Changing Oracle Collaboration Suite Network Configurations"](#)

Part I

Getting Started

Part I provides an introduction to Oracle Collaboration Suite and describes how to get started administering the system.

Part I contains the following chapters:

- Chapter 1, "[Getting Started After Installing Oracle Collaboration Suite](#)"
- Chapter 2, "[Starting and Stopping Oracle Collaboration Suite](#)"

Getting Started After Installing Oracle Collaboration Suite

This chapter introduces you to administering Oracle Collaboration Suite and provides instructions to help you get started with a brand new installation.

It contains the following sections:

- [Getting Started with Oracle Collaboration Suite](#)
- [Verifying the Current Configuration](#)

Getting Started with Oracle Collaboration Suite

Before Oracle Collaboration Suite is ready for a production environment, there are some initial tasks that you must perform. You should read through this section and perform the tasks, to prepare your Oracle Collaboration Suite deployment for use.

This section contains the following topics:

- [Set Up Operating System User Accounts](#)
- [Getting Started with Oracle Content Services](#)
- [Setting a Business Administrator Account for Oracle Real-Time Collaboration](#)
- [Enabling Enterprise Manager Accessibility Mode](#)
- [Using the Oracle Collaboration Suite Welcome Page](#)
- [Checking Oracle Collaboration Suite Port Numbers](#)

Set Up Operating System User Accounts

When you install each Oracle Collaboration Suite tier, you are logged in to your operating system with a particular user account. You should always log in using this account to manage the tier, because this account has permission to view and modify the files in this tier's Oracle home.

In order to use Oracle Collaboration Suite, you should set environment variables, as shown in the following tables, on every computer hosting one or more Oracle Collaboration Suite tiers:

- [Table 1-1, " Oracle Collaboration Suite Environment Variables for UNIX"](#)
- [Table 1-2, " Oracle Collaboration Suite Environment Variables for Windows"](#)

Table 1–1 Oracle Collaboration Suite Environment Variables for UNIX

Environment Variable	Value
DISPLAY	<code>hostname:display_number.screen_number</code>
LD_LIBRARY_PATH	On Solaris, make sure this contains the following directory: <code>\$ORACLE_HOME/lib32</code> On Linux, make sure this contains the following directory: <code>\$ORACLE_HOME/lib</code> On HP-UX, make sure this contains the following directory: <code>\$ORACLE_HOME/lib</code>
(Solaris only) LD_LIBRARY_PATH_64	Make sure this contains the following directory: <code>\$ORACLE_HOME/lib</code>
(HP-UX only) SHLIB_PATH	Make sure this contains the following directory: <code>\$ORACLE_HOME/lib32</code>
ORACLE_HOME	Set to the full path of the tier's Oracle home. This is automatically set by Oracle Universal Installer (OUI).
ORACLE_SID (Infrastructure installations only)	Set to the OracleAS Metadata Repository system identifier (SID) you supplied during installation. The default is <code>ocsdbs</code> for one-click installs, or <code>orcl</code> for all other installation types.
PATH	Make sure this contains the following directories, which contain basic commands used by all installations: <code>\$ORACLE_HOME/bin</code> <code>\$ORACLE_HOME/dcm/bin</code> <code>\$ORACLE_HOME/opmn/bin</code> When you start to work with specific components, you may want to add additional directories to your path, as recommended by the component documentation.

Table 1–2 Oracle Collaboration Suite Environment Variables for Windows

Environment Variable	Value
ORACLE_HOME	Set to the full path of the tier's Oracle home. This is automatically set by Oracle Universal Installer (OUI).
ORACLE_SID (Infrastructure installations only)	Set to the OracleAS Metadata Repository system identifier (SID) you supplied during installation. The default is <code>ocsdbs</code> for one-click installs, or <code>orcl</code> for all other installation types. This is automatically set by Oracle Universal Installer.
TEMP	Set to your temp directory, for example, <code>C:\temp</code> .
TMP	Set to your temp directory, for example, <code>C:\temp</code> .

Best Practices for Multiple Tiers on a UNIX Host

If you have installations of more than one Oracle Collaboration Suite tier on a UNIX host, it is very important to completely set your environment when managing a particular tier. For example, if you have installed both an Infrastructure tier and an Applications tier on a single host, you will have at least two Oracle home folders to manage.

Some commands use the `ORACLE_HOME` environment variable to determine which tier to operate on, and some use the directory location of the command. It is, therefore, not sufficient to simply reset the environment variables or `cd` into a different Oracle home as you move between tiers. You must fully change between tiers as follows:

- Log in with the user account you used to install the tier you want to work on.
On UNIX hosts, you may also use the `su` command to switch to the user account, but be sure to use the `"-"` (dash) option so your environment is set the same as it would have been had you actually logged in as the user.

```
su - user
```

- Set the correct environment variables for the tier, as described in [Table 1-1](#) and [Table 1-2](#).
- Execute commands in the Oracle home of the correct tier.

Multiple Installations by the Same User You may have installed multiple tiers on one host as the same user account. If so, make sure you are in the correct Oracle home and have the correct environment variables set when working on a particular tier. You may want to set up some scripts to enable you to easily change from one tier to another.

Getting Started with Oracle Content Services

Read the following sections for information about how to get started with Oracle Content Services.

Choosing Deployment Options for Oracle Content Services

After you have installed and configured Oracle Content Services, you may want to choose various deployment options, depending on your requirements. For example, you may want to integrate Oracle Content Services with an antivirus solution, enable the FTP protocol, or enable Oracle Records Management. See "Oracle Content Services Deployment Options" in Chapter 2 of *Oracle Content Services Administrator's Guide* for information about choosing deployment options.

Signing In to Oracle Content Services for the First Time

When you first sign in to Oracle Content Services, use the `orcladmin` user for the default realm. This user has all of the Oracle Content Services access roles. Once you have signed in, you need to delegate access roles to additional users, as well as set defaults for the Site. See *Oracle Content Services Application Administrator's Guide* for more information about delegating access roles and setting Site defaults.

Creating Additional Sites

In Oracle Content Services, a Site is a discrete organizational entity whose users can collaborate on files and folders. Users in one Site do not have access to the content of users in another Site. Sites are based on identity management realms.

A default Site, based on the default realm in Oracle Internet Directory, is created for you during installation. You can create additional Sites using the Oracle Collaboration Suite Control; see Chapter 9, "Managing Sites" in *Oracle Content Services Administrator's Guide* for more information.

Designating an Administrator E-mail Address for Site Quota Notifications

Each Site has an allocated quota that specifies the amount of content (in MB, GB, or TB) that can be stored in the Site. When the quota consumed by any given Site reaches

95% of the allocated quota, an e-mail notification is sent to any users of that Site with the Quota Administrator role, as well as to the administrator e-mail address specified in the `IFS.DOMAIN.EMAIL.AdministratorAddress` domain property.

This domain property is empty by default. If you want to designate an administrator e-mail address at which to receive the quota notifications, you can do so using the Oracle Collaboration Suite Control.

To designate an administrator e-mail address for site quota notifications:

1. Access the Oracle Collaboration Suite Control and navigate to the Collaboration Suite Home page.
2. Click the name of the Oracle Content Services domain (typically **Content**) in order to access the Content Services Home page.
3. In the Administration section, click **Domain Properties**.
4. On the Domain Properties page, click **IFS.DOMAIN.EMAIL.AdministratorAddress**. You may need to move to the next page to find this property, or you can use the **Search** field.
5. Provide the e-mail address you want to use for receiving error reports in the **Value** field and click **OK**.
6. Return to the Content Services Home page and click **Restart Domain**.

Setting a Business Administrator Account for Oracle Real-Time Collaboration

You must have at least one user with full business administrator privileges, so that you can use all of the administration tabs available in the Oracle Real-Time Collaboration user interface. The business administrator can monitor the system, view reports, create and maintain any custom sites, and check system status. To set this user, you use the `modifyRole` command within the Oracle Real-Time Collaboration `rtcctl` utility.

On a system containing a Oracle Real-Time Collaboration instance, enter the following command. Substitute the appropriate user name for the sample shown.

```
$ORACLE_HOME/imeeting/bin/rtcctl modifyRole -username susan.smith@mycompany.com  
-rolename businessadmin
```

Setting an Administrator Account for Oracle Mail and Oracle Discussions

You must have at least one user with full administrator privileges in order to manage Oracle Discussions and Oracle Mail. In order to manage Oracle Discussions, an Oracle Mail administrator must be provisioned.

To set these privileges, you must log on to the Oracle Internet Directory Provisioning Console and provision a user. When setting Oracle Mail attributes, set the Role attribute to System Administrator.

See:

- [Chapter 4, "Managing Oracle Collaboration Suite Users and Groups"](#)
- For more information about provisioning users in Oracle Mail, see "Managing Oracle Mail Users" in Chapter 2 and "oesucr" in Appendix D of *Oracle Mail Administrator's Guide*

Enabling Enterprise Manager Accessibility Mode

Oracle Collaboration Suite includes the Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite, and you may also have installed Oracle Enterprise Manager 10g Grid Control Console. By default, both of these tools are installed with 'Accessibility Mode' turned off.

Accessibility Mode in Enterprise Manager is used to integrate these GUIs with various accessibility tools, used by the disabled to assist with managing the interface. For example, various screen-readers designed to assist those with visual impairments will work properly only when Accessibility Mode is enabled.

To enable Accessibility Mode in Grid Control, perform the following procedure in every Oracle Home in which Grid Control is installed:

1. Locate the following file and open it using a text editor:

```
ORACLE_HOME/j2ee/OC4J_EM/applications/em/em/WEB-INF/uix-config.xml
```

2. Back up this file, and then comment out or delete the following line:

```
<accessibility-mode>inaccessible</accessibility-mode>
```

3. Restart all instances of Grid Control to complete the procedure.

To enable Accessibility Mode in Oracle Collaboration Suite Control, perform the following procedure in every Oracle Home:

1. Locate the following file and open it using a text editor:

```
ORACLE_HOME/sysman/webapps/emd/WEB-INF/uix-config.xml
```

2. Back up this file, and then comment out or delete the following line:

```
<accessibility-mode>inaccessible</accessibility-mode>
```

3. Restart all instances of Oracle Collaboration Suite Control to complete the procedure.

Using the Oracle Collaboration Suite Welcome Page

The Oracle Collaboration Suite Welcome Page is a great starting point for managing Oracle Collaboration Suite. It includes the following:

- A link to Enterprise Manager Application Server Control Console for Oracle Collaboration Suite (Oracle Collaboration Suite Control); a Web-based tool for managing Oracle Collaboration Suite
- A link to the Oracle Internet Directory Provisioning Console; a Web-based tool for managing and provisioning users
- A link to the online Oracle Technology Network documentation portal, where you can find the latest versions of product documentation for Oracle Collaboration Suite, Oracle Application Server, Oracle Database 10g, and other Oracle products
- A link to Oracle University, where you can get access training and presentations on Oracle products
- A link to Oracle MetaLink, where you can access support services for Oracle Collaboration Suite
- A link to the Collaboration Suite Development Center, where you can access information and resources about developing and customizing applications with Oracle Collaboration Suite

- A link to the Oracle Collaboration Suite Portal, the end-user Web site for accessing all configured Oracle Collaboration Suite components
- Links to the login pages for each of the configured Oracle Collaboration Suite components and Web clients
- A link to the Oracle Desktop Access page, where you can download all Oracle Collaboration Suite desktop clients, such as Oracle Connector for Outlook, the Oracle Calendar Desktop Client, and Oracle Messenger

Figure 1–1 Oracle Collaboration Suite Welcome Page



Accessing the Oracle Collaboration Suite Welcome Page

You can locate the URL for accessing the Oracle Collaboration Suite Welcome Page on the End of Installation Screen text, which is in the following file:

```
(UNIX) ORACLE_HOME/install/setupinfo.txt
(Windows) ORACLE_HOME\install\setupinfo.txt
```

The Oracle Collaboration Suite Welcome Page is accessible using the OracleAS Web Cache port on your Infrastructure installation. For example:

```
http://hostname.domain:7777
```

Tip If you cannot access the Oracle Collaboration Suite Welcome Page, try the following:

1. Check `setupinfo.txt` and make sure you are using the correct URL (hostname and port number).

2. Try restarting Oracle HTTP Server:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl startproc ias-component=HTTP_Server
```

3. Try restarting OracleAS Web Cache:

```
opmnctl stopproc ias-component=WebCache
opmnctl startproc ias-component=WebCache
```

Verifying the Current Configuration

Oracle Collaboration Suite administrators need to be familiar with your particular deployment topology. After the installation is complete, there are some verification steps you should take to ensure every installed component has started up properly and is functioning correctly.

This section contains the following topics:

- [Checking Oracle Collaboration Suite Port Numbers](#)
- [Verifying Portal Configuration](#)
- [Verifying Oracle Mail Configuration](#)
- [Verifying Oracle Content Services Configuration](#)
- [Verifying Oracle Calendar Configuration](#)
- [Verifying Oracle Real-Time Collaboration Configuration](#)
- [Verifying Oracle Voicemail & Fax Configuration](#)
- [Verifying Oracle Mobile Collaboration Configuration](#)

Checking Oracle Collaboration Suite Port Numbers

During installation, Oracle Universal Installer assigned port numbers to various components and services.

Oracle Universal Installer takes several measures to ensure that port number assignments are unique. However, it is possible that a port assignment could conflict with a non-Oracle Collaboration Suite process on your host that was not running during the installation. If you determine there is a conflict, stop the non-Oracle Collaboration Suite process and continue with the tasks in this chapter. Once you have completed the tasks in this chapter and have verified that your installation is running properly, you can consider changing Oracle Collaboration Suite port numbers.

See Also: [Chapter 14, "Changing Oracle Collaboration Suite Network Configurations"](#) for information on changing port numbers

You can find the complete list of port numbers in:

```
(UNIX) ORACLE_HOME/install/portlist.ini
(Windows) ORACLE_HOME\install\portlist.ini
```

[Example 1–1](#) shows sample content from these files.

Example 1–1 Sample portlist.ini Contents

```
Application Tier
-----
```

```

Oracle HTTP Server port = 80
Oracle HTTP Server Listen port = 7778
Oracle HTTP Server SSL port = 443
Oracle HTTP Server Listen (SSL) port = 4444
Oracle Notification Server Request port = 6004
Oracle Notification Server Local port = 6101
Oracle Notification Server Remote port = 6201
ASG port = 7891
Oracle Mail IMAP4 port = 143
Oracle Mail IMAP4 Secure port = 993
Oracle Mail POP3 port = 110
Oracle Mail POP3 Secure port = 995
Oracle Mail SMTP port = 25
Oracle Mail NNTP port = 119
Oracle Mail NNTP Secure port = 563
Application Server Control RMI port = 1851
Oracle Management Agent Port = 1831
Oracle HTTP Server Diagnostic port = 7201
Java Object Cache port = 7001
Log Loader port = 44001
DCM Discovery port = 7101
Application Server Control port = 1810
Web Cache HTTP Listen port = 80
Web Cache HTTP Listen (SSL) port = 443
Web Cache Administration port = 9400
Web Cache Invalidation port = 9401
Web Cache Statistics port = 9402
Oracle Net Listener = 1521
Oracle Calendar server = 5730
Oracle Calendar server manager (CSM) = 5734
Wireless PIM Notification Dispatcher = 9000
Wireless PIMAP UDP Dispatcher = 9300
RTC redirector Server port=1026
RTC redirector MX port=1025
RTC redirector XMPP port=5222
RTC redirector Secure XMPP port=5223
RTC process monitor port=1027
RTC messenger directory server first port=7340
RTC messenger directory server second port=7341
RTC messenger multiuser chat port=7350
RTC messenger connection manager port=7351
RTC messenger statistics collection port=7370
RTC messenger server to server connection port=5269
RTC messenger group service port=7360
RTC messenger voice proxy listener port=3478

Infrastructure Tier
-----
Oracle HTTP Server port = 7777
Oracle HTTP Server Listen port = 7777
Oracle HTTP Server SSL port = 4443
Oracle HTTP Server Listen (SSL) port = 4443
ASG port = 7890
Application Server Control RMI port = 1850
Java Object Cache port = 7000
Oracle HTTP Server Diagnostic port = 7200
Oracle Notification Server Request port = 6003
Oracle Notification Server Local port = 6100
Oracle Notification Server Remote port = 6200
Log Loader port = 44000

```

```

DCM Discovery port = 7100
Oracle Management Agent Port = 1157
Application Server Control port = 1156
Oracle Internet Directory port = 389
Oracle Internet Directory (SSL) port = 636
Enterprise Manager Console HTTP Port (orcl) = 5500
Enterprise Manager Agent Port (orcl) = 1830

```

Some things to note about `portlist.ini` are:

- As you view the `portlist.ini` file, you may wish to change some of the port numbers. You should leave the port numbers as they are until you have completed the tasks in this chapter and confirmed that all of your components are running properly. Then, you can consider changing port numbers. Note that some port numbers cannot be changed, and some require additional steps for updating other components.

See Also: [Appendix A, "Default Port Numbers and Ranges"](#) for information about port assignments and [Chapter 14, "Changing Oracle Collaboration Suite Network Configurations"](#) for information about changing port numbers

- You may notice that `portlist.ini` contains port numbers for components you did not select during installation. This is because Oracle Collaboration Suite reserves ports for all components during installation, even those that were not configured. These port numbers will be used if you configure components after installation.
- The `portlist.ini` file contains the port numbers that were assigned during installation and is very useful for getting started. However, it is not updated if you modify port numbers after installation. Once you start managing Oracle Collaboration Suite, you should use the Enterprise Manager Application Server Control Console for Oracle Collaboration Suite Ports Page for viewing port numbers, because it displays the current port numbers.

Verifying Portal Configuration

You can quickly verify that OracleAS Portal has been configured properly by visiting the portal page.

Verifying Oracle Discussions Configuration

You can verify that Oracle Discussions has been configured properly by logging in to Oracle Discussions, creating one or more topics, and posting one or more messages to a topic.

Verifying Oracle Mail Configuration

Verifying Oracle Content Services Configuration

To ensure that the Oracle Content Services node and HTTP node are running, run the following `opmnctl` command:

- UNIX: `ORACLE_HOME/opmn/bin/opmnctl status`
- Windows: `ORACLE_HOME\opmn\bin\opmnctl status`

The Oracle Content Services node typically appears with the ias-component Content and the process-type Node. The Oracle Content Services HTTP node typically appears with the ias-component Content and the process-type OC4J_Content.

Table 1–3 Expected Oracle Content Services Basic Functionality

Protocol	Access URL
WebDAV	http://applications_tier_host:port/content/dav

Note: The [FTP](#) and FTPS protocols, as well as the Oracle Records Management application, are not enabled by default after you install and configure Oracle Content Services. See Chapter 2, "Oracle Content Services Deployment Options" in *Oracle Content Services Administrator's Guide* for information about how to enable these options.

Verifying Oracle Calendar Configuration

To verify the Calendar server's configuration was successful, open the \$ORACLE_HOME/ocal/misc/unison.ini configuration file.

- To confirm that the Calendar was configured, and not simply installed, the value of the [PRODUCT] configured should be set to TRUE. If this parameter is not set to the expected value, the Calendar was not configured, and as a result, will not start.
- To confirm that the Calendar node was created, verify that the following section appears within the configuration file:

```
[1]
name = N0
version = A.06.10
timezone = <timezone>
```

Use the unidsup command-line utility to verify that the Calendar server can successfully contact [Oracle Internet Directory](#), and that Oracle Internet Directory is currently up and running:

```
$ORACLE_HOME/ocal/bin/unidsup
```

Run the following command-line utility to verify that the Calendar Server has started successfully:

```
$ORACLE_HOME/ocal/bin/unistatus
```

Note: For more information on these command-line utilities, refer to Chapter 6, "Calendar Server Utilities" of the *Oracle Calendar Reference Manual*

Verifying Oracle Real-Time Collaboration Configuration

Run the following test to verify that the Oracle Real-Time Collaboration core components have been configured correctly.

```
$ORACLE_HOME/imeeting/bin/rtcctl runtests -system true
```


To verify that any Voice Conversion server is set up correctly, shut down any other Voice Conversion servers that are assigned to serve the same Oracle Real-Time Collaboration core components. Then, on a core component machine, enter:

```
$ORACLE_HOME/imeeting/bin/rtcctl runtests -testlist voiceconvtest
```

Do the same for the Document Conversion Server:

```
$ORACLE_HOME/imeeting/bin/rtcctl runtests -testlist docconvtest
```

See the *Oracle Real-Time Collaboration Administrator's Guide* for information about how to handle any errors that appear in these tests.

Verifying Oracle Voicemail & Fax Configuration

After you have installed Oracle Voicemail & Fax, use the `opmnctl status` command to verify that the Voicemail & Fax Application services are up and running. The services are identified by the Process-Type ID (Table 1-4). All services should have a status of *Alive*.

Note: When you execute `opmnctl status`, only the first 17 characters of the process-type IDs are displayed and, therefore, some of the names get truncated.

Table 1-4 Required Oracle Voicemail & Fax Services

Process-Type IDs	Service Name
CallTransferService	Call Transfer Service
FaxReceivingService	Fax Receiving Service
InteractiveVoiceResponseService	Interactive Voice Response Service
MessageRecoveryService	Message Recovery Service
MWIService	MWI Service
RecordingService	Recording Service
RetrievalService	Retrieval Service
RoutingService	Routing Service
TelephonyMonitorService	Telephony Monitor Service

If your PBX uses SMDI (Simplified Message Desk Interface), the SMDI Monitor Service must also be running. (The process type ID is *SMDIMonitorService*.) By default, this service is disabled. To enable the SMDI Monitor Service, see "Enabling and Disabling Services" in Appendix F in *Oracle Voicemail & Fax Administrator's Guide*. The Message Delivery Service (process type Id is *MessageRecoveryService*) is not a required service. This service is enabled by default.

If the service is not defined, then there was a problem with the installation. Check the installation log files for any errors.

Configuring Oracle Voicemail & Fax

After you have installed Oracle Voicemail & Fax and verified that the Voicemail & Fax Application services are up and running, you must configure the PBX to work with the application. This step is required before you can run Oracle Voicemail & Fax. For more

information on configuring the Voicemail & Fax Application to work with the PBX, see Chapter 2, "Getting Started" in *Oracle Voicemail & Fax Administrator's Guide*.

Verifying Oracle Mobile Collaboration Configuration

You must perform several steps to verify Oracle Mobile Collaboration is working correctly. See "Configured Components" in Chapter 3 of *Oracle Mobile Collaboration Administrator's Guide* for complete instructions.

Verifying Oracle Workspaces Configuration

During installation and configuration, the `orcladmin` user is granted the Application Administrator role for Oracle Workspaces. This role allows the `orcladmin` user to further grant the Application Administrator role or the Workspace Creator role to other users or groups of users. Once the Workspace Creator role is granted to a user, that user can create new workspaces. The user becomes an Administrator of the workspaces she creates and can add other users or groups as members of the workspace.

Note: By default, the system property which controls which users can create workspaces (Workspace Creation Mode) is set to Restricted i.e. only users with the Workspace Creator role can create new workspaces.

See Also: For more information about managing Oracle Workspaces, including descriptions of the various roles you can assign to users and groups, see ["Managing Oracle Workspaces"](#) on page 5-59

Setting Up the End-User Documentation Portal

The End-user Documentation Portal is a set of customizable HTML pages that provide getting started info and download, installation and configuration information for each Oracle Collaboration Suite end-user component.

See the *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or the *Oracle Collaboration Suite Installation Guide for Microsoft Windows* for instructions on setting up the End-User Documentation Portal.

Starting and Stopping Oracle Collaboration Suite

This chapter describes how to start and stop Oracle Collaboration Suite components; Infrastructure tier instances; Applications tier instances; Oracle Collaboration Suite Databases; and various Oracle Collaboration Suite components; using Oracle Enterprise Manager 10g and command-line tools.

You can start, stop, or restart any component. Some components may be hard-restarted, meaning, the service is completely stopped and then restarted. Other components may be soft-restarted, meaning the service is re-initialized, but not completely stopped, and users will not experience a service interruption.

Oracle Collaboration Suite is a flexible product that you can start and stop in different ways, depending on your requirements. This chapter contains the following sections:

- [Overview of Starting and Stopping Oracle Collaboration Suite](#)

This section outlines the recommended order of operations for starting and stopping the entire Oracle Collaboration Suite deployment. Follow the procedures in this section when starting an entire deployment after a reboot, or when you would like to stop your entire instance, for example, in preparation for shutting down your system.

- [Starting and Stopping Oracle Collaboration Suite Tiers](#)

Oracle Collaboration Suite deployments include Oracle Collaboration Suite Infrastructure tiers and Oracle Collaboration Suite Applications tiers. Follow these instructions for starting and stopping Oracle Collaboration Suite tiers.

- [Starting and Stopping Oracle Collaboration Suite Database Instances](#)

Follow the procedures in this section when starting and stopping Oracle Collaboration Suite Database instances. Although the Oracle Collaboration Suite Database is often hosted as part of an Infrastructure tier, you start and stop it using separate commands.

- [Starting and Stopping Individual Components](#)

Use the procedures in this section to start or stop individual components without shutting down the entire Applications tier.

- [Enabling and Disabling Components](#)

This section describes how to disable components (prevent them from starting when you start a Applications tier instance) and enable components (allow them to start when you start a Applications tier instance).

- [Starting and Stopping: Special Topics](#)

This section describes some exceptions to the general procedures for starting and stopping, including starting and stopping the Log Loader, procedures to use in High Availability environments, and resolving errors that may occur.

Overview of Starting and Stopping Oracle Collaboration Suite

The Oracle Universal Installer will attempt to start Oracle Collaboration Suite when it completes installation. From time to time you will need to stop and restart various components of the system, or the entire deployment. If you are starting Oracle Collaboration Suite 'cold' (such as after rebooting a server) you should follow these instructions carefully to avoid problems.

In general, you should start Oracle Collaboration Suite in the following order:

1. First start the Collaboration Suite Infrastructure. The Infrastructure includes all instances of Enterprise Manager, Oracle Internet Directory, Identity Management, and the Collaboration Suite Database, hosted on Infrastructure tiers.

If you have a distributed Infrastructure installation, start all of the Infrastructure tiers.

In some deployment scenarios, the Collaboration Suite Database (including application data and the OracleAS Metadata Repository) is installed along with the Infrastructure. In this case, the database will start automatically when you start the Infrastructure, if you use the automatic script.

In other deployment scenarios, the Collaboration Suite Database is hosted separately. You may even have multiple Oracle Collaboration Suite Databases. Or, you may choose to start individual components manually. In these scenarios, you may start the Infrastructure and the Oracle Collaboration Suite Databases in any order. If you start the Infrastructure first, you can use Enterprise Manager to start all Collaboration Suite Databases.

Note: If you have upgraded from a previous version of Oracle Collaboration Suite, your Infrastructure will host an **instance** of the OracleAS Metadata Repository, while the Collaboration Suite Database (formally known as the Infostore) is in a separate Oracle Home. In fresh installations of Oracle Collaboration Suite 10g Release 1 (10.1.1), the OracleAS Metadata Repository may be integrated with the Collaboration Suite Database.

2. Second, start Applications tiers. Applications tier components include all the HTTP server and all OC4J applications. If you have configured Oracle Calendar on an Applications tier, you must also start the Oracle Calendar Application System (OCAS) control processes. If you have configured Oracle Mail on an Applications tier, you must also start the Oracle Mail Listener. You may not be able to successfully start Applications tier components unless all Infrastructure tiers and all Oracle Collaboration Suite Database instances are running.

In general, you should stop Oracle Collaboration Suite in the following order:

1. Stop all Applications tiers. To avoid data loss or corruption, never stop the Infrastructure or Collaboration Suite Database while any application is running.
2. Stop Infrastructure instances and Oracle Collaboration Suite Database instances.

The Infrastructure includes all instances of Enterprise Manager, Oracle Internet Directory, Identity Management, and may include the Oracle Collaboration Suite Database.

In many deployments, you will need to issue separate commands to stop the database, and to stop Infrastructure tiers.

You may stop the Infrastructure and the databases in any order. If you stop the databases first, you can use Oracle Enterprise Manager 10g to stop all Collaboration Suite Databases.

Scripted Starting and Stopping

Oracle has provided a sample Oracle Collaboration Suite control script (`ocscctl_sample`) to make starting up and shutting down your Infrastructure and Applications tiers easier. In the following sections, the procedure and syntax for using the script is provided.

Note: The `ocscctl_sample` script is a sample. It has not been extensively tested with all possible deployment scenarios. You should instead use it as a template for the creation of your own, customized startup and shutdown script. Oracle cannot guarantee that the `ocscctl_sample` script will properly start up or shut down any specific deployment.

While the script is running, it prints the name of processes on the console as and when they are started or stopped with the status as successful or failed. If all the processes are started or stopped successfully it prints "Infrastructure/Applications tier processes started successfully." Otherwise, it prints the list of processes that failed to start or stop.

Before running the script, make sure that `ORACLE_HOME` and `ORACLE_SID` have been set to the proper values. For example, if you want to start or stop the Infrastructure processes, you should set the `ORACLE_HOME` to the location of Infrastructure installation, and the `ORACLE_SID` to the name of the Oracle Collaboration Suite Database.

Starting and Stopping Oracle Collaboration Suite Tiers

Oracle Collaboration Suite is composed of two tiers; the Infrastructure tier, and the Applications tier (referred to as the 'middle tier' in previous releases of Oracle Collaboration Suite). Infrastructure tiers are comprised of the following five processes:

- OracleAS Metadata Repository Net listener
- One or more Oracle Collaboration Suite Databases
- Oracle Enterprise Manager 10g Application Server Control Console
- Oracle Enterprise Manager 10g Database Control
- Oracle Process Manager and Notification Server (OPMN) and all managed processes

Similarly, Applications tiers are comprised of the following four processes:

- Enterprise Manager Application Server Control Console for Oracle Collaboration Suite (Oracle Collaboration Suite Control)

- Oracle Process Manager and Notification Server (OPMN) and all managed processes, including all Oracle Collaboration Suite applications
- Oracle Mail listener
- Oracle Calendar Application System (OCAS) control processes

This section provides procedures for starting and stopping the various tiers of an Oracle Collaboration Suite deployment, tier-by-tier. A deployment can consist of multiple Infrastructure and Applications tier instances distributed across one or more hosts.

These instances are dependent on each other and it is important to start and stop them in the proper order. For an overview of the correct order for starting and stopping an entire Oracle Collaboration Suite deployment, see "[Overview of Starting and Stopping Oracle Collaboration Suite](#)" on page 2-2

This section describes how to start and stop Oracle Collaboration Suite tiers. It contains the following topics:

- [Starting the Infrastructure Tier](#)
- [Stopping the Infrastructure Tier](#)
- [Starting an Applications Tier](#)
- [Stopping an Applications Tier](#)

Starting the Infrastructure Tier

This section describes how to start all processes in an Infrastructure. You can follow this procedure after you have rebooted your host, or any other time you would like to start up your entire Infrastructure.

This procedure applies to all Infrastructure types:

- Identity Management and Oracle Collaboration Suite Database (which includes the OracleAS Metadata Repository and application data)
- Distributed Infrastructure deployments, with the Oracle Collaboration Suite Database hosted separately

Starting an Infrastructure Tier Manually

To perform a manual (unscripted) start of the Infrastructure:

1. Set the ORACLE_HOME environment variable to the Infrastructure Oracle home.
2. Set the ORACLE_SID environment variable to the Oracle Collaboration Suite Database **SID** (default is ocsdb).
3. Start the Net Listener:

```
ORACLE_HOME/bin/lsnrctl start
```

4. Start the Oracle Collaboration Suite Database:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> startup
SQL> quit
```

Note: If you have a distributed Infrastructure (you are hosting one or more Oracle Collaboration Suite Databases on separate computers or Oracle Homes), you can skip this step. Be sure to start the Oracle Collaboration Suite Database before you start any Applications tier instances.

See Also: For many more flexible ways to start the Oracle Collaboration Suite Database, see ["Starting and Stopping Oracle Collaboration Suite Database Instances"](#) on page 2-11

5. Start Infrastructure services:

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

This command starts OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and Oracle Internet Directory.

6. Start the Enterprise Manager Application Server Control Console for Oracle Collaboration Suite:

```
ORACLE_HOME/bin/emctl start iasconsole
```

Starting an Infrastructure Tier Using the Sample Script

To start the Infrastructure using the sample script:

1. Set the ORACLE_HOME environment variable to the Infrastructure Oracle Home
2. Set the ORACLE_SID environment variable to the Oracle Collaboration Suite Database SID (default is ocsdb).
3. Run the Oracle Collaboration Suite control script:

On UNIX/Linux:

```
ORACLE_HOME/bin/ocscctl_sample -start infra
```

On Windows:

```
ORACLE_HOME\bin\ocscctl_sample -start infra
```

This command starts the five processes of the Infrastructure. If the Oracle Collaboration Suite Database is installed on the Infrastructure, it will also be started. If you have a distributed Infrastructure (you are hosting the Oracle Collaboration Suite Database on a separate machine), you must start the Oracle Collaboration Suite Database separately. Be sure to start the Oracle Collaboration Suite Database before you start any Applications tiers.

Note: The ocscctl_sample script is a sample. It has not been extensively tested with all possible deployment scenarios. You should instead use it as a template for the creation of your own, customized startup and shutdown script. Oracle cannot guarantee that the ocscctl_sample script will properly start up or shut down any specific deployment.

Starting the Infrastructure Using Oracle Enterprise Manager Grid Control 10g

You can use Oracle Enterprise Manager Grid Control 10g (Grid Control) to administer your infrastructure, including starting it up and shutting it down. Grid Control is a

separate Oracle product that combines a GUI console, agents, common services, and tools to provide an integrated and comprehensive systems management platform for managing Oracle products. Grid Control enables you to start the Infrastructure using a GUI interface, rather than command line operations.

See Also:

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Managing Oracle Collaboration Suite*

Stopping the Infrastructure Tier

This section describes how to stop all processes in an Infrastructure instance. You can follow this procedure when you are preparing to shut down your host, or any other time you would like to stop an Infrastructure tier.

Note: To avoid possible data loss or corruption, you should stop all Applications tiers before stopping any Infrastructure tiers.

This procedure applies to all Infrastructure types:

- Identity Management and Oracle Collaboration Suite Database (which includes the OracleAS Metadata Repository and application data)
- Distributed Infrastructure deployments, with the Oracle Collaboration Suite Database hosted separately

Stopping an Infrastructure Tier Manually

To perform a manual (unscripted) shutdown of an Infrastructure instance:

1. Set the `ORACLE_HOME` environment variable to the Infrastructure Oracle home.
2. Set the `ORACLE_SID` environment variable is set to the Oracle Collaboration Suite Database SID (default is `asdb`).
3. Stop the Enterprise Manager Application Server Control Console for Oracle Collaboration Suite:

```
ORACLE_HOME/bin/emctl stop iasconsole
```

4. Stop components:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
```

This command stops OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and Oracle Internet Directory.

5. Stop the Oracle Collaboration Suite Database instance:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
SQL> quit
```

Note: If you have a distributed Infrastructure (you are hosting the Oracle Collaboration Suite Database on a separate machine), you can skip this step. The Oracle Collaboration Suite Database will continue to run without the Infrastructure, until you shut it down manually.

See Also: For many more flexible ways to stop the Oracle Collaboration Suite Database, see ["Starting and Stopping Oracle Collaboration Suite Database Instances"](#) on page 2-11

6. Stop the Net Listener:

```
ORACLE_HOME/bin/lsnrctl stop
```

Stopping an Infrastructure Tier Using the Sample Script

To stop the Infrastructure using the sample script:

1. Set the `ORACLE_HOME` environment variable to the Infrastructure Oracle Home
2. Set the `ORACLE_SID` environment variable to the Oracle Collaboration Suite Database SID (default is `ocsdB`).
3. Run the Oracle Collaboration Suite control script:

On UNIX/Linux:

```
ORACLE_HOME/bin/ocscctl_sample -stop infra
```

On Windows:

```
ORACLE_HOME\bin\ocscctl_sample -stop infra
```

This command stops the five processes of the Infrastructure in the reverse order they were started. If the Oracle Collaboration Suite Database is installed on the Infrastructure, it will also be stopped. If you have a distributed Infrastructure (you are hosting the Oracle Collaboration Suite Database on a separate machine), you must stop the Oracle Collaboration Suite Database separately.

Note: The `ocscctl_sample` script is a sample. It has not been extensively tested with all possible deployment scenarios. You should instead use it as a template for the creation of your own, customized startup and shutdown script. Oracle cannot guarantee that the `ocscctl_sample` script will properly start up or shut down any specific deployment.

Starting an Applications Tier

This section describes how to start all processes in a Applications tier instance. You can follow this procedure after you have rebooted your host, or any other time you would like to start up an Applications tier.

Starting an Applications Tier Manually

To start an Applications tier instance manually (unscripted):

1. Make sure that you have started the Infrastructure. If you have a distributed Infrastructure (the Oracle Collaboration Suite Database is hosted on a different

computer) make sure you have also started the Oracle Collaboration Suite Database.

2. Set the `ORACLE_HOME` environment variable to the Applications tier Oracle home.
3. Start the Enterprise Manager Application Server Control Console for Oracle Collaboration Suite:

On UNIX/Linux:

```
ORACLE_HOME/bin/emctl start iasconsole
```

On Windows:

```
ORACLE_HOME\bin\emctl start iasconsole
```

4. Start the Oracle Mail listener:

On UNIX/Linux:

Log in as root, if the listener is configured to run on a privileged port (such as port 25), and then run the following command:

```
ORACLE_HOME/bin/tnslsnr listener_es -user <user_id> -group <group_id>
```

On Windows:

```
ORACLE_HOME\bin\tnslsnr start listener_es -user <user_id> -group <group_id>
```

where `<user_id>` and `<group_id>` are the numeric user and group ID numbers.

Note: This command is not expected to return. On UNIX, you can add `'&'` to the end if you want to run it in the background.

5. Start components:

On UNIX/Linux:

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

On Windows:

```
ORACLE_HOME\opmn\bin\opmnctl startall
```

This command starts configured Applications tier applications, including OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, Web Cache, Oracle Calendar Server, Oracle Mail, Oracle Content Services, Oracle RTC, Oracle Voicemail & Fax, Oracle Mobile Collaboration, Portal, Collaborative Workspaces, Oracle Web Access, and Collaboration Suite Search.

6. The Oracle Calendar Application System (OCAS) control processes is running as an external fast CGI process, and therefore is not managed with HTTP Server. Further, because OCAS is not integrated with OPMN, when an Applications tier is started or stopped using `opmnctl`, OCAS is not started or stopped.

If this Applications tier hosts an instance of Oracle Calendar, you must start the Oracle Calendar Application System (OCAS) control processes separately:

On UNIX/Linux:

```
ORACLE_HOME/ocas/bin/ocasctl -start -t ochecklet
ORACLE_HOME/ocas/bin/ocasctl -start
```

On Windows:

```
ORACLE_HOME\ocas\bin\ocasctl -start -t ochecklet  
ORACLE_HOME\ocas\bin\ocasctl -start
```

Ports 8010 and 8020 are the default ports used by OCAS. The valid range is 8010-8020.

Starting an Applications Tier Using the Sample Script

To start an Applications tier instance using the sample script:

1. Make sure that you have started the Infrastructure. If you have a distributed Infrastructure (the Oracle Collaboration Suite Database is hosted on a different computer) make sure you have also started the Oracle Collaboration Suite Database.
2. Set the ORACLE_HOME environment variable to the Applications tier Oracle home.
3. Run the Oracle Collaboration Suite sample control script:

On UNIX/Linux:

```
ORACLE_HOME/bin/ocsctl_sample -start apps
```

On Windows:

```
ORACLE_HOME\bin\ocsctl_sample -start apps
```

Note: The Oracle Collaboration Suite sample control script starts the Oracle Mail listener, if you have configured Oracle Mail on this Applications tier. The Oracle Mail listener is configured to use port 25, a privileged port, by default. On UNIX platforms, superuser permissions are required to run processes on privileged ports. Therefore, if your Applications tier is hosting Oracle Mail, using a privileged port, on a UNIX platform, `ocsctl_sample` will prompt you to enter the root password.

The `ocsctl_sample` script starts all configured Applications tier applications, including OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, Web Cache, Oracle Calendar Server, Oracle Calendar Application System, Oracle Mail, Oracle Content Services, Oracle RTC, Oracle Voicemail & Fax, Oracle Mobile Collaboration, Portal, Collaborative Workspaces, Oracle Web Access, and Collaboration Suite Search. The script also starts the Enterprise Manager Application Server Control Console for Oracle Collaboration Suite, and the Oracle Mail listener.

Note: The `ocsctl_sample` script is a sample. It has not been extensively tested with all possible deployment scenarios. You should instead use it as a template for the creation of your own, customized startup and shutdown script. Oracle cannot guarantee that the `ocsctl_sample` script will properly start up or shut down any specific deployment.

Starting Applications Tiers Using Oracle Enterprise Manager Grid Control 10g

You can use Oracle Enterprise Manager Grid Control 10g (Grid Control) to administer your Applications tiers, including starting and stopping components. Grid Control is a separate Oracle product that combines a GUI console, agents, common services, and tools to provide an integrated and comprehensive systems management platform for managing Oracle products. Grid Control enables you to start your Applications tiers using a GUI interface, rather than command line operations.

See Also:

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Managing Oracle Collaboration Suite*

Stopping an Applications Tier

This section describes how to stop all processes in an Applications tier instance. You can follow this procedure when you are preparing to shut down your host, or any other time you would like to stop an Applications tier.

Stopping an Applications Tier Manually

To stop an Applications tier instance manually (unscripted):

1. Set the `ORACLE_HOME` environment variable to the Applications tier Oracle home.
2. The Oracle Calendar Application System (OCAS) control processes is running as an external fast CGI process, and therefore is not managed with HTTP Server. Further, because OCAS is not integrated with OPMN, when an Applications tier is started or stopped using `opmnctl`, OCAS is not started or stopped.

If this Applications tier hosts an instance of Oracle Calendar, you must stop the Oracle Calendar Application System (OCAS) control processes separately:

On UNIX/Linux:

```
ORACLE_HOME/ocas/bin/ocasctl -stopall
```

On Windows:

```
ORACLE_HOME\ocas\bin\ocasctl -stopall
```

3. Stop components:

On UNIX/Linux:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
```

On Windows:

```
ORACLE_HOME\opmn\bin\opmnctl stopall
```

This command stops all configured Applications tier applications, including OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, Web Cache, Oracle Calendar, Oracle Mail, Oracle Content Services, Oracle RTC, Oracle Voicemail & Fax, Oracle Mobile Collaboration, Portal, Collaborative Workspaces, Oracle Web Access, and Collaboration Suite Search.

4. On Applications tiers hosting an instance of Oracle Mail, stop the Oracle Mail listener:

On UNIX/Linux:

```
ORACLE_HOME/bin/lsnrctl stop listener_es -user <user_id> -group <group_id>
```

On Windows:

```
ORACLE_HOME\bin\lsnrctl stop listener_es -user <user_id> -group <group_id>
```

5. Stop the Enterprise Manager Application Server Control Console for Oracle Collaboration Suite:

```
ORACLE_HOME/bin/emctl stop iasconsole
```

Stopping an Applications Tier Using the Sample Script

To stop an Applications tier instance using the sample script:

1. Set the ORACLE_HOME environment variable to the Applications tier Oracle home.
2. Run the Oracle Collaboration Suite sample control script:

On UNIX/Linux:

```
ORACLE_HOME/bin/ocscctl_sample -stop apps
```

On Windows:

```
ORACLE_HOME\bin\ocscctl_sample -stop apps
```

This script stops all configured Applications tier applications, including OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, Web Cache, Oracle Calendar Server, Oracle Calendar Application System, Oracle Mail, Oracle Content Services, Oracle RTC, Oracle Voicemail & Fax, Oracle Mobile Collaboration, Portal, Collaborative Workspaces, Oracle Web Access, and Collaboration Suite Search.

3. Stop the Enterprise Manager Application Server Control Console for Oracle Collaboration Suite:

```
ORACLE_HOME/bin/emctl stop iasconsole
```

Note: The `ocscctl_sample` script is a sample. It has not been extensively tested with all possible deployment scenarios. You should instead use it as a template for the creation of your own, customized startup and shutdown script. Oracle cannot guarantee that the `ocscctl_sample` script will properly start up or shut down any specific deployment.

Starting and Stopping Oracle Collaboration Suite Database Instances

Many typical Oracle Collaboration Suite configurations include a single instance of the Collaboration Suite Database, installed on the Infrastructure tier. In these scenarios, the Collaboration Suite Database will start up and shut down automatically, when you start up or shut down the Infrastructure using the sample script. The most simple method for starting the Collaboration Suite Database manually is also listed in the instructions for manually starting the Infrastructure.

See Also:

- To start the Infrastructure and Collaboration Suite Database automatically, follow the instructions provided in ["Starting the Infrastructure Tier"](#) on page 2-4.
- To stop the Infrastructure and Collaboration Suite Database automatically, follow the instructions provided in ["Stopping the Infrastructure Tier"](#) on page 2-6.

In other deployment scenarios, you may be hosting the Collaboration Suite Database on a separate computer or Oracle home, or you may have multiple instances of the Collaboration Suite Database. If you upgraded from a previous version of Oracle Collaboration Suite to Oracle Collaboration Suite 10g Release 1 (10.1.1), your OracleAS Metadata Repository may be in a separate database from the Collaboration Suite Database. In these scenarios, you will have to start and stop your database instances directly.

All of the options for starting and stopping the Collaboration Suite Database directly are described in [Chapter 6, "Managing Oracle Collaboration Suite Databases"](#).

Starting and Stopping Individual Components

When you start up an Applications tier instance using Oracle Collaboration Suite Control, the sample `ocscctl_sample` script, or the Grid Control Console, all of the Oracle Collaboration Suite applications (and other Applications tier components) hosted on that tier are automatically started. When you stop an Applications tier using those methods, all of the Oracle Collaboration Suite applications (and other components) are stopped.

From time to time, you may wish to stop and start specific applications or components, rather than the entire tier. For example, you may wish to stop Oracle Real-Time Collaboration in order to perform maintenance, but you do not wish to also stop the Oracle Mail processes hosted on the same Applications tier.

You can use the following tools to start, stop, restart, and view the status of Oracle Collaboration Suite applications and components:

- Oracle Collaboration Suite Control Console—a Web-based tool
- `opmnctl`—a command-line tool
- Grid Control Console—a Web-based tool (for Oracle Voice Mail & Fax only)

These tools are completely compatible—they use OPMN as their underlying technology for managing processes—and can be used interchangeably. For example, you can start a component using `opmnctl` and stop it using the Oracle Collaboration Suite Control.

Although the tools can be used interchangeably, they offer different features. The `opmnctl` command allows you to start and stop sub-processes within components, as well as the entire component. For example, you can start and stop the Web Cache component, or you can start and stop only the Web Cache Admin sub-process. Oracle Collaboration Suite Control allows you to view components that cannot be started or stopped, but whose status depends on other components. For example, it displays the status of the Oracle Workspaces application, whose status depends on the `OC4J_OCSCClient` component. In addition to its other functions, the Grid Control Console provides a view of Oracle Voicemail & Fax similar to that of Oracle Collaboration Suite Control for other Oracle Collaboration Suite applications.

This section contains the following topics:

- [Starting and Stopping Using the Oracle Collaboration Suite Control](#)
- [Starting and Stopping Using opmnctl](#)
- [Starting and Stopping Oracle Calendar](#)
- [Starting and Stopping Oracle Content Services](#)
- [Starting and Stopping Oracle Discussions](#)
- [Starting and Stopping Oracle Mail](#)
- [Starting and Stopping Oracle Mobile Collaboration](#)
- [Starting and Stopping Oracle Real-Time Collaboration Components](#)
- [Starting and Stopping Oracle Collaboration Suite Search](#)
- [Starting and Stopping Oracle Voicemail & Fax](#)
- [Starting and Stopping Oracle Workspaces](#)

Starting and Stopping Using the Oracle Collaboration Suite Control

You can start, stop, restart, and view status of components on the Oracle Collaboration Suite home page:

1. Navigate to the Oracle Collaboration Suite home page for any Applications tier using the Oracle Collaboration Suite Control Console. Scroll to the System Components section.
2. Select the checkboxes in the Select column for the components you want to start, stop, or restart.
3. Click the **Start**, **Stop**, or **Restart** button on the top right of the System Components section.

Each component may be started and stopped using the controls on this page. The Oracle Collaboration Suite Database and the Infrastructure must be running before you can start any component.

For more information about using the Oracle Collaboration Suite Control Console, see ["Using Oracle Collaboration Suite Control Console"](#) on page 3-4.

Starting and Stopping Using opmnctl

Generally, you should use the Oracle Process Manager and Notification Server control for starting and stopping Applications tier components and processes of Oracle Collaboration Suite.

To start, stop, or restart any component:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=component
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=component
ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=component
```

To start, stop, or restart the sub-process of a component:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=component process-type=process
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=component
process-type=process
ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=component
process-type=process
```

To view the status of components and processes:

```
ORACLE_HOME/opmn/bin/opmnctl status
```

To learn more about using `opmnctl`, refer to *Oracle Process Manager and Notification Server Administrator's Guide*.

Starting and Stopping Oracle Calendar

The Oracle Calendar Server can also be started and stopped manually with command line utilities. There are two sets of commands. One set of command line utilities will start and stop the Oracle Calendar Server, and the other set will start and stop the Oracle Calendar application system. Using the command line utilities specific to the Oracle Calendar application system will affect the Oracle Calendar Web Client, Oracle Calendar Web Services, and the Oracle Calendar Sync Server.

1. To check the status of the Oracle Calendar Server before stopping or starting the server, use the `unistatus` command line utility:

```
$ORACLE_HOME/ocal/bin/unistatus
```

Running this utility will provide a summary of the state of the Oracle Calendar Server, indicating which daemons are currently up and running. Moreover, the utility will return a summary of the general status of the Calendar Server, in the form of:

The Calendar Server is up

or

The Calendar Server is down

To check the status of the Oracle Calendar application system, use the `ocasctl` command line utility:

```
$ORACLE_HOME/ocas/bin/ocasctl -status
```

2. To start the Oracle Calendar Server, use the `opmnctl` command line utility:

```
opmnctl startproc ias-component=CalendarServer
```

To start the Oracle Calendar application system, use the `ocasctl` command line utility, with the options specified below:

```
ORACLE_HOME/ocas/bin/ocasctl -start -t ochecklet
```

```
ORACLE_HOME/ocas/bin/ocasctl -start
```

Note: Ports 8010 and 8020 are default port numbers for `ocas` and `ochecklet`. The valid range is 8010 through 8020

3. To stop the Oracle Calendar Server, use the `opmnctl` command line utility:

```
opmnctl stopproc ias-component=CalendarServer
```

Running this utility will terminate all existing Oracle Calendar Server connections by stopping all of the Calendar Server daemons -- unless otherwise specified by utility exception options.

To stop the Oracle Calendar application system, use the `ocasctl` command line utility:


```
$ORACLE_HOME/ocas/bin/ocasctl -stopall
```

See Also: *Oracle Calendar Reference Manual*, *Calendar Server Utilities*,
Oracle Calendar Administrator's Guide, *Introduction to Calendar Administration*

Starting and Stopping Oracle Content Services

The Oracle Content Services software runs as a set of Applications tier processes, called **Oracle Content Services nodes**. Oracle Content Services nodes are processes that manage one or more services and servers, such as the Oracle Content Services FTP server. An **Oracle Content Services domain** is a logical grouping of Oracle Content Services nodes and an Oracle database instance that contains the Oracle Content Services data.

There are two types of nodes: regular nodes, and HTTP nodes. Oracle Content Services HTTP nodes run as part of an OC4J process. You cannot have more than two HTTP nodes on a single Applications tier: one to support the Oracle Content Services application, and one to support the Oracle Records Management application. The OC4J instance for the Oracle Content Services application is OC4J_Content, while the OC4J instance for the Oracle Records Management application is OC4J_RM.

You can start and stop Oracle Content Services node processes using the Application Server Control for Collaboration Suite, or using the `opmnctl` command-line tool.

You can choose to start and stop local Oracle Content Services processes on a single Applications tier, or you can start and stop processes across multiple Applications tiers. You can also start and stop Oracle Content Services sub-processes, such as protocol servers or agents.

For more information about starting and stopping Oracle Content Services processes, see Chapter 5, "Managing Oracle Content Services Processes" in *Oracle Content Services Administrator's Guide*.

Starting and Stopping Oracle Content Services Node Processes on a Single Applications Tier

See the following sections for information about how to start and stop Oracle Content Services node processes on a single Applications tier:

- ["Starting and Stopping Using opmnctl"](#) on page 2-13
- ["Starting and Stopping Using the Oracle Collaboration Suite Control"](#) on page 2-13

Starting and Stopping Oracle Content Services Node Processes Across Multiple Applications Tiers

You can start all Oracle Content Services node processes across multiple Applications tiers from the Oracle Content Services Home page in the Application Server Control for Collaboration Suite, or you can use `opmnctl`.

To start and stop all Oracle Content Services node processes using the Application Server Control for Collaboration Suite:

1. From the Collaboration Suite Home page, click the name of the Oracle Content Services **domain** (typically **Content**).
2. Perform one of the following actions from the Oracle Content Services Home page:

- Click **Start Domain** to start node processes across all Oracle Content Services Applications tiers.
- Click **Stop Domain** to stop all node processes across all Oracle Content Services Applications tiers.
- Click **Restart Domain** to restart node processes across all Oracle Content Services Applications tiers. Only those node processes that are running are affected; processes that are not running will not be started.

To start, stop, or restart all Oracle Content Services node processes across multiple Applications tiers using `opmnctl`, use the `@farm` option, as follows:

```
opmnctl @farm startproc ias-component=Content
opmnctl @farm stopproc ias-component=Content
opmnctl @farm restartproc ias-component=Content
```

You can find the `opmnctl` command-line tool in `ORACLE_HOME/opmn/bin`.

Note: If you have multiple Oracle Content Services domains registered in Oracle Internet Directory, you must specify which domain to start or stop. The first Oracle Content Services domain to be registered is typically identified as "Content," while the second domain to be registered is identified as "Content_2," and so on. You should specify the appropriate domain display name in `opmnctl` commands. For example:

```
opmnctl @farm startproc ias_component=Content_2
```

Starting and Stopping Oracle Content Services Sub-Processes

Use the Application Server Control for Collaboration Suite to start or stop Oracle Content Services protocol servers or agents. For more information, see "Starting, Stopping, Suspending, and Resuming Servers" in *Oracle Content Services Administrator's Guide*.

Starting and Stopping Oracle Discussions

You can start and stop Oracle Discussions by starting and stopping the `OC4J_OCSCClient` process.

The `OC4J_OCSCClient` process includes:

- Oracle Discussions
- Oracle Web Access Client client
- Oracle Collaboration Suite Search
- Oracle WebMail
- Oracle Voicemail & Fax administration pages
- The Oracle Collaboration Suite Welcome pages
- Oracle Workspaces

You can start and stop the `OC4J_OCSCClient` process using Oracle Collaboration Suite Control. See ["Starting and Stopping Using the Oracle Collaboration Suite Control"](#) on page 2-13.

You can start and stop the `OC4J_OCSCClient` process from the command line by using `opmnctl`.

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OC4J process-type=OC4J_
OCSCClient
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J process-type=OC4J_
OCSCClient
ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=OC4J process-type=OC4J_
OCSCClient
```

See "Starting and Stopping Using opmnctl" on page 2-13.

Starting and Stopping Oracle Mail

The Oracle Mail server resides on the Oracle Collaboration Suite application tier. Starting, stopping, or restarting the Oracle Mail server starts or stops all of the Oracle Mail processes, including Housekeeper, **IMAP**, NNTP, POP, list server, **SMTP**, and virus scrubber.

An administrator can prevent individual processes from starting by disabling them.

See Also: "Starting, Stopping, Restarting, or Refreshing All Server Processes" in Chapter 3 of *Oracle Mail Administrator's Guide* for more information about starting and stopping individual Oracle Mail processes

To start, stop, or restart the Oracle Mail server:

1. Open a Web browser and enter the following URL:
`http://host_name:port_number/emd/console`
2. Enter an administrator user ID, such as `ias_admin`, and password.
3. Click the name of the Oracle Collaboration Suite application tier in the **Name** column.
4. Select **E-mail Application**.
5. Click **Start**, **Stop**, **Restart**, or **Reload**.

E-mail service will be temporarily interrupted after clicking **Restart**, and will completely stop or resume after clicking **Stop** or **Start**.

Starting and Stopping Oracle Mobile Collaboration

Because Oracle Mobile Collaboration is configured on top of Oracle Application Server Wireless, its running status depends upon that of OracleAS Wireless; Oracle Mobile Collaboration runs only if OracleAS Wireless runs. Stopping OracleAS Wireless also stops Oracle Mobile Collaboration.

The Mobile Collaboration *Home* page displays the running status of the Mobile Collaboration Server (up, down, or unavailable) and a link to the OracleAS Wireless System Manager. Clicking the Wireless link enables you to access the Home page of the OracleAS System Manager, a tool that enables you to manage and configure the OracleAS Wireless server. Using the **Start All** and **Stop All** buttons on the *Home* page, you can start or stop the entire OracleAS Wireless instance, which includes the Web-based processes and the standalone processes. The Web-based processes, which are the OracleAS Containers for Java (J2EE) applications that run in the OracleAS Wireless instance, are started or stopped using the **Start OC4J Instance** and **Stop OC4J Instance** buttons. You can only start or stop these processes as a group; they cannot be started or stopped individually. The standalone processes, which include the processes

for such components as the Messaging Server, Notification Engine, and the Notification Event Collector, can be started or stopped individually.

You can start and stop the OC4J_Wireless process from the command line by using `opmnctl` as well:

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OC4J process-type=OC4J_Wireless
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J process-type=Wireless
ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=OC4J process-type=OC4J_Wireless
```

See ["Starting and Stopping Using opmnctl"](#) on page 2-13.

For more information on starting and stopping OracleAS Wireless and the OracleAS Wireless processes, see *Oracle Application Server Wireless Administrator's Guide*.

Starting and Stopping Oracle Real-Time Collaboration Components

In addition to the other utilities described in this chapter, if you need to start or stop the Oracle Real-Time Collaboration components, you can do so using the `rtcctl` utility on each Applications tier where Oracle Real-Time Collaboration components have been installed.

1. To check the status of Oracle Real-Time Collaboration components on this tier, use the `rtcctl getState` command:

```
$ORACLE_HOME/imeeting/bin/rtcctl getState
```

2. To start this Oracle Real-Time Collaboration instance, enter the following command:

```
$ORACLE_HOME/imeeting/bin/rtcctl start
```

The Document Conversion or Voice Conversion Servers, used to support conversion of documents for document sharing and streaming voice during conferences, are installed on Windows systems. The syntax of the command to start these instances is:

```
%ORACLE_HOME%\imeeting\bin\rtcctl start
```

3. You can stop any Oracle Real-Time Collaboration instance by using the `stop` command. On UNIX systems:

```
$ORACLE_HOME/imeeting/bin/rtcctl stop
```

On Windows systems:

```
%ORACLE_HOME%\imeeting\bin\rtcctl stop
```

See Also: Chapter 4, "rtcctl Command-line utility for Oracle Real-Time Collaboration," in *Oracle Real-Time Collaboration Administrator's Guide* for details about `rtcctl` and about how to start and stop individual components in an Oracle Real-Time Collaboration instance.

It is also possible to stop specific instance processes by choosing **Conference Details** and then **Diagnostics** from the Web Conference reports available under the **Monitor** tab. See "Monitoring Current Conferences" in Chapter 5 of *Oracle Real-Time Collaboration Administrator's Guide* for more details.

Starting and Stopping Oracle Collaboration Suite Search

You can start and stop Oracle Collaboration Suite Search by starting and stopping the OC4J_OCSClnt process.

The OC4J_OCSClnt process includes:

- Oracle Discussions
- Oracle Web Access Client client
- Oracle Collaboration Suite Search
- Oracle WebMail
- Oracle Voicemail & Fax administration pages
- The Oracle Collaboration Suite Welcome pages
- Oracle Workspaces

You can start and stop the OC4J_OCSClnt process using Oracle Collaboration Suite Control. See ["Starting and Stopping Using the Oracle Collaboration Suite Control"](#) on page 2-13.

You can start and stop the OC4J_OCSClnt process from the command line by using `opmnctl`.

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OC4J process-type=OC4J_
OCSClnt
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J process-type=OC4J_
OCSClnt
ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=OC4J process-type=OC4J_
OCSClnt
```

See ["Starting and Stopping Using opmnctl"](#) on page 2-13.

Starting and Stopping Oracle Voicemail & Fax

In addition to starting and stopping Oracle Voicemail & Fax using `opmnctl` or Oracle Collaboration Suite Control, you can also use Oracle Enterprise Manager Grid Control 10g to manage the Oracle Voicemail & Fax processes. From Grid Control, you can manage the Voicemail & Fax group and any of its subcomponents. Navigate to any Home page, Performance page, or Administration page of the Voicemail & Fax group or any of its subcomponents. From wherever you are in the hierarchy, you can stop, start, restart, or reload any component at that level or any subcomponent below it. For more information on starting and stopping Oracle Voicemail & Fax, see "Managing the Oracle Voicemail & Fax Components" in Chapter 6 in *Oracle Voicemail & Fax Administrator's Guide*.

Starting and Stopping Oracle Workspaces

You can start and stop Oracle Workspaces by starting and stopping the OC4J_OCSClnt process.

The OC4J_OCSClnt process includes:

- Oracle Discussions
- Oracle Web Access Client client
- Oracle Collaboration Suite Search
- Oracle WebMail

- Oracle Voicemail & Fax administration pages
- The Oracle Collaboration Suite Welcome pages
- Oracle Workspaces

You can start and stop the OC4J_OCSCClient process using Oracle Collaboration Suite Control. See ["Starting and Stopping Using the Oracle Collaboration Suite Control"](#) on page 2-13.

You can start and stop the OC4J_OCSCClient process from the command line by using `opmnctl`.

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OC4J process-type=OC4J_
OCSCClient
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J process-type=OC4J_
OCSCClient
ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=OC4J process-type=OC4J_
OCSCClient
```

See ["Starting and Stopping Using opmnctl"](#) on page 2-13.

Enabling and Disabling Components

When you disable a component, you prevent it from starting when you start the tier, and you remove it from the list of System Components displayed on the Oracle Collaboration Suite home page.

When you enable a component, you allow it to start when you start the tier, and it appears in the list of System Components displayed on the Oracle Collaboration Suite home page.

You can enable and disable components using Oracle Collaboration Suite Control. On the Oracle Collaboration Suite home page, click **Enable/Disable Components**. You can select which components to enable or disable. Notice that components that are dependent on each other are grouped, and are all enabled or disabled together.

Note: In order to enable or disable Oracle Content Services, you must select the Oracle Content Services domain display name (typically **Content**), along with any Oracle Content Services or Oracle Records Management OC4J instances (**OC4J_Content** or **OC4J_RM**).

Starting and Stopping: Special Topics

This section contains the following special topics about starting and stopping Oracle Application Server:

- [Using opmnctl Instead of Other Command-Line Tools to Start and Stop](#)
- [Starting and Stopping Log Loader](#)
- [Starting and Stopping in High Availability Environments](#)
- [Shutting Down Oracle Collaboration Suite Database with the IMMEDIATE Option](#)

Using opmnctl Instead of Other Command-Line Tools to Start and Stop

In previous versions of Oracle Collaboration Suite, which were based on Oracle9i Application Server Release 2 (9.0.2 and 9.0.3), `dcmctl` was the recommended command-line tool for starting and stopping Oracle HTTP Server, OC4J, and OPMN.

Other command-line tools, such as `webcachectl`, were used to start the rest of the components.

In Oracle Collaboration Suite 10g Release 1 (10.1.1), you should use `opmnctl` to start all components in your instance, with the exception of the following:

- OracleAS Certificate Authority—use `ocactl` to start and stop. See the *Oracle Application Server Certificate Authority Administrator's Guide* for details.
- Oracle Collaboration Suite Database—use SQL*Plus to start and stop. See ["Starting the Infrastructure Tier"](#) on page 2-4, and ["Stopping the Infrastructure Tier"](#) on page 2-6, for details.
- The Net Listener—use `lsnrctl` to start and stop. See ["Starting the Infrastructure Tier"](#) on page 2-4, and ["Stopping the Infrastructure Tier"](#) on page 2-6, for details.
- The Enterprise Manager Application Server Control Console for Oracle Collaboration Suite—use `emctl` to start and stop. See ["Starting an Applications Tier"](#) on page 2-7, and ["Stopping an Applications Tier"](#) on page 2-10, for details.
- Oracle Calendar Application System (OCAS) control processes—use `ocasctl` to start and stop. See ["Starting an Applications Tier"](#) on page 2-7, and ["Stopping an Applications Tier"](#) on page 2-10, for details.
- The Oracle Mail listener—use `tnslsnr` to start and stop. See ["Starting an Applications Tier"](#) on page 2-7, and ["Stopping an Applications Tier"](#) on page 2-10, for details.

Starting and Stopping Log Loader

The method for starting and stopping Oracle Application Server Log Loader is different from other components.

Log Loader is not started when you issue the `opmnctl startall` command or when you perform a **Start All** operation in the Oracle Collaboration Suite Control. You can start Log Loader in the following ways:

- Using the following command:

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=LogLoader
```

- By clicking the **Start** button on the Log Loader page in the Oracle Collaboration Suite Control.

Log Loader is not stopped when you issue a **Stop All** operation in the Oracle Collaboration Suite Control. You can stop Log Loader in the following ways:

- Using the following command:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=LogLoader
```

- By clicking the **Stop** button on the Log Loader page in the Oracle Collaboration Suite Control.

Refer to ["Using Oracle Collaboration Suite Log Loader"](#) on page 8-11 for detailed information on using the Oracle Application Server Log Loader.

Starting and Stopping in High Availability Environments

For complete instructions on starting and stopping in High Availability environments, see ["Starting and Stopping Oracle Collaboration Suite in a High-Availability Environment"](#) on page 13-19

Shutting Down Oracle Collaboration Suite Database with the IMMEDIATE Option

If you find that the Oracle Collaboration Suite Database instance is taking a long time to shut down, you can use the following command to force an immediate shutdown:

```
SQL> shutdown immediate
```

Immediate database shutdown proceeds with the following conditions:

- No new connections are allowed, nor are new transactions allowed to be started, after the statement is issued.
- Any uncommitted transactions are rolled back. (If long uncommitted transactions exist, this method of shutdown might not complete quickly, despite its name.)
- The immediate shutdown does not wait for users currently connected to the database to disconnect. The Oracle Collaboration Suite Database implicitly rolls back active transactions and disconnects all connected users.

The next startup of the database will not require any instance recovery procedures.

See Also: *Oracle10g Database Administrator's Guide* in the Oracle10g Database documentation library

Part II

Managing Oracle Collaboration Suite

This part of the Guide provides you with a series of chapters addressing the regular administration tasks you or another administrator should perform, to keep Oracle Collaboration Suite running efficiently and available to your users. The first chapter in this Part describes the general GUI tools you will use for most administrative tasks. The following chapters describe the tasks, and, where appropriate, the specialized tools, for administering each of the functional modules that comprise Oracle Collaboration Suite.

Part II contains the following chapters:

- [Chapter 3, "Oracle Collaboration Suite Management Tools"](#)
- [Chapter 4, "Managing Oracle Collaboration Suite Users and Groups"](#)
- [Chapter 5, "Managing Oracle Collaboration Suite Applications"](#)
- [Chapter 6, "Managing Oracle Collaboration Suite Databases"](#)
- [Chapter 7, "Managing Oracle Collaboration Suite Infrastructure"](#)
- [Chapter 8, "Managing Oracle Collaboration Suite Log Files"](#)
- [Chapter 9, "Managing Microsoft Active Directory Integration"](#)
- [Chapter 10, "Monitoring and Tuning Oracle Collaboration Suite Performance"](#)
- [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#)

Oracle Collaboration Suite Management Tools

This chapter introduces the most important administration tools used to manage Oracle Collaboration Suite.

It contains the following topics:

- [Oracle Collaboration Suite Administration Tools](#)
- [Using Oracle Collaboration Suite Control Console](#)
- [Using Grid Control to Manage Oracle Collaboration Suite](#)
- [Using Oracle Directory Manager to Manage Oracle Collaboration Suite](#)
- [Managing Oracle Collaboration Suite from the Command Line](#)

Oracle Collaboration Suite Administration Tools

The procedures you use to monitor and administer the applications running in Oracle Collaboration Suite will vary depending on how it has been deployed. Large or highly-distributed installations may have many Application Server installations, while smaller or more integrated solutions may have as few as one.

Oracle provides three main Web browser interfaces for managing Oracle Collaboration Suite:

- Enterprise Manager Application Server Control Console for Oracle Collaboration Suite, a customized version of the Oracle Enterprise Manager 10g Application Server Control, which is installed by default on every Application Server
- Oracle Enterprise Manager Grid Control 10g, an optional add-on tool which links to all of your Application Server instances, allowing you to centrally manage all the Applications tier components of Oracle Collaboration Suite
- Oracle Enterprise Manager 10g Database Control, a tool you can use for managing an Oracle Application Server Metadata Repository

Taken together, these three tools are often referred to as the Oracle Enterprise Manager 10g.

Introduction to Oracle Collaboration Suite Control

Oracle Enterprise Manager 10g Application Server Control for Collaboration Suite is installed with every tier of Oracle Collaboration Suite you set up with one or more Oracle Collaboration Suite components. As a result, you can immediately begin managing Oracle Collaboration Suite and its components from your Web browser.

From the Oracle Collaboration Suite Control Console, you can monitor and administer a single Oracle Collaboration Suite tier, a farm of tiers comprising an Oracle Collaboration Suite deployment, or an Oracle Application Server cluster.

Oracle Collaboration Suite Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for each component. The Oracle Collaboration Suite home page makes it easy to locate the most important monitoring data and the most commonly used administrative functions—all from your Web browser.

Introduction to Grid Control

Oracle Enterprise Manager 10g Grid Control is installed from a separate installation CD-ROM that is part of the Oracle Application Server CD-ROM pack. The Grid Control Console provides a wider view of your enterprise so you can manage multiple Oracle Application Server instances. In addition, the Grid Control Console provides a robust feature set designed to help you manage all aspects of your enterprise, including your Oracle databases, hosts, listeners, and other components.

See Also: *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite*

When used together, Oracle Collaboration Suite Control and Grid Control provide a complete set of efficient tools to reduce the cost and complexity of managing Oracle Collaboration Suite.

Introduction to the Database Control Console

Oracle Enterprise Manager 10g Database Control is installed and configured when you install any Oracle Collaboration Suite Database.

The Database Control Console is similar to the Oracle Collaboration Suite Control Console, but it is designed to help you manage your Oracle Database. It provides a Web-based user interface for performing a wide variety of database management tasks. For example, you can monitor the performance of the database, schedule backups, and manage the tablespaces of the database.

See Also: ["Using the Oracle Enterprise Manager 10g Database Control Console" on page 6-2](#)

Note that if you use Grid Control to manage your Oracle Collaboration Suite Database, there is no need to use Database Control. All the features of Database Control are available from the database management pages within the Grid Control Console.

Introduction to Oracle Directory Manager

You have two options for making changes to Oracle Internet Directory:

- You can make changes using the Oracle Internet Directory 10g administration tool, Oracle Directory Manager (`oidadmin`)
- You can make changes using the `ldapsearch` and `ldapmodify` command-line tools

See Also:

- *Oracle Internet Directory Administrator's Guide* for detailed information on the Oracle Directory Manager and command-line tools
- ["Adding Applications to your Oracle Collaboration Suite Deployment"](#) on page 5-64
- [Chapter 14, "Changing Oracle Collaboration Suite Network Configurations"](#)

Managing Oracle Collaboration Suite from the Command Line

Oracle Collaboration Suite provides command-line interfaces to several key management technologies. After you become familiar with the architecture and components of Oracle Collaboration Suite, command-line tools can help you automate your management procedures with scripts and custom utilities.

The two most important administration command-line tools are:

- `opmnctl` which provides a command-line interface to Oracle Process Manager and Notification Server (OPMN). You can use `opmnctl` to:
 - Start and stop components, instances, and OracleAS Clusters
 - Monitor processes

See Also: *Oracle Process Manager and Notification Server Administrator's Guide* and ["Starting and Stopping Using opmnctl"](#) on page 2-13

- `dcmctl` which provides a command-line interface to Distributed Configuration Management. You can use `dcmctl` to:
 - Create and remove Oracle Application Server Containers for J2EE (OC4J) instances and OracleAS Clusters
 - Archive and restore configuration information
 - Obtain configuration information

See Also: ["About the Underlying Technologies of Oracle Collaboration Suite Control"](#) on page 3-6 and *Distributed Configuration Management Administrator's Guide*

In addition to `opmnctl` and `dcmctl`, Oracle Collaboration Suite provides many other command-line tools for performing specific tasks. In this book, each of these tools is described when the procedure is presented.

Using Other Tools to Monitor the Built-In Performance Metrics

After you install and start Oracle Collaboration Suite, it automatically begins gathering a set of built-in performance metrics. These built-in performance metrics are measured continuously using performance instrumentation inserted into the implementations of Oracle Collaboration Suite components.

The Oracle Collaboration Suite Control presents a subset of these performance metrics in an organized fashion on the Oracle Collaboration Suite component home pages. For example, the Oracle HTTP Server metrics are presented as a series of charts on the Status Metrics page, which is available from the Oracle HTTP Server home page. You

can also display all the metrics for a particular component by using the All Metrics page.

See Also: ["Displaying the All Metrics Page"](#) on page 3-14

Alternatively, you may want to view the complete set of built-in performance metrics, or you may need to monitor a specific set of Oracle Collaboration Suite component metrics. As a result, Oracle Collaboration Suite also provides a set of command-line and servlet-based tools to view the Oracle Collaboration Suite built-in performance metrics directly, outside of the Oracle Collaboration Suite Control Console.

See Also: *Oracle Application Server Performance Guide*

Using Oracle Collaboration Suite Control Console

This section introduces how to use Enterprise Manager Application Server Control Console for Oracle Collaboration Suite (Oracle Collaboration Suite Control Console). Oracle Collaboration Suite Control is an extended version of Oracle Enterprise Manager 10g Application Server Control, which is a standard component of Oracle Application Server 10g. Use Oracle Collaboration Suite Control Console for locally managing any Oracle Collaboration Suite component.

With Oracle Collaboration Suite Control Console, you can use your Web browser to:

- Log on to Oracle Collaboration Suite Control (using a unique URL, or access from the Welcome Page)
- Start and stop the Oracle Collaboration Suite Infrastructure and Applications tier instances and individual component instances
- Monitor overall performance of Oracle Collaboration Suite
- Review the components of Oracle Collaboration Suite
- From the Infrastructure and Applications tier home pages:
 - Locate and search various Oracle Collaboration Suite log files and the Log Repository
 - Display a list of Oracle Collaboration Suite applications hosted on this Oracle Collaboration Suite Applications tier
 - Display a list of components hosted on any tier
 - List and modify port assignments
 - Use Oracle Identity Management, Central Management, or clustering capabilities
 - Enable and disable components
- Perform re-association, including Infrastructure Security Services re-association (Oracle Internet Directory/OracleAS Single Sign-On), and product metadata [schema](#) or Oracle Collaboration Suite Database re-association
- Use Oracle Collaboration Suite tier home pages to monitor and manage individual tiers
- Use component-level home pages to monitor and configure individual components
- Follow links to the various component administration modules
- Run key scripts

Oracle Collaboration Suite Control provides Web-based management capabilities designed specifically for Oracle Collaboration Suite. Using the Oracle Collaboration Suite Control Console, you can monitor, diagnose, and configure the components of Oracle Collaboration Suite. You can deploy applications, manage security, and create and manage Oracle Application Server clusters.

Oracle Collaboration Suite Control consists of:

- The Oracle Collaboration Suite Control Console and its Oracle Collaboration Suite home pages that you use to manage Oracle Collaboration Suite

These Web pages provide you with a high-level view of your Oracle Collaboration Suite environment. You can then drill down for more detailed performance and diagnostic information.

See Also: ["Introducing the Oracle Collaboration Suite Control Console Home Pages"](#) on page 3-5

- The underlying software technologies that keep track of your Oracle Collaboration Suite instances and components

These technologies automatically perform many of the management tasks as you select options and functions within the Oracle Collaboration Suite Control Console. For example, they discover the components of each Oracle Collaboration Suite instance, gather and process performance data, and provide access to application configuration information.

The following sections provide more information about Oracle Collaboration Suite Control Console:

- [Introducing the Oracle Collaboration Suite Control Console Home Pages](#)
- [About the Underlying Technologies of Oracle Collaboration Suite Control](#)
- [Using the Oracle Collaboration Suite Control Console Online Help](#)

Introducing the Oracle Collaboration Suite Control Console Home Pages

Oracle Collaboration Suite Control Console provides a wide variety of software solutions designed to help you run all aspects of Oracle Collaboration Suite. As a result, you can manage Oracle Collaboration Suite at different levels of detail.

At times, you may want to manage an entire Oracle Collaboration Suite tier. At other times, you will want to manage a specific Oracle Collaboration Suite component.

To support these multiple levels of management, Oracle introduces the Oracle Collaboration Suite home pages. Each home page provides the information you need to monitor the performance and availability of Oracle Collaboration Suite from a particular level of management detail. Selected home pages also provide tools for configuring your Oracle Collaboration Suite components.

From each home page, you can obtain high-level information or you can drill down to get more specific information about an instance, component, or application.

Consider the following home pages that are available when you use the Oracle Collaboration Suite Control Console:

- Use the Oracle Collaboration Suite Farm home page to view all of the Oracle Collaboration Suite tiers in your deployment. For more information, see [Using the Oracle Collaboration Suite Farm Home Page](#) on page 3-7.

- Use the Oracle Collaboration Suite home page to manage all aspects of an individual Oracle Collaboration Suite tier. For more information, see [Using the Oracle Collaboration Suite Home Page](#) on page 3-9.
- Drill down to a component home page to monitor or configure an individual component of Oracle Collaboration Suite. For example, use the Oracle HTTP Server home page to monitor the performance of your Web server, or use the Oracle Application Server Containers for J2EE (OC4J) home page to monitor the Oracle Collaboration Suite applications. For more information, see [Using an Oracle Collaboration Suite Component Home Page](#) on page 3-10.

About the Underlying Technologies of Oracle Collaboration Suite Control

The Oracle Collaboration Suite Control relies on various technologies to discover, monitor, and administer the environment. [Table 3-1](#) provides a summary of the underlying technologies leveraged by the Oracle Collaboration Suite Control.

Table 3-1 Summary of the Oracle Collaboration Suite Control Underlying Technologies

Technology	Description
Dynamic Monitoring Service (DMS)	The Oracle Collaboration Suite Control uses DMS to gather performance data about your Oracle Collaboration Suite components. For more information, see <i>Oracle Application Server Performance Guide</i> .
Oracle Process Manager and Notification Server (OPMN)	OPMN manages Oracle HTTP Server, OC4J, and other Oracle Collaboration Suite processes. It channels all events from different component instances to all components interested in receiving them. For more information, see <i>Oracle Process Manager and Notification Server Administrator's Guide</i> .
Distributed Configuration Management (DCM)	DCM manages configurations among Oracle Collaboration Suite instances that are associated with common Infrastructure Services (members of an Oracle Collaboration Suite Farm). The Oracle Collaboration Suite Control uses DCM to make configuration changes and to propagate configuration changes and deployed applications. For more information, see <i>Distributed Configuration Management Administrator's Guide</i> .
Oracle Management Agent	A local version of the Oracle Management Agent designed specifically to monitor and administer your Oracle Collaboration Suite components.
Oracle Management Watchdog Process	The Oracle Management Watchdog Process monitors the Oracle Management Agent and the Oracle Collaboration Suite Control to make sure both processes are running and available at all times. For more information, see <i>Oracle Enterprise Manager Advanced Configuration</i> .

Using the Oracle Collaboration Suite Control Console Online Help

At any time while using the Oracle Collaboration Suite Control Console, you can click **Help** at the top of the page to get more information. In most cases, the Help window displays a help topic about the current page. Click **Help Contents** in the Help window to browse the list of help topics or to search for a particular word or phrase. From the Table of Contents, click the **Search** tab to search for topics that contain a particular word or phrase.

Getting Started with the Oracle Collaboration Suite Control Console

Use the following sections to get started with the Oracle Collaboration Suite Control Console and become familiar with the home pages within Oracle Collaboration Suite Control:

- [Using the Oracle Collaboration Suite Farm Home Page](#)

- [Displaying the Oracle Collaboration Suite Control Console](#)
- [Using the Oracle Collaboration Suite Home Page](#)
- [Using an Oracle Collaboration Suite Component Home Page](#)

Using the Oracle Collaboration Suite Farm Home Page

All Oracle Collaboration Suite instances use an OracleAS Metadata Repository, so your start page for the Oracle Collaboration Suite Control Console is the Oracle Collaboration Suite Farm home page ([Figure 3–1](#)).

See Also: "What is a Farm?" in the *Oracle Application Server Installation Guide*

The Oracle Collaboration Suite Farm home page displays a list of the tiers in your Oracle Collaboration Suite deployment.

You can configure your Oracle Collaboration Suite instance to use Infrastructure Services by clicking **Infrastructure** on the Oracle Collaboration Suite Farm home page. For more information, see the online help.

Using the Farm home page, you can perform the following tasks:

- View multiple Oracle Collaboration Suite tiers on multiple hosts
- Drill down to the Oracle Collaboration Suite home page for each instance

Figure 3–1 The Oracle Collaboration Suite Farm Home Page

ORACLE Enterprise Manager 10g
Application Server Control for Collaboration Suite

Topology Preferences Help

Farm: OCSM14DB.us.oracle.com

Instances can be grouped and managed together by configuring standalone instances in a common repository. This collection of instances is known as an Oracle Application Server Farm.

Repository Type **Database**

Clusters

Create Cluster

Select Name Status Instances

There are no clusters in the farm.

Standalone Instances

These instances belong to the farm but are not part of any cluster.

Join Cluster

Select Name	Host	Oracle Home
☒ m14.umdev11.us.oracle.com	umdev11.us.oracle.com	C:\product\10.1.1\ocs_m14
☐ mid.usunbh09.us.oracle.com	usunbh09.us.oracle.com	/em10g/10.1.1/M14
☐ OCS_Apps.dsunrdd15.us.oracle.com	dsunrdd15.us.oracle.com	/private/qatest/OCS_M14/OCS_Apps
☐ OCS_Infra.dsunrdd16.us.oracle.com	dsunrdd16.us.oracle.com	/private/qatest/OCS_M14/OCS_Infra
☐ ocsm14.mcarrer-sun.us.oracle.com	mcarrer-sun.us.oracle.com	/private/oracle/products/ocsm14/apps

Topology Preferences Help

Copyright © 1996, 2005, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control for Collaboration Suite

Displaying the Oracle Collaboration Suite Control Console

The following sections describe how to display the Oracle Collaboration Suite Control Console and introduce you to the initial home pages you should see when you display the Oracle Collaboration Suite Control Console for the first time:

- [Using the Oracle Collaboration Suite Control Console URL](#)

- [Displaying the Oracle Collaboration Suite Control Console from the Welcome Page](#)

Using the Oracle Collaboration Suite Control Console URL The URL for the Oracle Collaboration Suite Control Console is included in the text file that displays at the end of the Oracle Collaboration Suite installation procedure. This text file is saved in the following location after you install the application server:

```
(UNIX) ORACLE_HOME/install/setupinfo.txt  
(Windows) ORACLE_HOME\install\setupinfo.txt
```

The Oracle Collaboration Suite Control Console URL typically includes the name of the host computer and the port number assigned to Oracle Collaboration Suite Control during the installation. For example:

```
http://mgmthost1.acme.com:1156
```

Note: The default port for the Oracle Collaboration Suite Control is usually 1156; however, if that port is in use, the installation procedure will assign another port. Refer to the `setupinfo.txt` file for the exact port for your installation of Oracle Collaboration Suite.

Displaying the Oracle Collaboration Suite Control Console from the Welcome Page To view the Oracle Collaboration Suite Control Console from the Oracle Collaboration Suite Welcome Page:

1. Display the Oracle Collaboration Suite Welcome Page by entering the following URL in your Web browser:

```
http://hostname.domain:port
```

For example, if you installed Oracle Collaboration Suite on a host called `sys42`, you would enter the following address in your Web browser:

```
http://sys42.acme.com:7777
```

Note: The default port for Oracle HTTP Server (and, as a result, the Welcome page) is listed in the text file (`setupinfo.txt`) that is generated and displayed at the end of the Oracle Collaboration Suite installation. You can find the `setupinfo.txt` file in the `install` directory of the Oracle Collaboration Suite Oracle Home.

2. Click **Log on to the Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite**.

Enterprise Manager displays the administrator logon dialog box.

3. Enter the Oracle Collaboration Suite administrator user name and password and click **OK**.

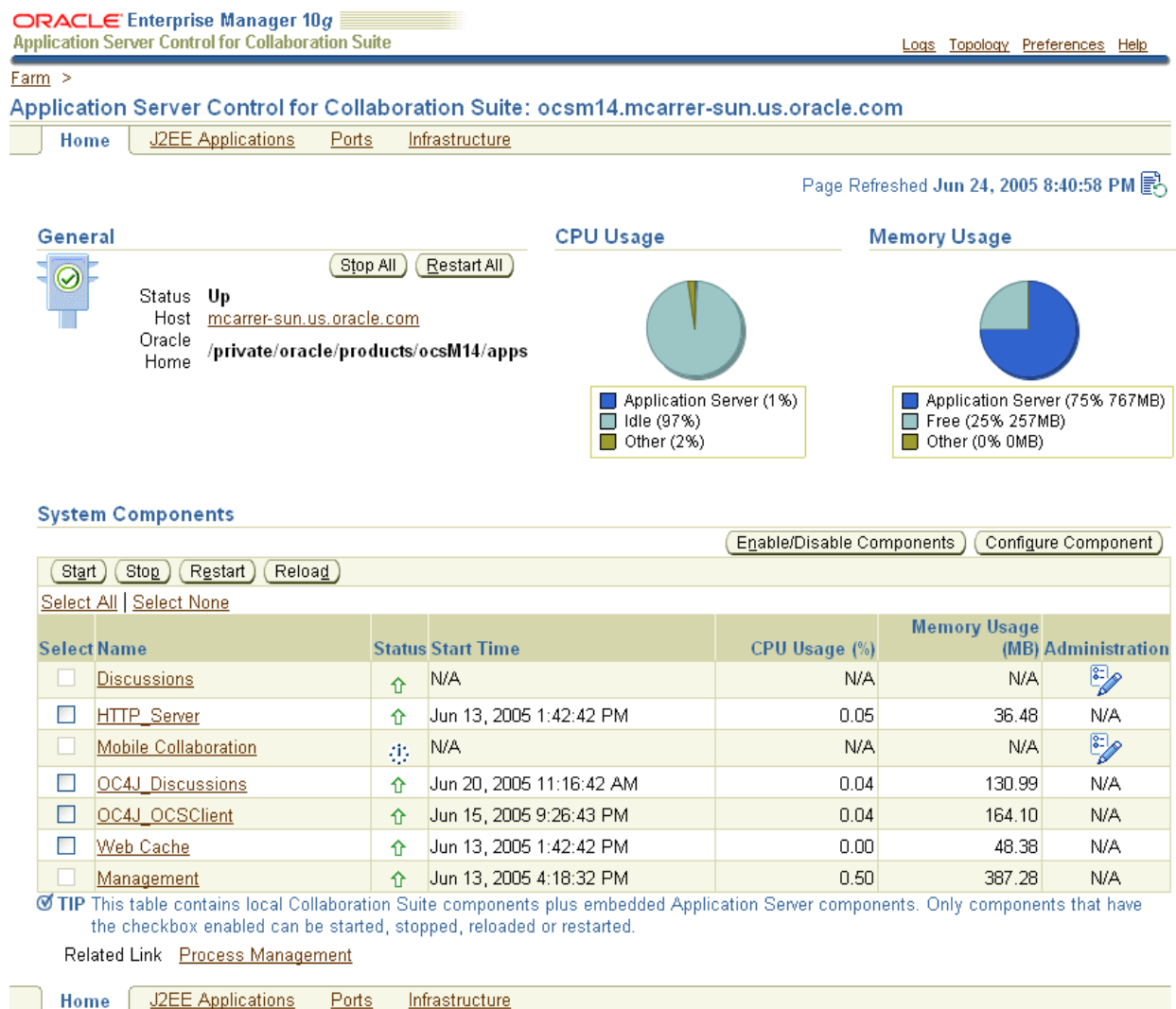
The user name for the administration super-user is `ias_admin`. The password is the one you supplied during the installation of Oracle Collaboration Suite.

Note: You can assign administrator privileges to normal user accounts, and then those authorized users may perform administrative functions using their own accounts. As a security measure, this is much more secure than sharing the `ias_admin` account between several people.

Using the Oracle Collaboration Suite Home Page

From the Oracle Collaboration Suite home page (Figure 3–2), you can start and stop the Oracle Collaboration Suite tier, monitor the overall performance of the server, and review the components of the server. You can also drill down and examine the performance of a particular component and configure the component.

Figure 3–2 Oracle Collaboration Suite home page



This figure displays the Oracle Collaboration Suite home page in Oracle Collaboration Suite Control

The Oracle Collaboration Suite home page provides a table that lists the components of the tier. From this table, you can also get a snapshot of how each individual component is performing.

From the **System Components** table, you can display a home page for each component of the Oracle Collaboration Suite tier.

You can perform the following management functions from the Instance home page:

- Click **Logs** at the top of the page to locate and search the various Oracle Collaboration Suite log files, as well as the Oracle Application Server Log Repository.
- Click **Topology** to view the Topology Viewer, which provides a graphical view of the application server processes managed by Oracle Process Manager and Notification Server (OPMN).

See Also: ["Reviewing the Oracle Collaboration Suite Component Topology"](#) on page 3-11

- Click **J2EE Applications** to display a list of the applications deployed on this tier of Oracle Collaboration Suite.
- Click **Ports** to view a list of all the ports currently in use by the various Oracle Collaboration Suite components. You can also modify many of the port assignments when necessary.
- Click **Infrastructure** to configure Oracle Identity Management, Grid Control Management, or OracleAS Farm Repository Management.
- Click **Enable/Disable Components** to control whether or not the selected components appears in the list of system components and whether or not the component is affected by server-wide actions, such as **Start All** or **Restart All**. When a component is disabled, it does not consume any system resources and you can always enable it later.

For more information, click **Help** after selecting an option on the Oracle Collaboration Suite home page.

See Also: [Using the Oracle Collaboration Suite Control Console Online Help](#) on page 3-6

Using an Oracle Collaboration Suite Component Home Page

Component home pages vary from one component to another because each component has different monitoring and configuration requirements. However, most of the component home pages have the following common elements:

- A general information section that includes an icon to indicate the current state of the component and buttons for starting and stopping the component (if applicable)
- Status information, including CPU and memory usage information, so you can get a snapshot of how the component is performing
- Component-specific information, such as a virtual hosts tab on the HTTP Server home page or a list of deployed applications on the OC4J home page
- Links to administrative functions where appropriate, so you can modify the configuration of selected components. In many cases, this means you can use a graphical user interface to modify complex configuration files.

Monitoring and Diagnosing with the Oracle Collaboration Suite Control Console

The Oracle Collaboration Suite Control Console is designed to encourage a top-down approach to your monitoring and diagnostic activities. For example, you can start by reviewing the basic characteristics of your Oracle Collaboration Suite tier on the Oracle Collaboration Suite home page and then drill down to examine the performance of individual components of the server.

The following sections provide an outline of this monitoring methodology:

- [Reviewing the Oracle Collaboration Suite Component Topology](#)
- [Reviewing General Information and Resource Usage](#)
- [Reviewing the Resources of the Host Computer](#)
- [Monitoring Oracle Collaboration Suite Components](#)
- [Displaying the All Metrics Page](#)
- [Monitoring J2EE Applications](#)

Reviewing the Oracle Collaboration Suite Component Topology

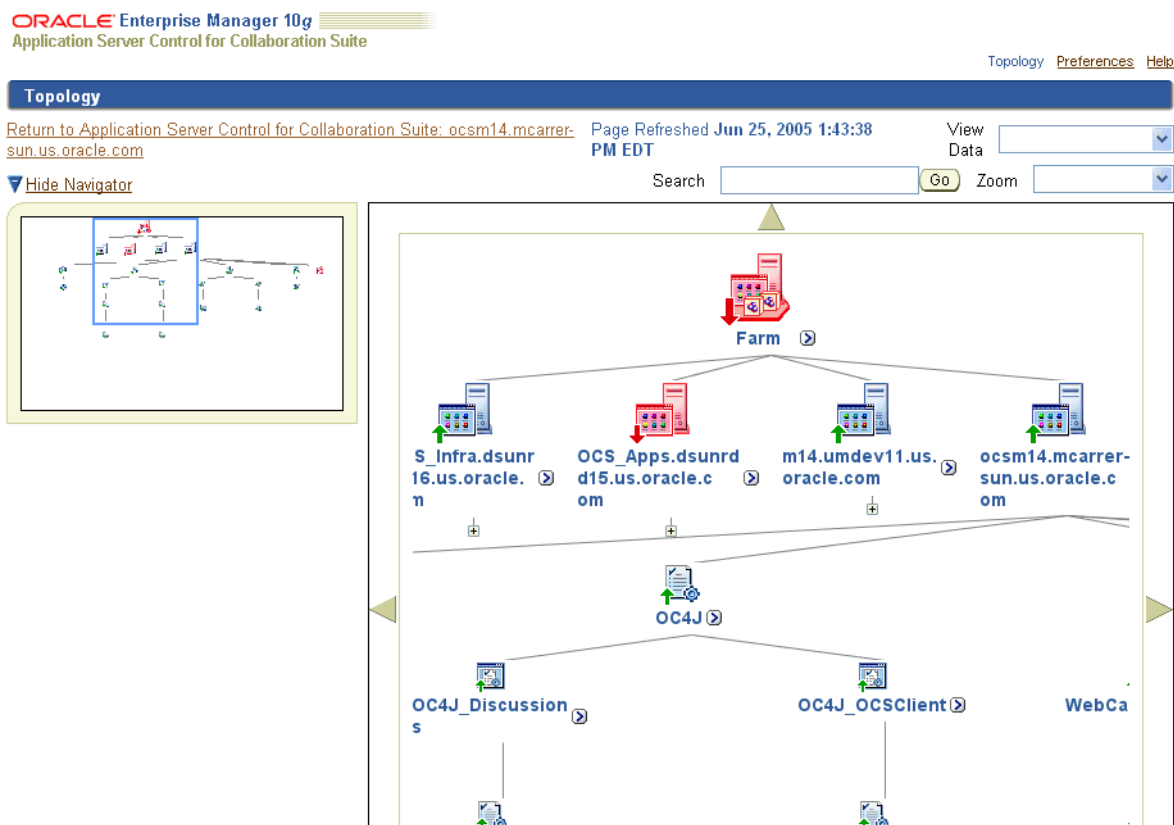
You can click **Topology** at the top of any page in Oracle Collaboration Suite Control Console to display the Topology Viewer ([Figure 3–3](#)). The Topology Viewer provides a graphical, real-time representation of Oracle Collaboration Suite processes managed by OPMN. You can use this viewer to better understand the component relationships of the application server.

The Topology Viewer identifies each component of Oracle Collaboration Suite with an icon. The position of each icon on the page and the connections between the icons represent the relationships between each component. Visual clues in the Topology Viewer help you quickly identify components that are down or performing poorly.

The viewer also shows the relationships between the Oracle Collaboration Suite tiers.

From Topology Viewer, you can perform the following tasks:

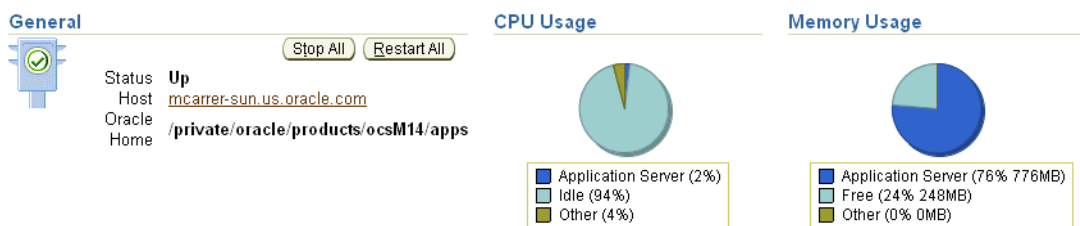
- View the status of components
- Start, stop, or restart processes
- Monitor performance across the Oracle Collaboration Suite environment
- Drill down to component home pages for details

Figure 3–3 Topology Viewer

See Also: "About Topology Viewer" in the Enterprise Manager online help

Reviewing General Information and Resource Usage

The Oracle Collaboration Suite home page provides general information about the status of your server, including the name, location, and application server availability. The home page also provides high-level information about CPU and Memory usage. When reviewing the home page, review the CPU Usage and Memory Usage charts for excessive CPU or Memory usage by the tier (Figure 3–4).

Figure 3–4 General Section of the Oracle Collaboration Suite Home Page

If you suspect that the Oracle Collaboration Suite tier is using too many resources, review the list of components to confirm that each component is up and running and to review the resource usage by each component (Figure 3–5).

Figure 3–5 System Components Table on the Oracle Collaboration Suite Home Page

System Components

[Enable/Disable Components](#)
[Configure Component](#)

[Start](#)
[Stop](#)
[Restart](#)
[Reload](#)

[Select All](#) | [Select None](#)

Select	Name	Status	Start Time	CPU Usage (%)	Memory Usage (MB)	Administration
☐	Discussions	↑	N/A	N/A	N/A	
☐	HTTP_Server	↑	Jun 13, 2005 1:42:42 PM	0.03	36.64	N/A
☐	Mobile Collaboration	⚙	N/A	N/A	N/A	
☐	OC4J_Discussions	↑	Jun 20, 2005 11:16:42 AM	0.12	131.49	N/A
☐	OC4J_OCSCClient	↑	Jun 15, 2005 9:26:43 PM	0.05	164.16	N/A
☐	Web Cache	↑	Jun 13, 2005 1:42:42 PM	0.00	48.54	N/A
☐	Management	↑	Jun 13, 2005 4:18:32 PM	1.90	394.97	N/A

TIP This table contains local Collaboration Suite components plus embedded Application Server components. Only components that have the checkbox enabled can be started, stopped, reloaded or restarted.

Related Link [Process Management](#)

Consider disabling any components that you are not currently using as part of this Oracle Collaboration Suite tier. Disabled components are not started when you start Oracle Collaboration Suite and as a result do not consume system resources. You can always enable a disabled component at a later time.

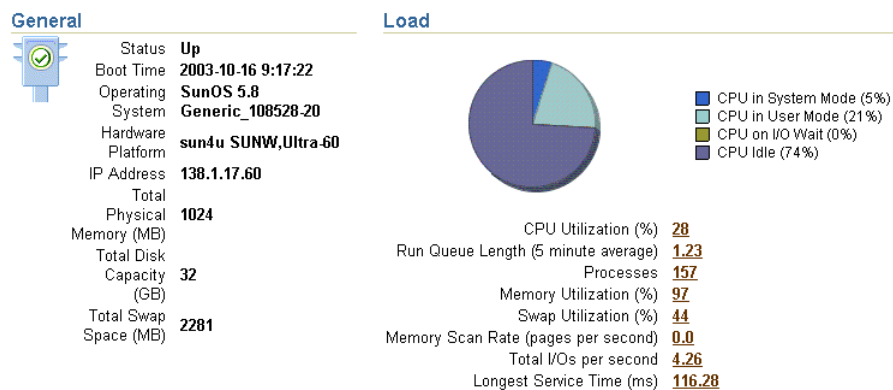
See Also: [Chapter 10, "Monitoring and Tuning Oracle Collaboration Suite Performance"](#), and "Disabling and Enabling Components" in the Enterprise Manager online help

Reviewing the Resources of the Host Computer

Many performance or configuration issues are directly related to a lack of available resources on the host. Before you drill down to analyze the performance and resource usage of the individual components, review the resources and characteristics of the Oracle Collaboration Suite host computer.

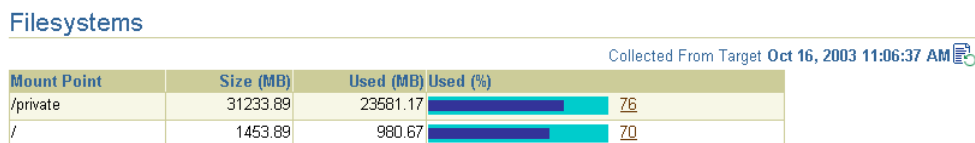
Click the host name in the General section of the Oracle Collaboration Suite home page to display the Host home page. The Host home page provides a summary of the operating system, memory, and disk capacity. The Load section of the page provides a CPU chart that breaks down the CPU usage into categories of usage; the load metrics beneath the chart provide details about system memory usage ([Figure 3–6](#)).

See Also: "About Memory Usage" in the Enterprise Manager online help for information about how Oracle Enterprise Manager 10g calculates the memory usage for your Oracle Collaboration Suite tier.

Figure 3–6 General Information and Load Statistics on the Host Home Page

Scroll to the bottom of the page to view a set of links to real-time performance metrics. If you are concerned about the CPU and Memory usage on the system, click **Top Processes** to display tables listing the processes that are using the most resources on the host.

Click **Filesystems** to display a bar chart that reveals the amount of disk space available on the host (Figure 3–7).

Figure 3–7 Disk Space Usage Chart Available from the Host Home Page

Monitoring Oracle Collaboration Suite Components

After you review the high-level performance metrics and the resources available on the Oracle Collaboration Suite tier host computer, you can then begin to look for potential issues within the individual components.

To diagnose problems with individual components, click the component name in the **System Components** table on the Oracle Collaboration Suite home page. This technique of "drilling down" to obtain more detail can help you isolate problems in a particular component or area of Oracle Collaboration Suite.

Displaying the All Metrics Page

The Oracle Collaboration Suite Control Console provides you with selected performance metrics that you can use to determine the overall performance of your Infrastructure or various Oracle Collaboration Suite components. In some cases, the metrics are shown as performance charts; in other cases, you can monitor the real-time value of the metrics in numeric format.

For a comprehensive list of the metrics that are monitored by Oracle Enterprise Manager 10g on the Infrastructure, you can view the All Metrics page. The All Metrics page is available from the Oracle Collaboration Suite Infrastructure tier home page, and from each of the component home pages.

For example, to view All Metrics page for an Infrastructure instance:

1. Navigate to the Oracle Collaboration Suite Infrastructure home page.

2. Click **All Metrics** in the Related Links section of the page.
Oracle Enterprise Manager 10g displays the All Metrics page for the Infrastructure.
3. Click **Expand All** to see all the metrics in each of the metric categories.
[Figure 3–8](#) shows the All Metrics page after you have expanded all the metric categories.
4. Click the name of metric to display the Metric detail page.
5. Click **Help** to display information about the metric.

Figure 3–8 Infrastructure All Metrics Page



To view the All Metrics page for a component, such as Oracle HTTP Server:

1. Navigate to the component Home page.
2. Click **All Metrics** in the Related Links section of the page.

Oracle Enterprise Manager 10g displays the All Metrics page for the selected component.

Monitoring J2EE Applications

The J2EE applications you deploy and maintain, including all Oracle Collaboration Suite components, represent the most important aspects of your Oracle Collaboration Suite deployments. As a result, Oracle Enterprise Manager 10g also provides a shortcut you can use to review the performance of your hosted applications. Click

J2EE Applications on the Oracle Collaboration Suite home page to display a list of the applications deployed from this tier ([Figure 3–9](#)).

Figure 3–9 List of Applications on the J2EE Applications Page

ORACLE Enterprise Manager 10g
Application Server Control for Collaboration Suite

Logs Topology Preferences Help

Farm >

Application Server Control for Collaboration Suite: ocsm14.mcarrrer-sun.us.oracle.com

Home J2EE Applications Ports Infrastructure

Page Refreshed Jun 25, 2005 2:08:40 PM

Name ▲	OC4J Instance
default	OC4J_OCSCClient
default	OC4J_Discussions
discussions	OC4J_OCSCClient
discussions	OC4J_OCSCClient
VMAdminApp	OC4J_OCSCClient
welcome	OC4J_OCSCClient

Home J2EE Applications Ports Infrastructure

From this list of hosted applications, you can navigate quickly to any hosted application page for information about the performance and availability of each application you have deployed.

Using Grid Control to Manage Oracle Collaboration Suite

Oracle Enterprise Manager Grid Control 10g (Grid Control) is an optional component for your Oracle Collaboration Suite deployment. Grid Control provides the greatest benefit when managing larger installations with many servers, because it allows you to view performance and perform administration of all of the servers from a single console. Generally you will use Grid Control to manage the various application processes as they run on your servers. Grid Control also allows you to view performance metrics over time, while Oracle Collaboration Suite Control only allows you to view real-time values.

Note: Grid Control is required for managing Oracle Voicemail & Fax.

Management tasks you can complete using Grid Control include:

- Logging in to the Grid Control Console
- Viewing a list of Infrastructure and Applications tiers in the Grid Control Console
- Setting thresholds for monitoring and notification
- Creating additional groups of tiers and comparing their performance
- Reviewing performance data and analyzing trends for optimization purposes
- Using the job system to automate standard and repetitive tasks, including:
 - Executing SQL scripts
 - Executing operating system commands
- Using Application Server Service Level Management to monitor J2EE application performance

Oracle Collaboration Suite Control provides all the tools you need to manage your Infrastructure and Applications tiers, clusters, and system components. However, if you have a distributed installation, or if you are using the Oracle Voicemail & Fax component of Oracle Collaboration Suite, consider using Oracle Enterprise Manager 10g Grid Control.

Grid Control, when used with Oracle Collaboration Suite Control, provides a wider view of your Oracle environment beyond the individual application server. From a central location, you can use the Grid Control Console to manage the Oracle Collaboration Suite Databases, Infrastructure, and Oracle Collaboration Suite components, as well as other Oracle applications, across your entire network.

The Grid Control Console offers advanced management features, such as a notification system to notify administrators of changes in your environment and a Job system to automate standard and repetitive tasks, such as executing a SQL script or executing an operating system command.

See Also: *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite*

Oracle Voicemail & Fax, an available component of Oracle Collaboration Suite, is fully integrated with Grid Control. As a result, if you install one or more instances of Oracle Voicemail & Fax, you must install Grid Control in order to administer the various functions of that application.

See Also: Chapter 6, "Managing Oracle Voicemail & Fax," in *Oracle Voicemail & Fax Administrator's Guide* for more information

The following sections provide more information about Grid Control:

- [About the Components of Grid Control](#)
- [Installing the Grid Control Components](#)
- [Logging In to the Grid Control Console](#)
- [Overview of Grid Control Monitoring Tasks](#)
- [Obtaining More Information about Grid Control](#)

About the Components of Grid Control

When you centrally manage your enterprise, including your Oracle Application Server instances, you install and implement a three-tier architecture:

- The Grid Control Console provides a Web-based graphical interface you can use to manage all aspects of your enterprise.
- The Oracle Management Service and a database repository provide a scalable Applications tier for storing crucial management data and processing system management tasks.

Note: The Management Repository is a separate repository from the OracleAS Metadata Repository. The Management Repository is designed specifically for Oracle Enterprise Manager 10g.

- The Oracle Management Agent, which you install on each host computer, monitors the host services and executes tasks from the Management Service.

See Also: *Oracle Enterprise Manager Concepts* for more information about the Oracle Enterprise Manager 10g components and architecture

Installing the Grid Control Components

You install Oracle Enterprise Manager 10g Grid Control from a separate CD-ROM.

To centrally manage your enterprise, you typically perform the following steps:

1. Install the Management Service and the Management Repository on a host computer.
2. Install the Oracle Management Agent on each of the computers that you want to manage from the Grid Control Console.

Note: You install the Oracle Management Agent into its own Oracle Home directory on each managed host.

On each host, the Management Agent gathers information about the various targets on the host. A target is a software component (such as an Oracle Collaboration Suite tier), a host computer, or other service that you manage with Oracle Enterprise Manager 10g. All Oracle Collaboration Suite components are discoverable targets.

Specifically, information about the targets on a host are discovered by the Management Agent during the Management Agent installation. When a target is discovered, information about the target is added to the Management Repository and the target displayed in the list of managed targets in the Grid Control Console.

If you later install additional tiers on a managed host, you can add them to the Grid Control Console. To add additional targets, click **Add** on the Oracle Application Server page in the Grid Control Console, or use the Grid Control Management section of the Infrastructure page in the Oracle Collaboration Suite Control Console.

See Also: *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for complete instructions about installing Grid Control and starting and stopping the Grid Control components.

Oracle Enterprise Manager Advanced Configuration for information about starting and stopping the Grid Control components.

Logging In to the Grid Control Console

After you have configured and started Oracle Management Service, you can log in to the Grid Control Console by entering the following URL in your Web browser:

`http://grid_control_hostname.domain:port/em`

For example:

`http://mgmthost2.acme.com:7777/em`

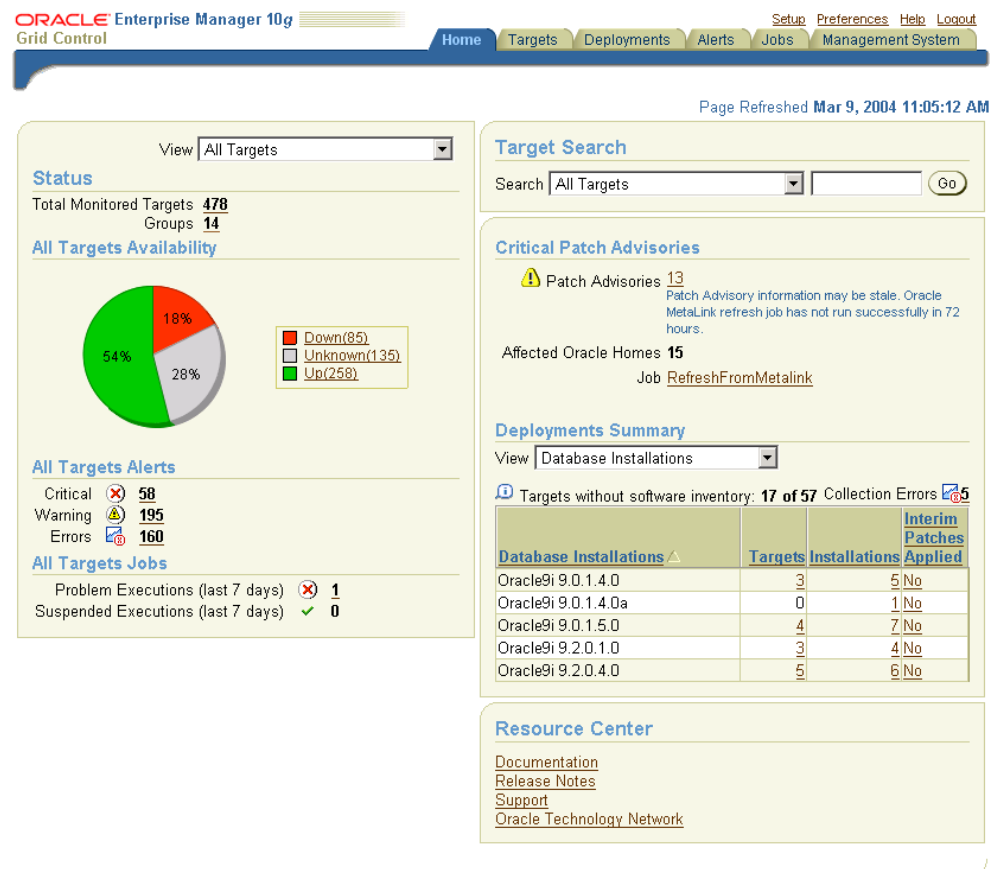
If you are uncertain about the port number, you can refer to one of the following files in the `install` directory of the Management Service Oracle home after you install the Management Service:

- The `setupinfo.txt`, which includes information displayed by the Oracle Universal Installer at the end of the Grid Control install
- The `portlist.ini`, which describes the ports assigned during the Management Service installation

When the Grid Control login page appears, enter the user name and password for the Super administrator SYSMAN account, which you defined during the Grid Control installation.

After you log in, Enterprise Manager displays the Grid Control Console Home page (Figure 3–10).

Figure 3–10 Grid Control Console Home Page



Overview of Grid Control Monitoring Tasks

After you have installed the Management Agent on the Oracle Collaboration Suite hosts and have identified your targets in the Grid Control Console, you can perform a variety of monitoring tasks. For example, you can:

- Set and adjust a set of default metric thresholds for the tiers that you monitor. You can then configure Oracle Enterprise Manager 10g so you are notified automatically when a particular metric reaches its threshold.
- Organize your targets into groups so you can monitor them as a single unit; groups also allow you to compare the performance of each tier you monitor and perform administration tasks, such as blackouts, on the group.

- Review historical data and analyze trends in the performance of your Oracle Collaboration Suite components and J2EE applications (including all Oracle Collaboration Suite applications). For example, you can:
 - Emulate and monitor the **client** experience from remote locations.
 - Measure real end-user performance against a Web application.
 - Trace Web site transactions through the application stack, Oracle HTTP Server, OC4J, and the back-end Oracle Collaboration Suite Database.
 - Correlate application performance across components to rapidly isolate problems.
- Use Application Service Level Management to measure the performance and availability of your J2EE Web applications.
- Perform configuration management tasks, such as software and hardware inventory tracking, cloning, and patching.

Obtaining More Information about Grid Control

For information about starting, configuring, and using Grid Control, see the following documentation:

- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Advanced Configuration*

The Grid Control Console also provides extensive online help. To display the Grid Control Console online help, click **Help** at the top of any of the Grid Control Console pages.

Using Oracle Directory Manager to Manage Oracle Collaboration Suite

You may need to make changes to the Oracle Internet Directory from time to time. Changes must be made manually when you perform any of the following procedures:

- Add a load-balancer and additional Applications tier nodes to your Oracle Collaboration Suite configuration
- Install or configure OracleAS Portal and Oracle Collaborative Portlets on separate Applications tiers
- Move an Applications tier to a new host computer, give it a new host name, or change ports used
- Change to **Secure Sockets Layer (SSL)** access to Oracle Collaboration Suite applications

For instructions on using the Oracle Directory Manager to edit the Oracle Internet Directory Service Registry, see "[Managing the Oracle Internet Directory Service Registry](#)" on page 7-7.

For instructions on creating load-balanced (High-Availability) Applications tiers, see *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

For instructions on changing host names and ports of your tiers, see [Chapter 14, "Changing Oracle Collaboration Suite Network Configurations"](#).

Managing Oracle Collaboration Suite from the Command Line

Oracle Collaboration Suite also provides command-line interfaces to several key management technologies. After you become familiar with the architecture and components of Oracle Collaboration Suite, command-line tools can help you automate your management procedures with scripts and custom utilities.

The two most important administration command-line tools are:

- `opmnctl`, which provides a command-line interface to Oracle Process Manager and Notification Server (OPMN). You can use `opmnctl` to:
 - Start and stop components, instances, and OracleAS Clusters
 - Monitor processes

See Also: ["Starting and Stopping Using `opmnctl`"](#) on page 2-13 and *Oracle Process Manager and Notification Server Administrator's Guide*

- `dcmctl`, which provides a command-line interface to Distributed Configuration Management (DCM). You can use `dcmctl` to:
 - Create and remove OC4J instances
 - Deploy and undeploy OC4J applications
 - Archive and restore configuration information
 - Obtain configuration information

See Also: *Distributed Configuration Management Administrator's Guide*

In addition to `opmnctl` and `dcmctl`, Oracle Collaboration Suite provides many other command-line tools for performing specific tasks. See the instructions for completing administrative tasks throughout this book for more information on command-line tools which you can use to automate your management procedures.

Managing Oracle Collaboration Suite Users and Groups

Oracle Collaboration Suite includes an integrated console interface for all tasks involving user account management. The console interface is fully integrated with [Oracle Delegated Administration Services](#), a component of Oracle Identity Management. Oracle Delegated Administration Services, in turn, stores user and group information in the Oracle Internet Directory database.

Whenever a user logs in to the console, they will see one of two possible interfaces, depending on their user credentials. End-users with normal permissions will see the [Oracle Internet Directory Self-Service Console](#), a ready-to-use application designed to allow users to edit their personal information, change or reset their password, and other basic user management tasks.

When an administrator (a user with the 'allow application provisioning' privilege set) logs in to the console, they will see the [Oracle Internet Directory Provisioning Console](#), a ready-to-use application designed to allow administrators to create user accounts, create groups, manage existing users and groups, set defaults for various user attributes, enable and disable accounts, and manage [identity management realms](#).

This chapter contains the following topics:

- [Introduction to the Oracle Internet Directory Provisioning Console](#)
- [Getting Started with the Provisioning Console](#)
- [Managing User Entries Using the Provisioning Console](#)
- [Managing Group Entries Using the Provisioning Console](#)
- [Configuring User Account Creation Using the Provisioning Console](#)
- [Changing the Default Password Policies](#)
- [Searching for Entries Using the Provisioning Console](#)
- [Managing Identity Management Realms Using the Provisioning Console](#)

Introduction to the Oracle Internet Directory Provisioning Console

The system that stores and manages user accounts and group definitions is Oracle Identity Management. Oracle Identity Management is a component of Oracle Application Server 10g. The primary tool for creating user accounts in Oracle Identity Management is the Oracle Internet Directory Provisioning Console. The Provisioning Console is a tool which interfaces with Oracle Delegated Administration Services, a component of Oracle Identity Management. Oracle Delegated Administration

Services, in turn, stores user and group information in the Oracle Internet Directory database.

Oracle Delegated Administration Services is a component of Oracle Identity Management. It is a set of service units that enable directory administrators to delegate responsibilities to lower administrators or to end users.

The Oracle Internet Directory Provisioning Console is a tool that is built using Oracle Delegated Administration Services units. The Oracle Delegated Administration Services units are like building blocks. The Provisioning Console is a particular tool built using those units. It comes prepackaged, but you can, if you wish, build your own tool using the same Oracle Delegated Administration Services units out of which the Provisioning Console is built.

See Also: For information about building provisioning interfaces using Oracle Delegated Administration Services, see: *Oracle Identity Management Application Developer's Guide*

Provisioning

Use the Provisioning Console to create one user account at a time, or to bulk-provision large numbers of users at once. Generally by importing or entering the appropriate information, user accounts in Oracle Internet Directory allow access to some or all of the Oracle Collaboration Suite components that you have deployed. When a user account is created, it will be provisioned for each Oracle Collaboration Suite component according to the provisioning policies you set. By default, each new user is provisioned for all available applications.

The privilege to create or import users, and set Oracle Collaboration Suite application provisioning policies, can be delegated. You or your delegated administrators control all user and group permissions for Oracle Collaboration Suite.

Policies

During installation and configuration of Oracle Collaboration Suite, each application in the suite registers with Oracle Identity Management, and creates a provisioning profile for itself. The provisioning profile contains all the configuration information concerning the specific application. Once the provisioning registration is completed successfully, the application becomes a provisionable target.

When they register with Oracle Internet Directory, each application that is installed uploads configuration data into the central directory by instantiating template files. The template files are written to Oracle Internet Directory using standard LDIF files, and also by using the provisioning registration tool (*ORACLE_HOME/bin/oidprovtool*).

When you create, modify, or delete user accounts and groups, the Provisioning Console follows the provisioning policy and displays the set of user account fields appropriate for each installed Oracle Collaboration Suite component.

Apart from specifying the default provisioning policy during the initial registration, the application can also implement a policy that is triggered for every user that is created. This policy can inspect whether the user should be provisioned for the particular application or not, based on specified business requirement logic. This policy is supported in form of a plug-in that the application provides out-of-the box or which your organization can write after installation and initial configuration. The administrator always has the privilege to override a provisioning policy at the time of provisioning a user account.

For more information on managing default application provisioning attributes, see ["Setting Default Provisioning Policies"](#) on page 4-28.

Delegating Access

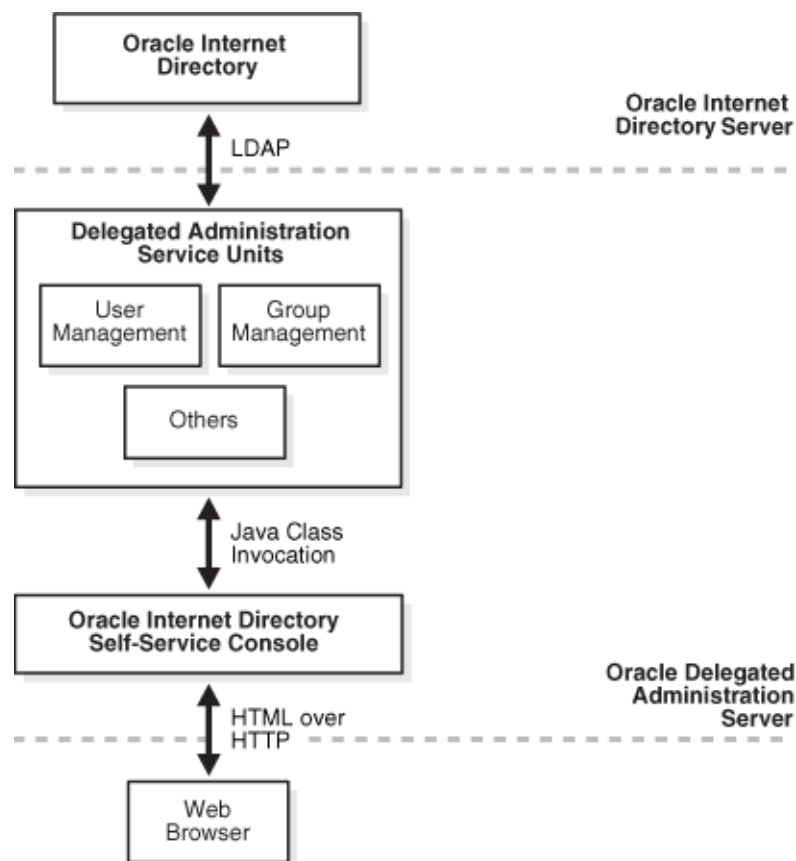
The Provisioning Console also enables you to delegate administrative privileges to various administrators and to end users. It provides a single graphical interface for delegated administrators and end users to manage data in the directory. The various provisioning controls are shown or hidden based on assigned privileges. If the user logging in has the "Allow Application Provisioning" privilege, then that user will see the Provisioning Console, with the full set of user provisioning controls. If the user does not have provisioning privilege, then they will only see the Self-Service Console, which provides controls for managing their own personal information. "Allow Application Provisioning" privileges can be granted using the "Assign Privileges" functionality.

During installation, the `orcladmin` super-user is bootstrapped as an "Allow Application Provisioning" enabled user. You can use this account to delegate this privilege to others, as described above.

Architecture

[Figure 4-1](#) shows how the Self-Service Console interacts with Oracle Delegated Administration Services.

Figure 4-1 Interactions of Oracle Internet Directory Self-Service Console with Oracle Delegated Administration Services



As an administrator, you can perform all of the tasks of an end user, as well as those for which you have the necessary administrative privileges.

Provisioning Process

In Oracle Collaboration Suite, the provisioning process includes the following steps, which are performed by the Provisioning Console:

1. Creating the user in the central directory
2. Enrolling the user in various applications—that is, creating application-specific user values and entitlements
3. Synchronizing the user information with the various applications

For example, provisioning a user to access Oracle Mail involves:

1. Creating the user in the central directory
2. Enrolling the user in Oracle Mail. This involves setting up an e-mail account, specifying the quota for that user, and creating the necessary public folders.
3. The user information in the central directory is kept in sync with the application user information with help of provisioning event propagation from the central directory to the various applications.

You can change information for users and groups from any of the following:

- Oracle Delegated Administration Services
- Oracle Human Resources or other applications integrated with Directory Integration and Provisioning
- Oracle Directory Manager
- Oracle Enterprise Manager tools—for example, Enterprise Security Manager
- Third-party standard LDAP tools

See Also: *Oracle Identity Management Integration Guide*

User Enrollment in Applications

When you create a user using the Provisioning Console, the user account is provisioned for Oracle Collaboration Suite components according to your policy. However, some Oracle Collaboration Suite components create internal user account objects which are separate from the information stored in the Oracle Internet Directory. Generally, the create is event-based, but on demand also exists in case an application was unavailable during the create process: this is called Automatic Enrollment, or "on-demand enrollment".

Automatic Enrollment

This method is sometimes called "on-demand enrollment." Instead of continuously synchronizing with the central directory, the application creates the user footprint when the user first accesses the application. Oracle Application Server [Single Sign-On \(SSO\)](#) uses this method to enroll a user accessing an application.

Provisioning Users in Oracle Calendar

Once users have been added to Oracle Internet Directory, they can be automatically provisioned to the Calendar server. Several provisioning models are available: on-demand, bulk, and notification-Based. These three models can be customized with

defined provisioning policies that help manage if users will be provisioned to calendar, and moreover, the node to which these users will be added.

For more information about provisioning users in Oracle Calendar Server, including information about provisioning models and provisioning policies, see *Oracle Calendar Administrator's Guide* Chapter 6, "Managing User Accounts"

Provisioning Users in Oracle Content Services

After users have been created in Oracle Internet Directory, users are automatically provisioned in Oracle Content Services every 15 minutes by the Oracle Internet Directory Credential Manager Agent. This agent is specific to Oracle Content Services and can be managed from the Content Services Home page in the Oracle Collaboration Suite Control.

Additionally, once a user has been created in Oracle Internet Directory, logging in to Oracle Content Services as that user will immediately provision the user in Oracle Content Services, irrespective of the time interval specified for the Agent.

For more information about provisioning users in Oracle Content Services, including information about changing the default time period for the Oracle Internet Directory Credential Manager Agent, see "Provisioning Users in Oracle Content Services" in Chapter 1 of *Oracle Content Services Administrator's Guide*.

Provisioning Users in Oracle Mail

When users are created in Oracle Internet Directory using Oracle Delegated Administration Services, they can also be provisioned in Oracle Mail. Alternatively, users can be created in Oracle Internet Directory but the administrator can opt not to provision the user in Oracle Mail, in which case users can be provisioned in Oracle Mail using either the Oracle WebMail client or the `oesucr` command-line utility.

For more information about provisioning users in Oracle Mail, see "Managing Oracle Mail Users" in Chapter 2 and "oesucr" in Appendix D of *Oracle Mail Administrator's Guide*.

Provisioning and Managing Oracle Voicemail & Fax Users

Once a user has been provisioned for voice or fax access through the Provisioning Console, an Oracle Voicemail & Fax plug-in automatically enables the user for voice access or fax access, or both. Users can also be provisioned individually or in bulk using the Oracle Voicemail & Fax Accounts Manager, a command-line tool.

Once an account is created, it can be managed in one of several ways, through the Provisioning Console, Grid Control, or the Voicemail & Fax Accounts Manager. Although there are some differences in the functionality of the three methods, they generally allow you to create and delete voice mail accounts, add and delete phone numbers, and manage the properties of the voice mail accounts.

See Chapter 5, "Managing Oracle Voicemail & Fax Accounts," in *Oracle Voicemail & Fax Administrator's Guide* for information about managing user accounts using Enterprise Manager or the Voicemail & Fax Accounts Manager.

Assigning Users Administrative Roles in Oracle Real-Time Collaboration

After you have provisioned users in Oracle Internet Directory, you should assign at least one of them administrative privileges for managing Oracle Real-Time Collaboration. You do this by assigning a user the business administrator role using the `rtcctl modifyRoles` command. This user will have access to all of the tabs

available in the Oracle Real-Time Collaboration Web Client, including the **Monitor**, **Reports**, **Sites** and **System** tabs.

You can also assign users the business monitor role (the user has access to **Monitor** and **Reports** tabs), or assign users a business monitor or business administrator role for a specific Oracle Real-Time Collaboration site.

For an overview of the tasks each user role can do, see "[Oracle Real-Time Collaboration Administration Tools](#)". See "Setting User Roles" in Chapter 4 of *Oracle Real-Time Collaboration Administrator's Guide* for details about how to assign user roles with `modifyRoles`.

Getting Started with the Provisioning Console

This section explains how to log in to the Provisioning Console.

To log in to the Provisioning Console:

1. Visit the URL of the Provisioning Console. For example, if the Provisioning Console is installed on `host1.acme.com` and the Oracle HTTP Server is running on port 7778, then the URL to the Provisioning Console is `http://host1.acme.com:7778/oiddas/`
2. In the upper right corner, select **Login**. This takes you to the Single Sign-On page.
3. In the Single Sign-On page, in the **User Name** field, enter your Single Sign-On user name. For example, `jdoe`.

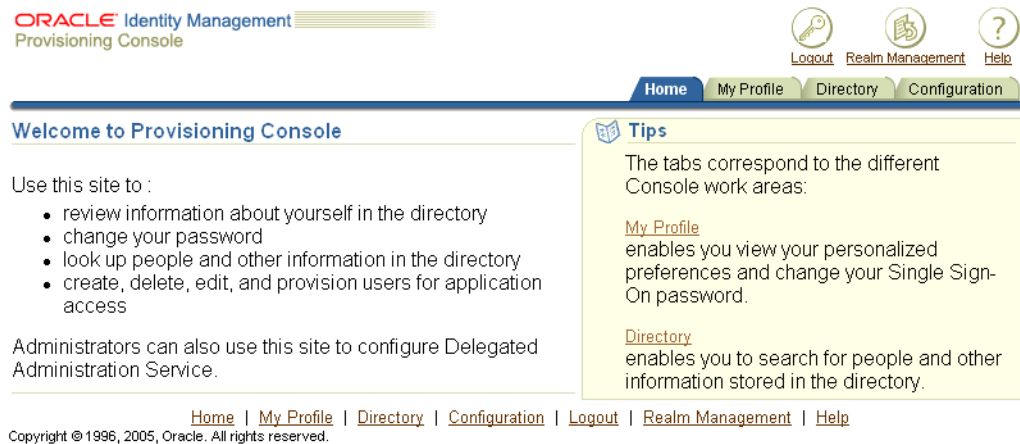
Note: When Oracle Collaboration Suite is installed, the super-user root administrator account `orcladmin` is created. You should use this account when you first log in to the Provisioning Console to create accounts. Once you have delegated user account privileges to other users, you should reserve the `orcladmin` account for procedures that require super-user access.

4. In the **Password** field, enter your Single Sign-On password.
5. If you are in a hosted environment in which there are multiple realms, then the **Company** field appears. Otherwise, it does not appear. If the **Company** field appears, then enter the name of your company.

See Also: For more information about setting up multiple realms, see "[Setting Up and Enabling Multiple Realms](#)" on page 7-1

6. Select **Login**. The Provisioning Console is displayed (see [Figure 4-2](#)).

Figure 4–2 Oracle Internet Directory Provisioning Console



Managing User Entries Using the Provisioning Console

You can use the Provisioning Console to establish the ways that users create user entries. You can also use it to create, modify, and delete user entries, change user passwords and assign privileges to users.

To create a user, you must complete the following step in a multi-step wizard process:

1. Specify the **base** user information.
2. Select the applications for which the user should be provisioned.
3. Specify the application-specific user **attributes**.
4. Verify all the entered information in the previous screens.
5. Submit the information for user creation and provisioning of the Oracle Collaboration Suite applications.

When you submit the user information in step 5, the Provisioning Console requests the provisioning of the user for the various Oracle Collaboration Suite applications. Some of the Oracle Collaboration Suite applications have application-specific user attributes that the application registered as provisioning configuration during the Oracle Collaboration Suite installation. The Provisioning Console exposes these attributes in step 3 with their default values, which you may then alter as appropriate.

When provisioning users for Oracle Collaboration Suite, for each deployed Oracle Collaboration Suite component, you must either enter a minimum amount of information for that user to be provisioned, or, disable provisioning of that user for that component in step 2. The Provisioning Console exposes all user provisioning fields for each deployed component in step 3. For a listing and description of the fields exposed by default for each Oracle Collaboration Suite component, see "[Oracle Collaboration Suite Application-Specific User Attributes](#)" on page 4-18. Aside from those listed in the tables, other Oracle Collaboration Suite applications do not require any additional fields for user creation.

This section contains the following topics:

- [Creating Individual User Entries](#)
- [Managing User Entries in Bulk](#)

- [Modifying User Entries](#)
- [Assigning Privileges to Users](#)
- [Changing the Password of a User](#)
- [Unlocking User Accounts](#)
- [Enabling and Disabling User Accounts](#)
- [De-provisioning Users from Applications](#)
- [Deleting User Accounts and Data](#)
- [Oracle Collaboration Suite Application-Specific User Attributes](#)

Creating Individual User Entries

To create a user entry:

1. Select the **Directory** tab, then select **Users**.
2. Choose **Create** to display the Create User: General window ([Figure 4-3](#)).

Figure 4-3 Provisioning Console Create User: General Window

ORACLE Identity Management Provisioning Console

Logout Realm Management Help

Home My Profile **Directory** Configuration

Users | Groups | Services | Applications

General Provisioning Applications Application Attributes Review

Logged in as orcladmin

Create User: General

Cancel Step 1 of 4 Next

▼ Basic Information

* User ID

* Email Address

* Password (minimum length is 5 with at least 1 numeral(s).)

* Confirm Password

First Name

Middle Name

* Last Name

User default group  

Time Zone

► Additional Details

► Roles Assignment

► Resource Access Information

Cancel Step 1 of 4 Next

[Home](#) | [My Profile](#) | [Directory](#) | [Configuration](#) | [Logout](#) | [Realm Management](#) | [Help](#)

Copyright © 1996, 2005, Oracle. All rights reserved.

3. In the Create User: General window, enter the appropriate information. Fields designated with an asterisk (*) are mandatory.

Note: User names may not contain spaces or any of the following characters: & ' % ? \ / + = () * ^ , ; | ' ~

4. Select **Next** to display the Create User: Application Provisioning window ([Figure 4-4](#)).

Figure 4–4 Provisioning Console Create User: Application Provisioning Window

ORACLE Identity Management Provisioning Console

Home | My Profile | **Directory** | Configuration

Users | Groups | Services | Applications

General | **Provisioning Applications** | Application Attributes | Review

Logged in as **orcladmin**

Create User jwayne : Application Provisioning

This page lists all the provisionable applications and the current provisioning policy for each. The administrator can override the policy.

Cancel Back Step 2 of 4 Next

Provisioning Applications

Component Name	Required	Provisioning	
		Provision	Do Not Provision
Calendar	☒ Yes (by default)	☐	☐
Mail	☒ Yes (by default)	☐	☐
Files	☒ Yes (by default)	☐	☐
RTC	☒ Yes (by default)	☐	☐
Oracle Voicemail & Fax	☒ Yes (by default)	☐	☐

Cancel Back Step 2 of 4 Next

Home | My Profile | Directory | Configuration | Logout | Realm Management | Help

Copyright © 1996, 2005, Oracle. All rights reserved.

5. In the Create User: Application Provisioning window, deployed Oracle Collaboration Suite components are listed, along with a default provisioning policy and override options.

Note: The default provisioning policy determines which Oracle Collaboration Suite components are provisioned by default whenever a new user is created. To change the default provisioning policy, see "[Setting Default Provisioning Policies](#)" on page 4-28.

Select a policy override option to override provisioning policy for any component.

6. Select **Next** to display the Create User: Application Attributes window (Figure 4–5).

Figure 4–5 Provisioning Console Create User: Application Attributes Window

ORACLE Identity Management Provisioning Console

Logout Realm Management Help

Home My Profile Directory Configuration

Users | Groups | Services | Applications

General Provisioning Applications Application Attributes Review

Logged in as orcladmin

Create User jwayne : Application Attributes

This page accepts user input for all application specific user attributes. Some attributes are defaulted as per application configuration.

Cancel Back Step 3 of 4 Next

Calendar

* Calendar storage	Default	Suspend alert period	00:00-00:00
Calendar access	TRUE	Alert suspension period action	Send alerts
Publish status	Not published	Send alert on meeting	TRUE
Enable global agenda view	FALSE	Send alert on day event	FALSE
Alternate e-mail address		Send alert on daily note	FALSE
Reminder delivery rule	Alternate	Send alert on journal	FALSE
Enable alert	FALSE	Send alert on owned event	TRUE
Suspend alert	FALSE	Send alert on declined event	FALSE

Mail

* E-mail Quota (M)	38	Auto Reply	
	(numbers only)	Expiration	(mm/dd/yyyy)
Information Store	OCSM14DB.us.oracle.com	Forward E-mail Address	
User Status	Active	Text Indexing	Disable
Auto Reply Mode		Role	User

- In the Create User: Component Attributes window, required and optional fields are displayed for all Oracle Collaboration Suite Components for which this user is being provisioned.

You must complete at least the required fields shown in this window. For details about all of the Oracle Collaboration Suite Component fields, see [Table 4–2, "Oracle Calendar User Attributes"](#) on page 4-19, [Table 4–3, "Oracle Mail User Attributes"](#) on page 4-20, and [Table 4–4, "Oracle Voicemail & Fax User Attributes"](#) on page 4-21.

Note: Context-sensitive help is available for all of the standard Oracle Collaboration Suite Components. To view context-sensitive help, for a given component, select Help within that component's field selection region of the Create User: Component Provisioning window.

- Select **Next** to display the Create User: Review window ([Figure 4–6](#)).

Figure 4–6 Provisioning Console Create User: Review Window

ORACLE Identity Management Provisioning Console

Logout Realm Management Help

Home My Profile Directory Configuration

Users | Groups | Services | Applications

General Provisioning Applications Application Attributes Review

Create User jwayne : Review

Cancel Back Step 4 of 4 Finish

General

- **Basic Information**
 - User ID **jwayne**
 - Email Address **jwayne@oracle.com**
 - Password
 - Confirm Password
 - First Name **John**
 - Middle Name
 - Last Name **Wayne**
 - User default group
 - Time Zone **(UTC-08:00) US Pacific Time**
- **Additional Personal Details**
 - Single Sign On
 - Enabled
 - Start Date **06/25/2005**
 - End Date
 - Known As
 - Maiden Name
 - Date of Birth
 - Language
- **Organizational Details**
 - Employee Number
 - Job Title
 - Department
 - Manager
 - Assistant
 - Hire Date
- **photograph**

9. In the Create User: Review window, all of your selections from the previous steps are displayed. Confirm that all of the entries are correct and select **Finish** to create the user.

If you need to make any corrections, select **Back** to return to previous Create User windows. You will not lose information entered in later Create User windows unless you completely exit the Create User tab of Provisioning Console.

Managing User Entries in Bulk

You can upload an **LDIF (LDAP Data Interchange Format)** file to the Provisioning Console to create, edit, or delete users in bulk mode.

Note: The LDIF file may contain only base user attributes and no application specific attributes. So, if an application has mandatory attributes that cannot be set to the default value for certain users, the automatic provisioning of those users will fail.

It is possible to create a plug-in which will override default attribute information according to business requirements. The LDIF file import process will honor that plug-in while creating and provisioning users. For more information on managing default application provisioning attributes, see "[Setting Default Provisioning Policies](#)" on page 4-28.

To create, edit, or delete users in bulk mode:

1. Select the **Directory** tab, then **Users**.
2. Select **Bulk** to display the Bulk User Management window.
3. Select **Browse** to browse for an LDIF-formatted file containing the properly formatted user entries.

Note: The LDIF file must be formatted according to [Lightweight Directory Access Protocol \(LDAP\)](#) LDIF file format standards. Every user entry must contain at least the required fields for all applications for which that user is being provisioned.

4. Select or de-select the Ignore Failed Users box. It is selected by default. If you select this option, the bulk create process will attempt to create, edit, or delete users regardless of failures. Failed user accounts will be placed in a file you can download at the end of the process. If you do not select the Ignore Failed Users box, the bulk management process will abort at the first failed user. If you are testing bulk user creation for the first time, Oracle recommends you deselect this box, to avoid cases where hundreds of errors are generated due to a repeating formatting error, missing default field, or other common problem.
5. Select **OK** to begin importing user entries.

See Also: For more information about creating and formatting an LDIF file for bulk user creation, see the *Oracle Internet Directory Administrator's Guide*

Modifying User Entries

Note: If you do not have the privileges to edit a user entry, then the **Edit** button does not appear, and you cannot perform this operation. See [Assigning Privileges to Users](#) on page 4-13 and ["Assigning Privileges to Groups"](#) on page 4-24 for information on setting privileges.

To modify a user entry:

1. Select the **Directory** tab, then **Users**, and perform a search for the user whose entry you want to modify.
2. Select the user whose entry you want to modify, then choose **Edit** to display the Edit User window.
3. In the Edit User: General window, enter the appropriate information. Fields designated with an asterisk (*) are mandatory.

Note: User names may not contain spaces or any of the following characters: & ' % ? \ / + = () * ^ , ; | ' ~

4. Select **Next** to display the Edit User: Component Provisioning window.
5. In the Edit User: Component Provisioning window, all deployed Oracle Collaboration Suite components are listed. You may select any provisioned component and De-Provision that component.
6. Select **Next** to display the Edit User: Application Attributes window.
7. In the Edit User: Application Attributes window, required and optional fields are displayed for all Oracle Collaboration Suite Components that have been provisioned for this user.

You must complete at least the required fields shown in this window. For details about all of the Oracle Collaboration Suite Component fields, see [Table 4-2, "Oracle Calendar User Attributes"](#) on page 4-19, [Table 4-3, "Oracle Mail User Attributes"](#) on page 4-20, and [Table 4-4, "Oracle Voicemail & Fax User Attributes"](#) on page 4-21.

Note: Context-sensitive help is available for all of the standard Oracle Collaboration Suite Components. To view context-sensitive help, for a given component, select Help within that component's field selection region of the Create User: Component Provisioning window.

8. Select **Next** to display the Edit User: Review window.
9. In the Edit User: Review window, all of your selections from the previous steps are displayed. Confirm that all of the entries are correct and select **Finish** to edit the user.

If you need to make any corrections, select **Back** to return to previous Edit User windows. You will not lose information entered in later Edit User windows unless you completely exit the Edit User tab of the Provisioning Console.

Assigning Privileges to Users

You can assign or revoke privileges for users. The privileges available are described in [Table 4-1, "User Privileges"](#) on page 4-13.

Note: You can also assign and revoke privileges for groups. Many organizations find that it is easier to manage privileges for users by assigning them to groups which have the desired privileges, rather than assigning and revoking privileges directly for each user.

For instructions on how to assign and revoke privileges to groups, see ["Assigning Privileges to Groups"](#) on page 4-24.

Table 4-1 User Privileges

Privilege	Description of Access Granted
Allow user creation	Create user entries
Allow user editing	Modify user entries
Allow user deletion	Delete user entries
Allow group creation	Create group entries
Allow group editing	Modify group entries
Allow group deletion	Delete group entries
Allow privilege assignment to users	Assign access rights to users
Allow privilege assignment to groups	Assign access rights to groups
Allow service management	Enable group members to manage services for users. If this is selected, then a Services link becomes available in the Directory tab page when the latter is accessed by group members.

Table 4–1 (Cont.) User Privileges

Privilege	Description of Access Granted
Allow account management	Enable group members to manage accounts for users. If this is selected, then an Accounts link becomes available in the Directory tab page when the latter is accessed by group members.
Allow Oracle Delegated Administration Services configuration	Configure Oracle Delegated Administration Services user interface
Allow resource management for Oracle Reports- and Forms-based applications	Enable users to configure resources—such as databases or applications—to which access is allowed
Allow User Management and Application Provisioning	Allows provisioning users; also automatically enables user account creation, editing, and deletion access

To assign or revoke privileges to a user:

1. Select the **Directory** tab, then **Users**.
2. Perform a search for the entry of the user account to which you want to assign or revoke privileges.
3. From the search results list, select the desired user, then choose **Privileges**. The Assign Privileges to User window displays a list of privileges.

Select the privileges you want to assign to this user. De-select privileges you want to revoke from this user.

Note: Any user account may inherit privileges from a group in which it is a member. Even if you leave a privilege de-selected on this screen, if the user belongs to a group that has that privilege, the user will have access to that privileged function.

4. Select **Submit** to assign or revoke privileges as shown.

Changing the Password of a User

You can change the password of a user other than yourself if:

- You have the necessary access rights
- You have configured user entries so that the `userpassword` attribute is available for modification. The steps for specifying a user attribute for modification is described in ["Configuring the Self-Service Console for User Management"](#) on page 4-26.

To change another user's password:

1. Select the **Directory** tab, then select **Users**.
2. Perform a search for the entry of the user whose password you want to change.
3. From the results of your search, select the user entry, then choose **Edit** to display the Edit User window.
4. In the Edit User window, enter and confirm the password you want to assign to the user.

5. Choose **Submit**.

Note: If you do not have the privileges to edit a user entry, then the **Edit** button does not appear, and you cannot perform this operation.

Unlocking User Accounts

If a user's account has been locked for any reason—for example, if the user entered an incorrect password for a specified number of times while signing in—then you can unlock it without resetting the user password. This saves you from having to explicitly tell the user the new password. Instead, the user can simply log in by using the old password.

To unlock a user's account:

1. Select the **Directory** tab, then select **Users**.
2. Perform a search for the user account that has become locked. A checkmark appears in the Locked column for any user account which has become locked.
3. Select the account that you want to unlock.
4. Select **Unlock**.

Enabling and Disabling User Accounts

You can temporarily disable any user account. While an account is disabled, the user cannot log in. However, the user will continue to be available in the applications. E-mail messages sent to a disabled Oracle Mail user will accumulate in the user's Inbox. Disabled Oracle Calendar users will still be available to be added to appointments and meetings.

If a user's account has been disabled, you can enable it. To enable or disable user accounts:

1. Select the **Directory** tab, then select **Users**.
2. Perform a search for the user account that you wish to enable or disable. A checkmark appears in the Enabled column for any user account which enabled, and there is no checkmark in this column for any user account which has become suspended.
3. Select the user account that you want to enable or disable.
4. Select **Enable** to enable the user account. Select **Disable** to **Disable** the user account.

De-provisioning Users from Applications

When you create a user account, you provision that account for one or more Oracle Collaboration Suite applications. You can later provision the user for additional Oracle Collaboration Suite applications.

At any time, you can de-provision a user account from one or more provisioned applications. De-provisioning means that the user will no longer be able to access the application. De-provisioning is different from disabling in the following ways:

- A disabled user continues to exist in the application; other users of that application will see the disabled user ID in contact lists, calendar appointments, shared folders, and so forth.
- A de-provisioned user is no longer available in the de-provisioned application. E-mail messages sent to a user ID which has been de-provisioned from Oracle Mail will be rejected by the system. Users cannot add a user de-provisioned from Oracle Calendar to appointments or meetings.
- A de-provisioned user account remains in Oracle Internet Directory. The account can later be re-provisioned for an application, and regain access to stored data such as Oracle Mail e-mail messages, and Oracle Content Services stored files.

Note: For Oracle Content Services, de-provisioning a user is the same as disabling a user.

To de-provision a user from one or more applications:

1. Using the Provisioning Console, select the Directory tab and then search for the user you wish to de-provision.
2. Select the user and click Edit. The Edit User: General window is shown.
3. Select Next. The Edit User: Application Provisioning window is shown (Figure 4-7). In this window, all available applications are shown. Select each provisioned application in the De-Provision column to de-provision those applications.

Figure 4-7 Provisioning Console Edit User: Application Provisioning Window

ORACLE Identity Management Provisioning Console

Home My Profile **Directory** Configuration

Users | Groups | Services | Applications

General Provisioning Applications Application Attributes Review

Logged in as orcladmin

Information
Some Rows in the tables are disabled.
Oracle Voicemail & Fax

Edit User mickey.mouse : Application Provisioning

This page lists the provisioned applications from which the administrator can de-provision the user. [Cancel](#) [Back](#) [Step 2 of 4](#) [Next](#)

Component Name	De-Provision
Calendar	☐
Mail	☐
Files	☐
RTC	☐
Oracle Voicemail & Fax	☐

[Cancel](#) [Back](#) [Step 2 of 4](#) [Next](#)

[Home](#) | [My Profile](#) | [Directory](#) | [Configuration](#) | [Logout](#) | [Realm Management](#) | [Help](#)

Copyright © 1996, 2005, Oracle. All rights reserved.

4. Click Next. The Edit User: Application Attributes window opens. De-provisioned applications will not show attributes on this page.

5. Click Next. The Edit User: Review window opens. At the bottom of the page, a section titled 'Applications to be De-Provisioned' lists all applications that will be de-provisioned.
6. Click Finish. The user will be de-provisioned from applications, and any other changes you have made while editing the user account will be saved.

De-provisioning Users from Oracle Voicemail & Fax

When a user is de-provisioned from Oracle Voicemail & Fax, the Oracle Internet Directory user object allocated for this user is deleted. The user's existing voice mail messages stored in the system will not be impacted by this function. However, the user's greeting messages and the language preferences (if any) are deleted. The user will need to be 're-provisioned' for Oracle Voicemail & Fax in order to be 're-enabled'.

The user object is deleted to ensure that the system can re-use the phone number of a disabled user. Users cannot log into Oracle Voicemail & Fax or use any of the Oracle Voicemail & Fax services while their accounts are de-provisioned.

Deleting User Accounts and Data

You can delete a user account. When you delete a user account, the user is de-provisioned from all provisioned applications. Additionally, the base user information is removed from Oracle Internet Directory. Once a user account has been deleted, the only way to recover that user account is to restore a backup of Oracle Internet Directory, and then re-provision the user account for applications.

When a user account is deleted, certain types of stored application data is retained in the system. This data includes e-mail messages stored by Oracle Mail, files stored in Oracle Content Services, and voice mail messages stored by Oracle Voice Mail & Fax.

Applications which do not directly store user data, or which are not directly provisioned for users, are not listed below. For example, users are not directly provisioned for Oracle Discussions; rather, Oracle Discussions data are stored in the Oracle Mail schema, and you perform data deletion processes by using the Oracle Mail deletion procedure.

Note: Your organization may be legally required to retain certain types of electronic communications and records for certain amounts of time. Oracle has designed the user deletion process in Oracle Collaboration Suite to assist you with this task.

Most types of user data are retained in the system unless explicitly deleted, either by a user or by performing special data removal procedures for each Oracle Collaboration Suite application which retains user data after an account is deleted.

Deleting a User Account

Note: If you do not have the privileges to delete a user entry, then the **Delete** button does not appear, and you cannot perform this operation.

To delete a user entry:

1. Select the **Directory** tab, then **Users**.

2. In the Search for user window, perform a search for the user whose entry you want to delete.
3. Select the user account and click **Delete**. A confirmation page loads.
4. Select **Yes** to delete the account. Select **No** to cancel.

Removing User Data from Oracle Calendar

Deleting a user causes all Oracle Calendar user data to be deleted. See "Calendar User Account Deprovisioning" in Chapter 7 of *Oracle Calendar Administrator's Guide* for more information about Oracle Calendar de-provisioning.

Removing User Data from Oracle Content Services

Because all files in Oracle Content Services reside in Libraries, users do not own content. All content belongs to the Library in which it is located. When users are deleted from Oracle Content Services, any data that was uploaded by that user remains in the Oracle Content Services repository.

In some cases, you may want to delete the Personal Library of a deleted user. To do this, you must sign on to Oracle Content Services as a user with the Library Administrator role and switch to Administration Mode. You can then navigate to the appropriate Personal Library and delete it.

Removing User Data from Oracle Mail

For complete information on removing user data from Oracle Mail, see "Clearing Data from the Oracle Collaboration Suite Database" in Appendix D of *Oracle Mail Administrator's Guide*.

Removing User Data from Oracle Real-Time Collaboration

For information about removing Oracle Real-Time Collaboration user data, see "Deleting User Data from the Oracle Real-Time Collaboration Database" in Appendix D of *Oracle Real-Time Collaboration Administrator's Guide*.

Removing User Data from Oracle Voicemail & Fax

When a user is deleted from Oracle Voicemail & Fax, the user's existing voice mail messages stored in the system will not be deleted. However, the user's greeting messages and the language preferences (if any) are deleted. The user will need to be 're-provisioned' for Oracle Voicemail & Fax in order to regain access to stored voice mail messages.

Oracle Collaboration Suite Application-Specific User Attributes

Oracle Calendar, Oracle Mail, and Oracle Voicemail & Fax have user attributes in addition to the General user attributes. When you create or modify user entries, after you specify the General user attributes, you can specify these application-specific attributes.

[Table 4-2, "Oracle Calendar User Attributes"](#), [Table 4-3, "Oracle Mail User Attributes"](#), and [Table 4-4, "Oracle Voicemail & Fax User Attributes"](#) list those attributes, along with their default and available values and a description of each attribute.

See Also: ["Managing Oracle Collaboration Suite Application-Specific Attribute Defaults"](#) on page 4-26 for instructions on how to change the application-specific attribute default values

Table 4–2 Oracle Calendar User Attributes

Component/Field	Default Value	Available Values	Description
Calendar Storage ¹	Based on policy	Default, select from list of available storage	Which Calendar storage to use for storing this user's Calendar data
Calendar Access	TRUE	TRUE, FALSE	Use this option to enable or disable the user's access to Calendar
Publish Status	Not Published	Not Published, Published	Determines whether this user's agenda information is visible to other calendar users
Enable Global agenda view	TRUE	TRUE, FALSE	Determines whether the user's agenda information can be made visible to other people on the web
Reminder Delivery Rule	Alternate	Alternate, Primary	Determines whether e-mail reminders should be sent to the user's alternate or primary e-mail address
Alternate E-mail Address	null	user entry	Specifies the user's alternate e-mail address for reminder delivery
Enable Alert	FALSE	TRUE, FALSE	Use this option to enable or disable alerts
Suspend Alert	FALSE	TRUE, FALSE	Temporarily disable alerts for a specified period
Suspend Alert period	00:00-00:00	Hours:minutes-Hours:minutes	Specify duration for alerts to be suspended
Alert Suspension Period Action	Send Alerts	Discard Alerts, Hold Alerts, Send Alerts	During alert suspension period, option determines what should happen to outgoing alerts
Send Alert on Meeting	TRUE	TRUE, FALSE	Determines whether this user will receive an alert when a meeting is created or modified
Send Alert on Day Event	FALSE	TRUE, FALSE	Determines whether this user will receive an alert when a day event is created or modified
Send Alert on Daily Note	FALSE	TRUE, FALSE	Determines whether this user will receive an alert when a daily note is created or modified

Table 4–2 (Cont.) Oracle Calendar User Attributes

Component/Field	Default Value	Available Values	Description
Send Alert on Journal	FALSE	TRUE, FALSE	Determines whether this user will receive an alert when a journal entry is created or modified
Send Alert on Owned Event	TRUE	TRUE, FALSE	Determines whether this user will receive an alert when an event owned by this user is created or modified
Send Alert on Declined Event	FALSE	TRUE, FALSE	Determines whether this user will receive an alert when an event that was previously declined is modified

¹ This is a required field

Table 4–3 Oracle Mail User Attributes

Component/Field	Default Value	Available Values	Description
E-mail Quota (M) ¹	38	Numbers (Megabytes)	Size of user's allocated storage on the server
Information Store	null	Default, <list of available>?	If there are multiple Information storage units, select one for this user
User Status	Active	Active, Inactive	An Active user is a user with all permissions to access. An Inactive user cannot access the mail system at all. However, messages sent to an Inactive account are stored in the information store and can be accessed once the account is activated.
Auto Reply Mode	null	Echo, Reject, Reply, Vacation	Users can modify their reply mode. Echo replies with a copy of the sender's message along with the Auto Reply Text. Reject rejects all incoming messages. Reply replies to every incoming message with the Auto Reply Text only. Vacation replies with only one message per sender, with the Reply Text.
Auto Reply Text	null	user entry	If the Auto Reply Mode is set to Reply, this text will be included in the Reply message.
Auto Reply Expiration	null	mm/dd/yyyy	This date sets when Auto Reply Mode will switch back to normal delivery mode.

Table 4–3 (Cont.) Oracle Mail User Attributes

Component/Field	Default Value	Available Values	Description
Forward E-mail Address	null	user entry	When Forward E-mail Address attribute is set with an e-mail address, all messages will be forwarded to this e-mail address. If this attribute is blank, messages will not be forwarded.
Text Indexing	none	Disable, Enable	This setting determines whether Search functions will access message body and attachments, or just sender and subject lines.
Role	User	Domain Administrator, System Administrator, User	Specifies the permissions for this user: A domain administrator will have permissions to administer and configure Oracle Mail within a particular domain; A system administrator will have permissions to administer and configure the entire Oracle Mail system; A user will only have permissions to access, read, and send e-mail and voice mail messages.
Archive Policy	Null	<any existing archive policy name>	Enter an archive policy name to enable an offsite, third-party message storage solution. See "Oracle Mail Archive Policies" in chapter 8 of the <i>Oracle Mail Administrator's Guide</i> for details.

¹ This is a required field

Table 4–4 Oracle Voicemail & Fax User Attributes

Component/Field	Default Value	Available Values	Description
International Phone Number ¹	null	user entry	Enter a unique phone number for this voice mail user.
Group Name ¹	null	list of available groups	Assign the user to one of the available groups.
Voicemail Password ¹	null	user entry	Create or reset the user's password.
Confirm Password ¹	null	user entry	Enter the password again in this box. The password must match the Voicemail Password exactly.

Table 4–4 (Cont.) Oracle Voicemail & Fax User Attributes

Component/Field	Default Value	Available Values	Description
Voice Preferred Language	null	American English, Arabic, Brazilian Portuguese, British English, Danish, Dutch, Finnish, French, German, Greek, Italian, Japanese, Korean, Mandarin-China, Mandarin-Taiwan, Norwegian, Portuguese, Spanish, Swedish, Turkish	Select the language to be used for the voice mail user's voice prompts.
Phone Access Allowed	null	true, false, Group Default	You can enable or deny voice mail access to the user or have the user inherit this setting from the user's group.
Faxin Access Allowed	null	true, false, Group Default	You can enable or deny fax access to the user or have the user inherit this setting from the user's group.
Message Waiting Indicator	null	true, false, Group Default	If the user's phone has a message waiting indicator and this option is enabled, the system turns the message waiting indicator on to let the user know there is a new voice mail message. Setting it to the Group Default causes the user to inherit the setting from the user's group.
Additional Voice Quota	null	Numbers (bytes)	Voice mails are counted against the user's e-mail quota. You can use this setting to allocate additional storage for both e-mail and voice mail messages. This can help prevent large voice mail messages from filling up the user's e-mail quota.

¹ This is a required field

Managing Group Entries Using the Provisioning Console

This section describes how to use the Provisioning Console to create, modify, and delete group entries and to assign privileges to groups. It contains the following topics:

- [Creating Group Entries](#)
- [Modifying Group Entries](#)
- [Deleting Group Entries](#)
- [Assigning Privileges to Groups](#)

Creating Group Entries

To create a group entry:

1. Select the **Directory** tab, then select **Groups**.
2. Choose **Create**. This displays the Create Group window.
3. In the Create Group window, in the **Basic Information** section, in the **Name** field, enter the name for this group.
4. In the **Display Name** field, enter the friendly name for this group. For example, if the RDN is `OracleDBCreators`, then you could enter the display name as `Oracle Database Creators`.
5. Optionally, in the **Description** field, enter a brief description of this group.
6. To hide this group entry from all but its owners, in the **Group Visibility** field, select **Private**. Otherwise, accept the default, namely, **Public**.
7. Configure owners of this group. Note that the creator of the group is automatically a group owner.

To add a user as an owner of this group:

- a. In the **Owners** section, choose **Add User**. This displays the Search and Select: User window.
- b. Search for the entry of the user you want to add as an owner of the group.
- c. Choose **Select**. This returns you to the Create Group window. The user you specified is listed in the **Owners** section.

To add a group as an owner of this group:

- a. In the **Owners** section, choose **Add Group**. This displays the Search and Select: Group window.
- b. Search for the entry of the group you want to add as an owner of the group.
- c. Choose **Select**. This returns you to the Create Group window. The group you specified is listed in the **Owners** section.

To remove a user or group as an owner of this group, select the user or group, then choose **Remove**.

8. Configure members of this group.

To add a user as a member of this group:

- a. In the **Members** section, choose **Add User**. This displays the Search and Select window.
- b. Search for the entry of the user you want to specify as a member of this group.
- c. Choose **Select**. This returns you to the Create Group window. The user you specified is listed in the **Members** section.

To remove a user from this group, in the **Members** section, select the user's name and choose **Remove**.

To add a group as a member of this group:

- a. In the **Members** section, choose **Add Group**. This displays the Search and Select window.
- b. Perform a search for the entry of the group you want to specify as a member of this group, then choose **Select**. This returns you to the Create Group window. The group you specified is listed in the **Members** section.

9. You can assign roles to this group.

To specify the roles that you want to assign to this group, in the **Roles Assignment** section, in the **Select** column, select the role that you want to assign to this group.

To remove the role from the group, in the **Roles Assignment** section, in the **Select** column, deselect the role that you want to remove from this group.

Modifying Group Entries

To modify a group entry:

1. Select the **Directory** tab, select Groups, then perform a search for the group entry you want to modify.
2. From the search results, select the group entry you want to modify.
3. Choose **View Manage**. This displays the Manage Group window.
4. Choose **Edit**. The Edit Group window appears.
5. In the Edit Group window, modify the fields as described in ["Creating Group Entries"](#) on page 4-22.
6. Choose **Submit**.

Deleting Group Entries

To delete group entries:

1. Select the **Directory** tab, select **Groups**, then perform a search for the group whose entry you want to delete.
2. From the search results, select the group whose entry you want to delete.
3. Choose View/Manage. This displays the Manage Group window.
4. In the Manage Group window, choose **Delete**. The Confirmation of Deletion window appears.
5. In the Confirmation window, choose either Yes or No.

Assigning Privileges to Groups

You can assign or revoke privileges for groups. The privileges available are described in [Table 4-5, "Group Privileges"](#) on page 4-24.

Note: You can also assign and revoke privileges for users directly. However, many organizations find that it is easier to manage privileges for users by assigning them to groups which have the desired privileges, rather than assigning and revoking privileges directly for each user.

For instructions on how to assign and revoke privileges to users, see ["Assigning Privileges to Users"](#) on page 4-13.

Table 4-5 Group Privileges

Privilege	Description of Access Granted
Allow user creation	Create user entries
Allow user editing	Modify user entries

Table 4–5 (Cont.) Group Privileges

Privilege	Description of Access Granted
Allow user deletion	Delete user entries
Allow group creation	Create group entries
Allow group editing	Modify group entries
Allow group deletion	Delete group entries
Allow privilege assignment to users	Assign access rights to users
Allow privilege assignment to groups	Assign access rights to groups
Allow service management	Enable group members to manage services for users. If this is selected, then a Services link becomes available in the Directory tab page when the latter is accessed by group members.
Allow account management	Enable group members to manage services for users. If this is selected, then an Accounts link becomes available in the Directory tab page when the latter is accessed by group members.
Allow Oracle Delegated Administration Services configuration	Configure Oracle Delegated Administration Services user interface
Allow resource management for Oracle Reports- and Forms-based applications	Enable users to configure resources—such as databases or applications—to which access is allowed
Allow User Management and Application Provisioning	Allows provisioning users; also automatically enables user account creation, editing, and deletion access

To assign or revoke privileges to a group:

1. Select the **Directory** tab, then **Groups**.
2. Perform a search for the entry of the group to which you want to assign or revoke privileges.
3. From the search results list, select the desired group, then choose **Assign Privileges**. The Assign Privileges to Group window displays a list of privileges.
Select the privileges you want to assign to this group. De-select privileges you want to revoke from this group.
4. Select **Submit** to assign or revoke privileges as shown.

Configuring User Account Creation Using the Provisioning Console

There are several options for customizing the user account creation process. This section contains the following topics:

- [Managing Oracle Collaboration Suite Application-Specific Attribute Defaults](#)
- [Configuring the Self-Service Console for User Management](#)
- [Setting Default Provisioning Policies](#)

Managing Oracle Collaboration Suite Application-Specific Attribute Defaults

Several of the Oracle Collaboration Suite applications provide a list of custom user attributes which are exposed when you provision a user for that application. Each application attribute has a default value. Complete lists of attributes and their default values for each application are shown in [Table 4-2, "Oracle Calendar User Attributes"](#) on page 4-19, [Table 4-3, "Oracle Mail User Attributes"](#) on page 4-20, and [Table 4-4, "Oracle Voicemail & Fax User Attributes"](#) on page 4-21.

You can set the default attribute for each custom field. The default settings will appear in the Component Attributes window any time a new user is created. Changing defaults will not affect existing users, even if those users were created using previous default values.

To make changes to the default attribute values:

1. Select the **Directory** tab, and then select **Applications**. The Manage Defaults: Select Application screen is shown.
2. Select the applications corresponding to the default attributes you wish to modify. You cannot select an application which has no user attributes. Select **Continue** to display the Manage Defaults: Attributes screen.
3. On the Manage Defaults: Attributes screen, enter the new default value for any attribute displayed. When you are finished making changes, select **Submit** to apply your changes.

Configuring the Self-Service Console for User Management

When a user creates or edits a user entry, the Self-Service Console displays various categories—including, for example, basic information, password, and photo—each with its own set of attributes. You can specify which of these categories the console displays, how it displays them and their corresponding attributes, and which can be edited by users themselves.

Specifically, you can:

- Associate object classes with user entries, and add and modify these object classes
- Specify the categories of attributes you want to enable users to add or modify
- Customize the way the Self-Service Console displays those categories and attributes

To configure user entries:

1. Select the **Configuration** tab, then select **User Entry**. This displays the Configure User Object Classes window listing the existing object classes associated with user entries.
2. To add an **object class** for user entries:
 - a. In the Configure User Object Classes window, choose **Add Object Class**. This displays the All Object Classes window.
 - b. Select an object class you want to add, then choose **Add**. This returns you to the Configure Object Class window. The object class you just chose is now listed as an object class for user entries.
 - c. To add more object classes, repeat these steps, or, to move to the next step, choose **Next** to display the Configure User Attributes window.
3. The Configure User Attributes window lists some—but not all—of the attributes of the object classes you specified in Step 2 on page 4-26. There may be other

attributes belonging to those object classes as well. You can add as many of those other attributes as you wish by following the instructions in this step. You can modify how the attributes are displayed or delete attributes.

To add attributes to user entries:

- a. In the Configure User Attributes window, choose **Add New Attribute**. This displays the Add New Attribute window.
- b. In the Add New Attribute window, enter values for the fields.
- c. Choose **Done**. This returns you to the Configure User Attributes window. The attribute you just chose is now listed in the attribute list.
- d. To add more attributes, repeat these steps.

To modify the display of attributes:

- a. In the Configure User Attributes window, in the **Directory Attribute Name** column, select the attribute you want to modify, then choose **Edit**. This displays the Editing Attribute window.
- b. In the Editing Attribute window, enter values for the fields.
- c. Choose **Done**. This returns you to the Configure User Attributes window. The attribute configurations you just made are now reflected in the Directory Attribute Name list.
- d. To configure or modify more attributes, repeat these steps.

To delete attributes of user entries, in the Configure User Attributes window, in the **Directory Attribute Name** list, select the attribute you want to configure, then choose **Delete**.

4. To customize the display of categories, in the Configure User Attributes window choose **Next** to display the Configure Attribute Categories window. This window contains a table listing the existing categories, the name displayed to the user, and the display order of each category.
 - a. To add a new category, choose **Create**. This displays the Create window. In the **UI Label** field, enter the name of the category as you would like it displayed in the interface.
 - b. To modify the display name of a category, in the **UI Label** column, edit the field for each attribute you want to modify.
 - c. To set the display order of categories, choose **Order Category**. The Order Category window displays the various categories you just specified. Use the up and down arrows to move the categories into the desired order.
 - d. To set the display order of attributes for each category, select the category, then choose **Edit**. In the Order Category window, use the arrow buttons to set the display order of the attributes, or to remove an attribute from being displayed.
 - e. To delete a category, select the category, then choose **Delete**.

When you have finished configuring attribute categories, choose **Next** to display the Configure Search Table Columns window.

5. When a user performs a search, the results are displayed in a table. You can specify the number of columns in that table and their headings. To configure search table columns:

- a. In the Configure Search Table Column window, in the **All Attributes** box, select one or more attributes that you want to be represented in the search results. These will serve as column headings in the search results table.
- b. Use the left-right arrows to move the attributes to the **Selected Attributes** box.
- c. In the **Selected Attributes** box, order the attributes by using the up-down arrows to the right of the box. The first attribute in the list represents the column farthest to the left in the search results table.

When you have finished configuring the search results table, choose **Next** to display the Configure Roles window.

6. To enable users to assign roles to users, in the Configure Roles window, in the **Enable Roles** category, select Enable Role assignment in the user management interface.

You can specify the roles that users can assign to other users.

To add a role that users can assign to other users:

- a. Choose **Add Role** to display the Search and Select: Roles window.
- b. In the **Group Name Begins With** field, enter the first few letters of the name of the administrative group you want to add.
- c. From the search results, select the name of the administrative group you want to add, then choose **Select**. This returns you to the Configure Roles window. The administrative group you just selected appears in the Roles list.

To delete a role, select it from the table and choose **Delete**.

7. When you have finished configuring user entries, choose **Finish**.

Setting Default Provisioning Policies

A provisioning policy is a set of rules that determines whether, and how, a given user will be provisioned for available Oracle Collaboration Suite applications. Oracle Delegated Administration Services implements the policy each time a user account is created, edited, or deleted. The action of creating or modifying a user account triggers the provisioning policy.

A default provisioning policy is set during installation of Oracle Collaboration Suite. This property, the `DEFAULT_PROVISIONING_POLICY` may be updated using the provisioning tool `$ORACLE_HOME/bin/oidprovtool`. The default provisioning policy for Oracle Collaboration Suite specifies that new users should be provisioned for all available (configured) Oracle Collaboration Suite applications. When you create a new user individually using the Provisioning Console, you can override this policy for each available Oracle Collaboration Suite application.

See Also: For more information about default provisioning policies and the `oidprovtool`, see [Appendix C, "User Provisioning Java API"](#).

You can create a new default provisioning policy that is triggered for every user that is created for some Oracle Collaboration Suite applications. This policy can inspect whether the user should be provisioned for the particular application or not, based on specified business requirement logic. It can also be used to set or override the default values of application-specific user attributes.

Custom policies are supported in the form of a plug-in that a developer can write after installation and initial configuration. When administrators create new accounts, they always have the privilege to override the policy.

See Also: ["Java Plug-ins for User Provisioning"](#) on page C-17

[Table 4–6](#) shows the way the various Oracle Collaboration Suite applications use the provisioning framework to perform user provisioning. This is the out-of-the-box behavior. You can alter this behavior and implement business policies by implementing or altering the pre- and post-data entry plug-ins. However, you cannot alter the provisioning plug in. If an application already has a pre- or post-data entry plug-in, you should not attempt to modify the existing plug-in; doing so could cause the plug-in to stop working, disabling provisioning. However, you can write your own pre- and post-data entry plug-ins for those applications which do not already have them.

See Also: [Table C–2, "Interfaces and Their Configuration"](#) on page C-7

Table 4–6 Oracle Collaboration Suite Application Provisioning Plug-in Implementation

Application	Provisioning Mode	Provisioning Plug-in Type	Pre-Data Entry Plug-in	Post-Data Entry Plug-in
Oracle Mail	Synchronous	Data Access Plug-in	Yes	Yes
Oracle Voicemail & Fax	Synchronous	Data Access Plug-in	Yes	Yes
Oracle Content Services	Asynchronous	PLSQL	No	No
Oracle Real-Time Collaboration	Asynchronous	PLSQL	No	No
Oracle Calendar	Asynchronous	PLSQL	No	Yes
Oracle Mobile Collaboration	Asynchronous	PLSQL	No	No

Managing Provisioning Profiles

Use the Provisioning Subscription Tool to perform these activities:

- Create a new provisioning profile. A new provisioning profile is created and set to the enabled state so that the Oracle Directory Integration and Provisioning platform can process it
- Modify an existing provisioning profile
- Enable or disable an existing provisioning profile
- Delete an existing provisioning profile
- Get the current status of a given provisioning profile
- Clear all of the errors in an existing provisioning profile

Use the Oracle Internet Directory Server Manageability functionality in the Oracle Collaboration Suite Control to monitor provisioning profiles.

The Provisioning Subscription Tool shields the location and [schema](#) details of the provisioning profile entries from the callers of the tool. From the callers' perspective, the combination of an application and a subscriber uniquely identify a provisioning

profile. The constraint in the system is that there can be only one provisioning profile for each application for each subscriber.

Note: To run shell script tools on the Windows operating system, you need one of the following UNIX emulation utilities:

- Cygwin 1.3.2.2-1 or later. Visit: <http://sources.redhat.com>
 - MKS Toolkit 6.1. Visit: <http://www.datafocus.com/>
-

The name of the executable is `oidProvTool`, located in `ORACLE_HOME/bin`. To invoke this tool, use this command:

```
oidprovtool param1= param1_value param2= param2_value param3= param3_value ...
```

The Provisioning Subscription Tool accepts the following parameters:

Table 4–7 Provisioning Subscription Tool Parameters

Name	Description	Operations	Mandatory/Optional
operation	The subscription operation to be performed. The legal values for this parameter are: create, enable, disable, delete, status and reset. Only one operation can be performed for each invocation of the tool.	All	M
ldap_host	Host-name of the directory server on which the subscription operations are to be performed. If not specified, the default value of 'localhost' is assumed.	All	O
profile_status	The status of the profile (ENABLED/DISABLED). Default is ENABLED	Create	O
profile_mode	INBOUND/OUTBOUND/BOTH. Default is OUTBOUND	Create	O
profile_debug	The debugging level with which the profile is executed by the Oracle directory integration and provisioning server.	All	O
sslmode	Indicator of whether to execute the Provisioning Subscription Tool in SSL mode. A value of 0 indicates non-ssl and 1 indicates SSL mode.	All	O
ldap_port	The TCP/IP port on which the Oracle directory server is listening for requests. If not specified, the default value of '389' is assumed.	All	O
ldap_user_dn	The LDAP distinguished name (DN) of the user on whose behalf the operation is to be performed. Not all users have the necessary permissions to perform Provisioning Subscription operations. Please see the administrative guide to grant or deny LDAP users the permission to perform Provisioning Subscription operations.	All	M
ldap_user_password	The password of the user on whose behalf the operation is to be performed.	All	M

Table 4–7 (Cont.) Provisioning Subscription Tool Parameters

Name	Description	Operations	Mandatory/Optional
application_dn	The LDAP distinguished name of the application for which the Provisioning Subscription Operation is being performed. The combination of the application_dn and the organization_dn parameters help the subscription tool to uniquely identify a provisioning profile.	All	M
organization_dn	The LDAP distinguished name of the organization for which the Provisioning Subscription Operation is being performed. The combination of the application_dn and the organization_dn parameters help the subscription tool to uniquely identify a provisioning profile.	All	M
interface_name	Database schema name for the PLSQL package. Format of the value should be: [Schema].[PACKAGE_NAME]	Create only	M
interface_type	The type of the interface to which events have to be propagated. Valid Values: PLSQL (if not specified this is assumed as the default)	Create only	O
interface_connect_info	Database connect string Format of this string:[HOST]:[PORT]:[SID]:[USER_ID]:[PASSWORD]	Create only	M
interface_version	The version of the interface protocol. Valid Values: 1.0 or 1.11.0 will be the old interface. If not specified, this is used as the default.	Create only	O
interface_additional_info	Additional information for the interface. This is not currently used.	Create only	O
schedule	The scheduling information for this profile. The value is the length of the time interval in seconds after which DIP will process this profile. If not specified, a default of 3600 is assumed.	Create only	O
max_retries	The number of times the Provisioning Service should retry a failed event delivery. If not specified, a default value of 5 is assumed.	Create only	O
event_subscription	Events for which DIP should send notification to this application. Format of this string:"[USER]GROUP]:[<Domain of interest>]:[DELETE]ADD]MODIFY(<list of attributes separated by comma>)]"Multiple values may be specified by listing the parameter multiple times each with different values. If not specified the following defaults are assumed:USER:<org.DN>:DELETEDGROUP:<org.DN>:DELETEDeqQthat is, send user and group delete notifications under the organization DN.	Create only	O

Changing the Default Password Policies

Oracle Collaboration Suite sets up basic password policies by default during installation. For example, by default all passwords expire (and must be changed) after 60 days. You can change the password policies by using Oracle Directory Manager to edit the Oracle Internet Directory.

To change the password policies:

1. Start the Oracle Directory Manager:

Unix:

```
ORACLE_HOME/bin/oidadmin
```

Windows:

```
Start > Programs > Oracle Application Server > OracleHome >  
Integrated Management Tools > Oracle Directory Manager
```

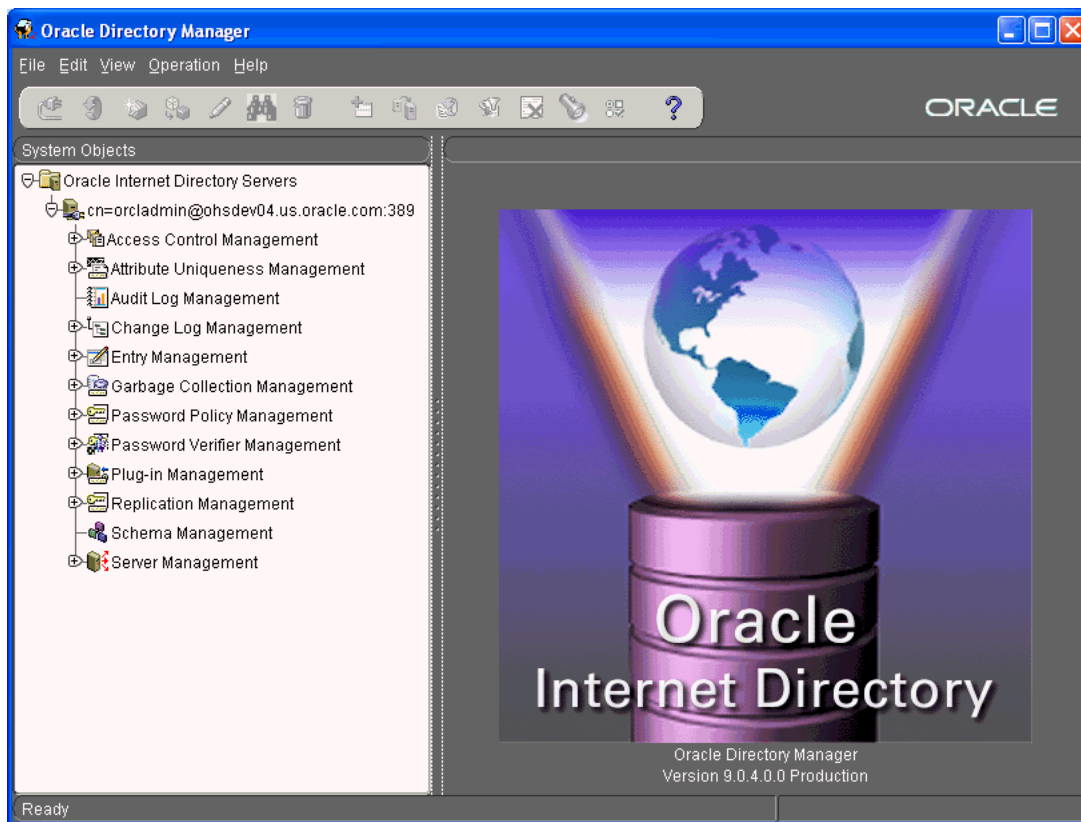
2. When you start Oracle Directory Manager, it will prompt you for connection information. Enter the following information to connect to your Oracle Internet Directory, typically hosted in the Oracle Collaboration Suite Database on your Oracle Collaboration Suite Infrastructure:

```
Host: <infrahost.yourdomain.com>  
Port: 389  
Username: cn=orcladmin  
Password: <password>
```

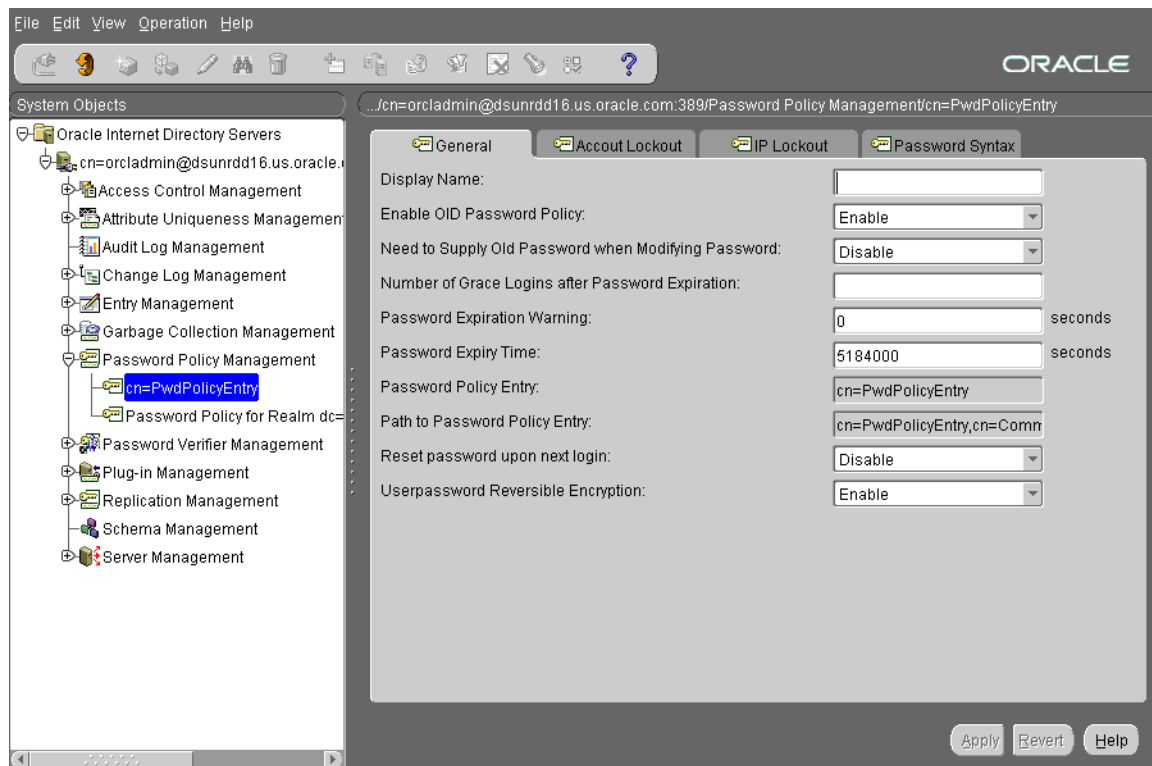
Port 389 is the default port used by Oracle Internet Directory. You may be using a different port. If so, enter the correct Oracle Internet Directory port.

If you have configured your Oracle Internet Directory to be accessed using Secure Socket Layers (SSL), select the **SSL Enabled** checkbox. Otherwise, leave it blank.

3. Select **Login** to log in to the Oracle Internet Directory. When the connection is successful, the Oracle Internet Directory management screen is displayed. See [Figure 4-8, "Accessing Oracle Internet Directory with Oracle Directory Manager"](#) on page 4-33.

Figure 4–8 Accessing Oracle Internet Directory with Oracle Directory Manager

4. Expand **Password Policy Management** to display the policy management objects. You will see one entry called `cn=PwdPolicyEntry`, and one additional entry for each Realm in your deployment. [Figure 4–9](#) shows the `PwdPolicyEntry` object.

Figure 4–9 Password Policy Management in Oracle Internet Directory

5. Make changes to the password policy fields as required. You can specify policies for all realms at once by editing the PwdPolicyEntry object, or you can specify specific policies for each realm by editing each Password Policy for Realm . . . object. Password policies specified in the PwdPolicyEntry object do not override password policies specified in any specific realm. Therefore, if you make a change to the PwdPolicyEntry object, it may not affect one or more realms that already have existing password policies specified.
6. After making changes to the password policies, your changes will not appear in the Oracle Internet Directory Provisioning Console until you refresh the user entry page. To do this, from the Provisioning Console, select the **Configuration** tab, and then click **User Entry**. On the User Entry page, click the refresh icon to refresh the page. This will cause the Provisioning Console to read your changes to the password policies and update the page

The following tables provide descriptions of the fields in the password policy management objects.

Table 4–8 Fields in the Password Policies General Tab Page

Field	Description
Enable OID Password Policy	To disable the default Oracle Collaboration Suite password policy, select Disable. The default is Enable.
Need to Supply Old Password When Modifying Password	Specify whether user must supply old password with new one when modifying password. By default, the old password is not required.
Number of Grace Logins after Password Expiration	Maximum number of grace logins allowed after a password expires. By default, no grace logins are allowed. The default value is 3.

Table 4–8 (Cont.) Fields in the Password Policies General Tab Page

Field	Description
Reset password upon next login	Indicator of whether users must change their passwords after the first login, or after the password is reset by the administrator. Enabling this option requires users to change their passwords even if user-defined passwords are disabled. By default, users need not change their passwords after reset.
Password Expiration Warning	Enter the number of seconds in which users must modify their passwords before those passwords expire. The directory server sends a password expiration warning if these two conditions are met: ■ The attribute for the expiry time for a user's password is set ■ This attribute is also enabled From that point, the user has a specified number of seconds in which to modify the password. If the user does not modify the password within the specified number of seconds, then the password expires and the user is locked out until the password is changed by the administrator. For example, suppose that: ■ The Password Expiry Time is set to 7200—that is, your password expires after 2 hours ■ The Password Expiration Warning is set to 3600—that is, 1 hour In this example, if you log in during the last hour, then you receive a warning that your password is about to expire. If you do not modify your password during that time, then your password expires and you are locked out of your account until the administrator changes your password. For this feature to work, the client application must support it. The default is 0, which means no warnings are sent.
Password Expiry Time	Enter the number of seconds that a given password is valid. For example, if you set the value of this attribute to 7200, then the password expires in two hours from the time that you set it. If this attribute is not present, or if the value is 0, then the password does not expire. By default, passwords expire in 60 days.
Password Policy Entry	This field displays the RDN of the password policy entry. You cannot edit this field.
Path to Password Policy Entry	This field displays the full DN of the password policy entry. You cannot edit this field.

Table 4–9 Fields in the Password Policies Account Lockout Tab Page

Field	Description
Global Lockout Duration	Enter the number of seconds a user is locked out of the global directory if both of the following are true: - Global lockout is enabled - The user has been unable to log in successfully for at least the number of times specified by <code>pwdMaxFailure</code> You can set user lockout for a specific duration, or until the administrator resets the user's password. The default value is 24 hours. A user account stays locked even after the lockout duration has passed unless the user logs in with the correct password.
Password Failure Count Interval	Enter the number of seconds after which the password failure times are purged from the user entry.
Password Maximum Failure	Enter the number of consecutive failed log in attempts after which a user account is locked.

Table 4–10 Fields in the Password Policies IP Lockout Tab Page

Field	Description
IP Lockout Duration	Specify the number of seconds you want to enforce account lockout for a specific IP address. A user account stays locked even after the lockout duration has passed unless the user logs in with the correct password.
IP Lockout Maximum Failure	Specify the maximum number of failed logins from a specific IP address after which the account is locked.

Table 4–11 Fields in the Password Policies Password Syntax Tab Page

Field	Description
Minimum Number of Characters of Password	Specify the minimum number of characters required in a password.
Number of Numeric Characters in Password	Specify the number of numeric characters required in a password.
Number of Password History	Specify how many of a user's previous passwords the directory server is to store. If a user attempts to reuse one of the passwords the directory server has stored, then the password is rejected. The directory server does not maintain a password history by default.
Password Illegal Values	Enter the common words and attribute types whose values cannot be used as a valid password. By default, all words are acceptable password values.

Searching for Entries Using the Provisioning Console

This section describes how to use the Provisioning Console to search for user and group entries. It contains the following topics:

- [Searching for User Entries](#)
- [Searching for Group Entries](#)

Searching for User Entries

To search for user entries:

1. In the Oracle Internet Directory Self-Service Console, select the **Directory** tab, then select **Users**.
2. In the **Search for User** field, enter any part of one of the following:
 - First name
 - Last name
 - Login name
 - The e-mail identifier

For example, if you are searching for Anne Smith, you could enter Ann or Smi or ith.

To generate a list of all users in the directory, leave this field blank.
3. Select **Go** or press Enter to display the search results.

Searching for Group Entries

To search for a group entry:

1. Select the **Directory** tab, then select **Groups**. The Search for Groups window appears.
2. In the **Search Group Name** text box, enter any part of the name of the group for which you are searching.

To generate a list of all groups in the directory, leave this field blank.
3. Select **Go** or press Enter to display the entries that match the criteria you entered.

Managing Identity Management Realms Using the Provisioning Console

This section describes how to use the Provisioning Console to configure a [realm](#), modify those configurations, and create additional realms. Identity management realms are useful for segregating users into multiple separate domains. For example, if you have two user populations, each with e-mail addresses resolving to two separate e-mail domains, you might wish to create two [identity management realms](#) to manage them.

This section contains the following topics:

- [Configuring an Identity Management Realm](#)
- [Viewing Configuration Settings for an Identity Management Realm](#)
- [Modifying Configuration Settings for an Identity Management Realm](#)
- [Configuring the Parent Distinguished Name for Entries in a Realm](#)
- [Creating an Additional Identity Management Realm](#)

See Also: ["Setting Up and Enabling Multiple Realms"](#) on page 7-1

Configuring an Identity Management Realm

If you have the correct administrative privileges, then you can specify the following for an [identity management realm](#):

- The attribute by which you want users to identify themselves when they log in

- The root entries of the **user search base** and of the group search base—that is, the locations in the **directory information tree (DIT)** containing entries for users and groups
- The root entries for the user creation base and the group creation base—that is, the location in the DIT where users and groups are created. This can be the same as the user search base or a location under the user search base.
- The display of realm and product logos

To configure an identity management realm:

1. Select the **Configuration** tab.
2. In the Identity Management Realm window, enter values for the various fields.
3. Choose **Submit** to save your changes.

Note: Although you can enter more than one value in the **User Search Base** field, doing so can degrade performance.

Viewing Configuration Settings for an Identity Management Realm

To view the configuration settings of an identity management realm:

1. Select the Configuration tab.
2. At the top right of the Self-Service Console, choose the **Realm Management** icon. This displays the Identity Management Realms window.
3. In the Identity Management Realms window, in the **Search Identity Management Realm** field, enter all or part of the name of the realm whose entry you want to view, then choose **Go**. This displays a list of realms that match your search criteria.
4. From the search results list, select the realm you want to modify, then choose **View**. This takes you to the Identity Management Realm window where you can view the configuration settings.

Modifying Configuration Settings for an Identity Management Realm

You can modify the settings of an identity management realm for which you are the administrator. To do this:

1. Select the Configuration tab.
2. In the Identity Management Realm window, enter values for the various fields.
3. Modify the fields, then choose **Submit**.

Configuring the Parent Distinguished Name for Entries in a Realm

You can specify one or more parent distinguished names (DNs) for entries in a realm. If you specify more than one, then a delegated administrator can choose the one under which to place a new user entry.

There are two ways to specify a parent **distinguished name (DN)**. The first is by specifying values for the user creation base, and the second is by specifying values for the organizational units (**ou**) attribute. If you specify a different set of values for each, then those for the **ou** attribute prevail.

To specify parent DNs by providing values for the User Creation Base:

1. Select the **Configuration** tab, then select **Identity Management Realm**.
2. In the **User Creation Base** field, enter one or more DNs, one line for each DN.
3. Choose **Submit**.

Alternatively, you can specify parent DNs by setting the value for the organizational unit (ou) attribute. If you do this, then a delegated administrator can choose the organization unit under which to place user entries. To specify a parent DN by using this method:

1. Select the **Configuration** tab, then select **User Entry**.
2. Choose **Next**. The Configure User Attributes window appears.
3. Choose **Add New Attribute**. The Add New Attribute window appears.
4. In the Add New Attributes window, from the **Directory Attribute Name** list, select the ou attribute.
5. From the **UI Type** list, select **Predefined List**.
6. In the **LOV Values** field, enter the display name of the parent DN, followed by three semicolons (;), followed by the DN itself.

For example:

```
Sales;;;cn=users,dc=us,dc=my_company,dc=com
HR;;;cn=groups,dc=us,dc=my_company,dc=com
```

Following this example, when a delegated administrator chooses the organizational unit under which to place a user entry, she selects from a list displaying **Sales** and **HR**.

You can add more parents DNs, one line for each.

Creating an Additional Identity Management Realm

If you have the administrative privileges, then you create an entry for an identity management realm as follows:

1. Select the Configuration tab.
At the top right of the Oracle Internet Directory Self Service Console, choose the **Realm Management** icon. This displays the Identity Management Realms window.
2. In the Identity Management Realms window, choose **Create**. The Create Identity Management Realm window appears.
3. In the Create Identity Management Realm window, enter the appropriate values in the fields.
4. Choose **Submit**.

Managing Oracle Collaboration Suite Applications

This chapter provides a summary of the tools available for managing the various Oracle Collaboration Suite components. It is primarily comprised of short descriptions of the tools and tasks related to each component, along with direct links to detailed information in the component documentation.

This chapter describes the administration of the following Oracle Collaboration Suite components in detail:

- Oracle Discussions
- Oracle Collaboration Suite Search
- End-User Documentation Portal
- Oracle Web Access Client
- Oracle Workspaces

This chapter contains the following topics:

- [Administrating Oracle Collaboration Suite Components using Component Administration Tools](#)
- [Overview of Typical Administration Tasks for Oracle Collaboration Suite Components](#)
- [Managing Oracle Collaboration Suite Search](#)
- [Managing Oracle Contacts](#)
- [Managing Oracle Discussions](#)
- [Managing the End-User Documentation Portal](#)
- [Managing Oracle Application Server Portal and Oracle Collaborative Portlets](#)
- [Managing Oracle Web Access Client](#)
- [Managing Oracle Workspaces](#)
- [Adding Applications to your Oracle Collaboration Suite Deployment](#)

Administrating Oracle Collaboration Suite Components using Component Administration Tools

This section introduces the various component-specific tools used to administer Oracle Collaboration Suite components. This section serves only as an introduction to these

tools. For detailed component administration instructions, see the relevant component Administrator's Guide.

This section includes the following topics:

- [Oracle Calendar Administration Tools](#)
- [Oracle Mail Administration Tools](#)
- [Oracle Content Services Administration Tools](#)
- [Oracle Real-Time Collaboration Administration Tools](#)
- [Oracle Voice Mail & Fax Administration Tools](#)
- [Oracle Mobile Collaboration Administration Tools](#)

Oracle Calendar Administration Tools

At the component level, Oracle Calendar offers two methods of administration. Administrators have the choice of using command-line utilities and the Oracle Calendar administrator.

Oracle Calendar Command-Line Utilities

The Oracle Calendar server comes with a number of command-line utilities that provide control over a wide range of Calendar server information, features, and administrative tasks. These command-line utilities are installed in the `$ORACLE_HOME/ocal/bin` subdirectory.

For a complete list of the utilities included for calendar and details on their operation, refer to Chapter 6, "Calendar Server Utilities" of the *Oracle Calendar Reference Manual*.

Oracle Calendar Administrator

The Oracle Calendar administrator is an on-line server management tool that allows users and administrators to manage user accounts, resources, event calendars, groups and holidays in the Calendar server database. In addition, the Oracle Calendar administrator provides easy access to basic system administration tasks such as viewing the status of calendar nodes and databases, and starting or stopping nodes and servers.

Access the Oracle Calendar Administrator by using the following URL:

`http://host_name:port/ocad-bin/ocad.cgi?object=nodeadm`

For more information on administering Oracle Calendar using the Oracle Calendar administrator, refer to the *Oracle Calendar Administrator's Guide*.

Oracle Mail Administration Tools

This section includes the following topics:

- [The Oracle WebMail Client](#)
- [Oracle Collaboration Suite Control Console](#)
- [Grid Control Console](#)
- [Oracle Mail Command-Line Utilities](#)

The Oracle WebMail Client

Use the Oracle WebMail client to manage Oracle Mail objects, including domains, users, distribution lists, aliases, newsgroups and peer servers, and filters and routing of mail.

Access the Oracle WebMail client at the following URL:

`http://host_name:port/um/traffic_cop`

Enter the host name of the system upon which Oracle Mail is installed and enter the Oracle Application Server Web Cache port number.

Click the appropriate sub-tab in the **Administration** tab of the Oracle WebMail client to perform domain, user, list, alias, news, and policy management tasks.

See Also:

- Chapter 4, "Oracle Collaboration Suite 10g WebMail Client" of *Oracle Mail Administrator's Guide* for more information about the Oracle WebMail client
- Chapter 2, "Managing Oracle Mail Objects" of *Oracle Mail Administrator's Guide* for information about administration tasks performed with Oracle WebMail

Oracle Collaboration Suite Control Console

Use the Oracle Collaboration Suite Control Console to administer the various Oracle Mail server processes located on the Applications tier, including Housekeeper, IMAP, NNTP Inbound and Outbound, POP, List Server, SMTP Inbound and Outbound, and Virus Scrubber.

See Also: Chapter 3, "Oracle Mail Server Processes" of *Oracle Mail Administrator's Guide* for more information about using the Oracle Collaboration Suite Control Console to administer Oracle Mail server processes

Grid Control Console

With Grid Control, you can monitor the performance of Oracle Mail and drill down to analyze specific performance metrics. The Grid Control Console provides a convenient grouping and summarization of Oracle Mail status and performance.

See Also: "Monitoring Oracle Mail Using Oracle Enterprise Manager 10g Grid Control Console" in Chapter 7 of *Oracle Mail Administrator's Guide* for more information about using Oracle Enterprise Manager Grid Control 10g to monitor Oracle Mail

Oracle Mail Command-Line Utilities

There are various utilities an administrator can employ from the command-line to perform various administrative tasks.

See Also: Appendix D, "Oracle Mail Command-Line Reference" of *Oracle Mail Administrator's Guide* for more information about Oracle Mail command-line utilities

Oracle Content Services Administration Tools

Oracle Content Services Administrator's Guide details a number of advanced administration tasks for Oracle Content Services. This section describes the various tools that you can use specifically to administer Oracle Content Services, along with links to relevant topics in other guides.

Oracle Content Services Administration Mode

Administrators of the Oracle Content Services application, such as Category or Container Administrators, can switch to Administration Mode in Oracle Content Services to perform administration tasks for their Site.

For detailed information about Oracle Content Services Administration Mode, see *Oracle Content Services Application Administrator's Guide*.

Oracle Content Services Command-Line Tools

You can use the Oracle Content Services command-line tools to create Oracle Content Services groups, update Oracle Content Services groups, create Libraries, and update Libraries. The Oracle Content Services command-line tools were formerly known as the Bulk Tools. See "Oracle Content Services Command-line Tools" in Chapter 9 of *Oracle Collaboration Suite Migration and Coexistence Guide* for more information.

Oracle Real-Time Collaboration Administration Tools

This section gives an overview of each of the tools administrators can use to manage the Oracle Real-Time Collaboration system and components. For more information, see Chapter 1, "Introduction to Oracle Real-Time Collaboration" of *Oracle Real-Time Collaboration Administrator's Guide*.

This section includes the following topics:

- [Oracle Real-Time Collaboration Configuration Utility](#)
- [Oracle Real-Time Collaboration Web Client for Administrators](#)
- [Oracle Real-Time Collaboration Monitoring Interfaces](#)
- [Oracle Real-Time Collaboration Configuration Tests](#)

Oracle Real-Time Collaboration Configuration Utility

The `rtccctl` utility provides a command-line interface for administering and configuring the Oracle Real-Time Collaboration system. The utility lets administrators:

- Start, stop, or restart Oracle Real-Time Collaboration instances
- Configure system attributes, such as features available in conferences
- Monitor the system
- Run diagnostics on the system
- Troubleshoot system issues

See Chapter 4, "`rtccctl` Command-Line Utility for Oracle Real-Time Collaboration" of *Oracle Real-Time Collaboration Administrator's Guide* for details about how to use `rtccctl` commands.

Oracle Real-Time Collaboration Web Client for Administrators

Oracle Real-Time Collaboration Web Client lets administrators monitor system usage and manage business-related activities using four administrative tabs available from

the Oracle Real-Time Collaboration Web Client pages. These tabs are visible only to users with administrator privileges. The installing administrator can assign privileges to selected users by using the `rtcctl modifyRole` command and assigning one of the following roles:

Business Monitor: A business monitor can view and user the four default tabs available to all users (Home, Schedule, Materials, and Archive) as well as the following tabs:

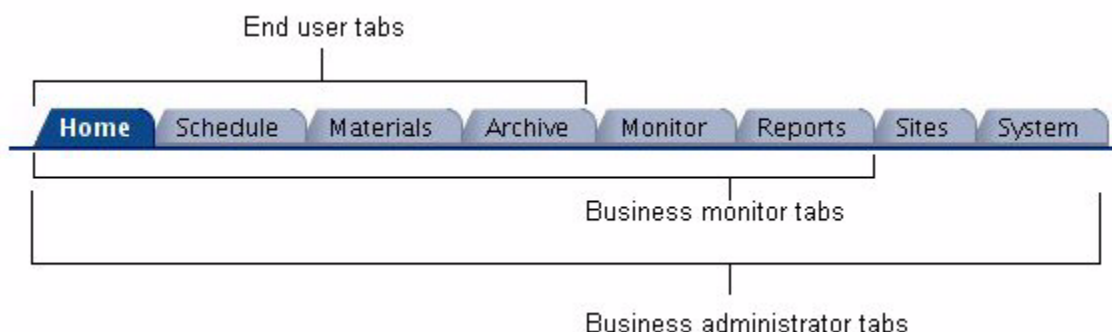
- *Monitor tab* lets administrators view currently running conferences, including conference details, diagnostics, and information about conference attendees. Administrators can even end server processes from this area.
- *Reports tab* displays information about each conference run on the system, details about web conferencing and messaging system usage, rollup of conference host feedback about the system, a security report showing what security features have been used in conferences, and quality of service reports that show key performance metrics and information about successes and failures of Oracle Real-Time Collaboration processes.

Business Administrator: A business administrator can see both of the tabs above, as well as the following tabs:

- *Sites tab* lets administrators customize a single Oracle Real-Time Collaboration deployment for several different lines of business. Each line of business can have its own appearance and its own customized integration with the Oracle Real-Time Collaboration system. Administrators must create sites in order to use the Oracle Real-Time Collaboration integration services.
- *System tab* lets administrators record and view information about each host for this Oracle Real-Time Collaboration system, and monitor the activity of instances and components running within the Real-Time Collaboration system.

Figure 5–1 shows all of the Oracle Real-Time Collaboration Web Client tabs available to end users, business monitors, and business administrators. See "Setting User Roles" in Chapter 4 of *Oracle Real-Time Collaboration Administrator's Guide* for details about how to assign user roles with `modifyRoles`.

Figure 5–1 Oracle Real-Time Collaboration Tabs and Administrator Levels



Oracle Real-Time Collaboration Monitoring Interfaces

The Oracle Real-Time Collaboration system includes **servlet interfaces** to let administrators monitor the availability of various Oracle Real-Time Collaboration services and components. Administrators can output this information into their own

administrative tools, if desired, and display the output in a custom availability report that they can appear from the **Reports** tab.

See "Oracle Real-Time Collaboration Monitoring Interfaces" in Chapter 5 of *Oracle Real-Time Collaboration Administrator's Guide* for details.

Oracle Real-Time Collaboration Configuration Tests

Administrators can run configuration tests to make sure that Oracle Real-Time Collaboration components are running and providing services. The tests include:

- Web conference service tests
- Voice conversion service tests
- Document conversion service tests
- Oracle Messenger router service tests

See "Monitoring Service Availability" in Chapter 5 of *Oracle Real-Time Collaboration Administrator's Guide* for details.

Oracle Voice Mail & Fax Administration Tools

You can use the following tools to manage Oracle Voicemail & Fax:

Enterprise Manager Grid Control

For Oracle Voicemail & Fax, Enterprise Manager Grid Control is the primary administrative tool. Enterprise Manager Grid Control gives you system-wide management capabilities, allowing you to manage all Oracle Voicemail & Fax groups in your Oracle environment. You can start and stop processes, view the status of the components within the Oracle Voicemail & Fax hierarchy, monitor the performance of the system, and configure the components.

See Chapter 6, "Managing Oracle Voicemail & Fax," in *Oracle Voicemail & Fax Administrator's Guide* for more information.

Oracle Collaboration Suite Control

Oracle Collaboration Suite Control allows you to start and stop the Oracle Voicemail & Fax application on a particular Applications tier. However, the functionality of the Oracle Collaboration Suite Control for Oracle Voicemail & Fax differs slightly from other Oracle Collaboration Suite components. You cannot use Oracle Collaboration Suite Control to manage the individual services on the Applications tier. You can only use it to start and stop the entire application.

See Chapter 6, "Managing Oracle Voicemail & Fax," in *Oracle Voicemail & Fax Administrator's Guide* for more information.

Oracle Voicemail & Fax Accounts Manager

Oracle Voicemail & Fax Accounts Manager is a command-line tool that allows you to create, delete, and manage voice mail accounts. You can also use the tool to create voice mail accounts in bulk.

See "Oracle Voicemail & Fax Accounts Manager Tool" in Chapter 5 of *Oracle Voicemail & Fax Administrator's Guide* for information about managing user accounts using the Voicemail & Fax Accounts Manager.

Interactive Voice Response Manager

The **Interactive Voice Response (IVR)** Manager is a command-line tool that allows you to create and manage simple, auto-attendant applications. An auto-attendant application guides callers through a series of menu options directing them to a specific person or department.

See "Interactive Voice Response Manager Commands" in Appendix E of *Oracle Voicemail & Fax Administrator's Guide* for more information on the Interactive Voice Response Manager commands.

Oracle Mobile Collaboration Administration Tools

The Oracle Mobile Collaboration administration pages, accessed from the *Mobile Collaboration* link in the *System Components* table of the Application Server Control *Home* page, include features that enable you to manage the client applications that provide client devices with Oracle Mobile Push Mail support and synchronization with Oracle Collaboration Suite 10g Calendar. In addition, the administration pages enable you to manage the voice support for the voice access to user directories by generating the Dual Tone Multi-Frequency (DTMF) equivalents and grammars of the user names stored in the Oracle Internet Directory (OID). The DTMF equivalents enable users to look up names using a keypad and the grammars enable users to find names through a speech-recognition engine.

Oracle Application Server Wireless System Management

Because the Oracle Mobile Collaboration Server depends upon the proper configuration of Oracle Application Server Wireless, the *Home* page of the Oracle Mobile Collaboration administration provides a link to the OracleAS Wireless System Manager. This tool enables you configure and manage the OracleAS Wireless Server. Using the System Manager, you can perform such tasks as:

- Starting and Stopping the OracleAS Wireless Server.
- Monitoring the health of the OracleAS Wireless Server through performance metrics.
- Configuring the Messaging Server, its drivers and its processes.
- Entering the entry points for the voice gateway and the access points for Async services, which enable users to access services through asynchronous technologies, such as SMS and e-mail.

Note: You can also access the OracleAS Wireless System Manager through the *Wireless* link in the *System Components* table. Clicking the administration icon enables you to access the OracleAS Wireless tools. For more information, see *Oracle Application Server Wireless Administrator's Guide*

Overview of Typical Administration Tasks for Oracle Collaboration Suite Components

This section describes the typical tasks that you or another administrator will perform, specific to each of the Oracle Collaboration Suite components. Each task includes a link to the detailed task instructions in the relevant component Administrator's Guide.

This section includes the following topics:

- [Oracle Calendar Administration Tasks](#)

- [Oracle Mail Administration Tasks](#)
- [Oracle Content Services Administration Tasks](#)
- [Oracle Real-Time Collaboration Administration Tasks](#)
- [Oracle Voicemail & Fax Administration Tasks](#)
- [Oracle Mobile Collaboration Administration Tasks](#)

Oracle Calendar Administration Tasks

Oracle Calendar server's typical administration tasks can be divided into two possible sections: monitoring and maintenance.

Monitoring

Use the following command-line utilities to monitor Oracle Calendar

- `unilogons`: Display Calendar server SIGNON/SIGNOFF statistics. For details on how to use the `unilogons` utility, refer to the *Oracle Calendar Reference Manual*.
- `unimem`: Display information on memory usage. For details on how to use the `unimem` utility, refer to the *Oracle Calendar Reference Manual*.
- `unireqdump`: View, and optionally delete, requests in the queue of the Corporate-Wide Services (CWS) daemon. For details on how to use the `unireqdump` utility, refer to the *Oracle Calendar Reference Manual*.

Maintenance

Use the following command-line utilities for Calendar server maintenance:

- `unidbbackup`: Create a backup of the calendar server. For details on how to use the `unidbbackup` utility, refer to the *Oracle Calendar Reference Manual*.
- `unidbfix`: Check, repair, defragment and maintain a calendar server node database. For details on how to use the `unidbfix` utility, refer to the *Oracle Calendar Reference Manual*.
- `unirmold`: Remove old events and tasks from agendas in a calendar server node database. For details on how to use the `unirmold` utility, refer to the *Oracle Calendar Reference Manual*.

Oracle Mail Administration Tasks

Typical administration tasks for Oracle Mail include:

- Managing Oracle Mail objects including domains, users, distribution lists, aliases, and news objects
- Managing Oracle Mail servers processes including SMTP, IMAP, POP, NNTP, Housekeeper, Virus Scrubber, and List Server
- Managing Oracle Mail security, including anti-spam and anti-virus protection
- Managing Oracle Mail policies including managing filters, routing control, and setting archive policies for messages
- Monitoring Oracle Mail performance using the Grid Control Console, and the `oesmon` and `oeschart` utilities

Oracle Content Services Administration Tasks

Oracle Content Services Administrator's Guide provides detailed information about a variety of Oracle Content Services administrative tasks. Specifically, system administrators can:

- Set up Oracle Content Services for various deployment scenarios, such as enabling the FTP or FTPS protocols, integrating Oracle Content Services with an antivirus solution, integrating with a retention hardware solution, setting up BFILE storage, or setting up the OmniPortlet. See Chapter 2, "Oracle Content Services Deployment Options" in *Oracle Content Services Administrator's Guide* for more information.
- Set up the Oracle Workflow notification mailer, as well as create and register custom BPEL workflows for use with Oracle Content Services. See Chapter 3, "Managing Workflows in Oracle Content Services" in *Oracle Content Services Administrator's Guide* for more information.
- Manage Oracle Content Services processes using the Oracle Collaboration Suite Control or OPMN. See Chapter 5, "Managing Oracle Content Services Processes" in *Oracle Content Services Administrator's Guide* for more information.
- Change configuration settings for Oracle Content Services domain properties, nodes, services, and servers using the Oracle Collaboration Suite Control. See Chapter 6, "Changing Oracle Content Services Configuration Settings" in *Oracle Content Services Administrator's Guide* for more information.
- Monitor Oracle Content Services domain, node, service, and server performance using the Oracle Collaboration Suite Control. See Chapter 7, "Monitoring Domain, Node, Service, and Server Performance" in *Oracle Content Services Administrator's Guide* for more information.
- Manage formats using the Oracle Collaboration Suite Control. See "Chapter 8, Managing Oracle Content Services Formats" in *Oracle Content Services Administrator's Guide* for more information.
- Manage Sites using the Oracle Collaboration Suite Control. See "Chapter 9, Managing Oracle Content Services Sites" in *Oracle Content Services Administrator's Guide* for more information.
- Optimize Oracle Content Services performance and scalability. See Chapter 10, "Maintenance and Tuning" in *Oracle Content Services Administrator's Guide* for more information.
- Configure or unconfigure Oracle Content Services Applications tiers. See Appendix B, "Configuring and Unconfiguring Oracle Content Services" in *Oracle Content Services Administrator's Guide* for more information.
- Manage and maintain the Oracle Text index. See Appendix C, "Oracle Text Reference" in *Oracle Content Services Administrator's Guide* for more information.

In addition, *Oracle Content Services Application Administrator's Guide* provides information about Oracle Content Services application administration tasks, such as allocating quota or restricting access to content.

Oracle Real-Time Collaboration Administration Tasks

Administrators will perform the following tasks for Oracle Real-Time Collaboration. All of these tasks are covered in the *Oracle Real-Time Collaboration Administrator's Guide*.

- Add or modify properties to customize the Oracle Real-Time Collaboration system, instances, and components, or to configure the behavior of the clients used

for web conferencing or messaging. See Chapter 3, "Configuring Oracle Real-Time Collaboration" and Chapter 4, "rtctl Command-Line Utility for Oracle Real-Time Collaboration" of *Oracle Real-Time Collaboration Administrator's Guide* for details

- Monitor system behavior and running processes. See Chapter 5, "Monitoring Oracle Real-Time Collaboration Processes" of *Oracle Real-Time Collaboration Administrator's Guide* for details.
- Evaluate system performance. See Chapter 6, "Historical and Statistical Reports for Oracle Real-Time Collaboration" of *Oracle Real-Time Collaboration Administrator's Guide* for details.
- Manage Oracle Real-Time Collaboration archives. See Chapter 7, "Managing Oracle Real-Time Collaboration Archives" of *Oracle Real-Time Collaboration Administrator's Guide* for details.
- Create custom sites for integrating applications. See Chapter 8, "Oracle Real-Time Collaboration Sites" of *Oracle Real-Time Collaboration Administrator's Guide* for details.

Oracle Voicemail & Fax Administration Tasks

The following are the administrative tasks that a system administrator will typically need to perform on an Oracle Voicemail & Fax system:

- Check the status of the services, making sure that all required services are up and running. See Chapter 6, Managing Oracle Voicemail & Fax, in the *Oracle Voicemail & Fax Administrator's Guide* for more information.
- Monitor the message recording metric (the length of time it takes to record a voice mail message) and the message retrieval metric (the length of time it takes to retrieve a voice mail message from the Oracle Collaboration Suite Database). See Chapter 10, Performance and Monitoring, in the *Oracle Voicemail & Fax Administrator's Guide* for more information.
- Add and delete voice mail accounts.
- Make changes to voice mail accounts, including changing the user's location, resetting passwords, and enabling and disabling features.

See Chapter 5, Managing Oracle Voice Mail & Fax Accounts, in *Oracle Voicemail & Fax Administrator's Guide* for more information.

- Monitor log files to resolve users' issues. See Appendix A, Troubleshooting, in *Oracle Voicemail & Fax Administrator's Guide* for more information.
- Add new sites, for example, when a new office is added or when migrating from a boarded deployment to a VoIP (Voice over IP) deployment. See Chapter 12, Scaling the Oracle Voicemail & Fax System in *Oracle Voicemail & Fax Administrator's Guide* for more information.

Oracle Mobile Collaboration Administration Tasks

The Oracle Mobile Collaboration *Administration* page, which you access by clicking the *Mobile Collaboration* check box in the *System Components* table of the Application Server Control *Home* page, enables you to manage the Oracle Mobile Push Mail clients and Oracle Mobile Data Sync clients as well as the voice support for the user directories.

Managing Mobile Push Mail Clients and Oracle Mobile Data Sync Clients

Management tasks related to the Oracle Mobile Push Mail clients and Oracle Mobile Data Sync clients include making these client applications available to user devices by adding them to the repository. You can also remove a client application from the repository. For security, you can remotely shut down and then delete client programs on user devices that have been lost, stolen, or have been used maliciously in the system.

Managing Voice Support

Voice support management includes generating the Dual Tone Multi-Frequency (DTMF) equivalents and the grammars of user names stored in the Oracle Internet Directory (OID).

In addition to these administrative tasks, you can also configure the logging level of the Oracle Mobile Push Mail Server as well as set the number of users for the Oracle Mobile Push Mail Server. You can also monitor the performance of mobile text access, mobile voice access, and mobile browser access. For more information, see Chapter 3, "Administering Mobile Collaboration" in *Oracle Mobile Collaboration Administrator's Guide*.

Managing Oracle Collaboration Suite Search

Oracle Collaboration Suite Search is a cross-application search tool. It uses the Oracle Ultra Search framework for conducting searches of Oracle Content Services, Oracle Mail, Oracle Calendar, and an Oracle Ultra SearchWeb crawler instance, combining the results into a single set. The searches of Oracle Content Services, Oracle Mail, and Oracle Calendar are managed through a set of 'searchlet' processes. The searchlets regularly update their respective indexes, allowing Oracle Collaboration Suite Search to produce combined results quickly. Users can perform searches which will check all of this indexed content to present a combined set of results. Users can also specify which source or sources they wish to search.

You can view performance data on Oracle Collaboration Suite Search from Oracle Collaboration Suite Control Console. You can administer Oracle Collaboration Suite Search by using the Oracle Ultra Search administration pages, available when you log in to the Oracle Ultra Search Web application with administration privileges. You can also configure the application searchlets individually.

To administer Oracle Collaboration Suite Search, connect to the Oracle Ultra Search administration tool:

```
http://<host>:<port>/ultrashow/admin/index.jsp
```

The <host> is the Applications tier hosting Oracle Collaboration Suite Search. The default <port> is 7777. Log in using an account with administrator privileges, such as orcladmin.

Oracle Calendar

By default, the Oracle Calendar searchlet indexes meeting title, location, task title, daily notes, and daily events.

The Oracle Calendar searchlet searches a user's agenda for meetings, daily notes and day events by searching the title, location or description. The Oracle Calendar searchlet does not index the information; it retrieves it from the Oracle Calendar Server and caches it for the Search UI to display it. The Oracle Calendar searchlet maintains a 2-minute cache by default.

You can configure the time which the Oracle Calendar searchlet maintains its cache by editing a file. To configure the time:

1. Open the file `ORACLE_HOME/j2ee/OC4J_OCSCClient/connectors/CalendarSearchlet/CalendarSearchlet/META-INF/oc4j-ra.xml` on the Applications tier hosting Oracle Calendar.

2. Add the exact syntax below:

```
<?xml version="1.0"?>
<!DOCTYPE oc4j-connector-factories PUBLIC "-//Oracle//DTD Oracle Connector
9.04//EN" "http://xmlns.oracle.com/ias/dtds/oc4j-connector-factories-9_04.dtd">
<oc4j-connector-factories>
  <connector-factory
location="eis/oracle/calendar/CalendarSearchlet" connector-name="Calendar
Search Adapter">
    <config-property name="webClientBaseURL" value=""/>
    <config-property name="webServiceURL" value=""/>
    <config-property name="verbose" value=""/>
    <config-property name="cacheTimeout" value=""/>
  </connector-factory>
</oc4j-connector-factories>
```

You do not need to enter a value for `webClientBaseURL` or `webServiceURL`. These values are specified in the Oracle Internet Directory Service Registry. However, if you do enter values for these properties, the values you enter will be used by the searchlet instead of those found in the Service Registry.

Set a new value for `cacheTimeout` to equal the desired cache timeout period, in minutes. The default period is two minutes. Enter any integer between 0 and 4,000,000,000. If you use a value of 0, caching is disabled.

You can specify a boolean value for `verbose` (True or False). By default `verbose` is false. If you set it to True, you will greatly increase the amount of information logged, which may impact the performance of the searchlet.

3. Save and close the file.

Oracle Mail

By default, the Oracle Mail searchlet indexes only the subject line of messages. You can enable body text indexing through Oracle Internet Directory Provisioning Console by setting a user's Text Indexing attribute.

You can modify the OJMA properties. In addition, you can modify the `baseurl` property by editing the `ra.xml` file for the Oracle Mail searchlet. This is the base URL for the client which will be used to display messages returned by the search.

See Also: For more information about editing Oracle Mail user attributes, see ["Modifying User Entries"](#) on page 4-12

Oracle Content Services

Oracle Collaboration Suite Search performs searches against the content of files stored in Oracle Content Services. You can change which formats are indexed, and you can manage those DBMS jobs that control the indexing.

Oracle Content Services administrators can designate whether certain formats (MIME types) should be indexed, like `.doc` or `.htm`. For instructions on designating searchable formats, see "Default Formats" in Chapter 8 of *Oracle Content Services Administrator's Guide*

There are two DBMS jobs that run automatically, Sync Job and Optimize Job, that control the Oracle Text indexing. Sync Job calls `ctx.ddl.sync_index`, which synchronizes the index by adding and deleting items that have changed since the last sync. Sync Job runs by default every 30 minutes. Optimize Job calls `ctx.ddl.optimize_index`, which optimizes the index to prevent it from becoming fragmented. Optimize Job runs by default every 24 hours, starting at midnight. You can also synchronize the index manually. For more information, refer to "Creating and Maintaining the Oracle Text Index" in Appendix C of *Oracle Content Services Administrator's Guide*.

The Oracle Content Services searchlet writes to the OPMN log for the Oracle Collaboration Suite Search OC4J instance.

Oracle Ultra Search

Oracle Ultra Search is a default component of Oracle Application Server which is included as part of Oracle Collaboration Suite.

You can view performance metrics for Oracle Ultra Search by selecting the icon in the Administration column for the Search component, from the Oracle Collaboration Suite Control Console Applications tier home page.

Note: Oracle Ultra Search configuration settings are applied in two ways: to the Oracle Ultra Search Web crawler instance, which you may use to index and search your Intranet Web-based resources, and to Oracle Collaboration Suite Search, which aggregates results from both the Oracle Ultra Search Web crawler index, and the Application-specific searchlet indexes. Any changes you make to the configuration settings apply to both types of search.

See Also: *Oracle Ultra Search Administrator's Guide* for more information about managing Oracle Ultra Search

Monitoring Oracle Collaboration Suite Search

You can monitor Oracle Collaboration Suite Search from its Oracle Collaboration Suite Control Console home page.

To monitor Oracle Collaboration Suite Search performance:

1. From the Oracle Collaboration Suite home page, click **Search** in the System Components list. The Collaboration Suite Search home page is displayed.
2. Select **All Metrics** from the Related Links list. The All Metrics page for Oracle Collaboration Suite Search is displayed.

From the All Metrics page, you can drill down to view any of 23 collected search performance metrics.

You can configure the Default Timeout and Maximum Results parameters.

Configuring Oracle Collaboration Suite Search

Oracle Ultra Search provides the Federator, which is used by the Oracle Collaboration Suite Search application to submit search requests to 'Web', 'Oracle Content Services', 'Oracle Mail', and 'Oracle Calendar' sources. The Federator is the technology framework, not a GUI; it is not exposed to end users or administrators.

Oracle Ultra Search itself supports the Web search (Oracle Content Services, Oracle Mail, and Oracle Calendar searches are performed by the searchlets described previously in this chapter). When you submit a search request to a Web source from the Oracle Collaboration Suite Search application, it will send the request to the Oracle Ultra Search repository through the Federator.

To configure Oracle Collaboration Suite Search, you use the Oracle Ultra Search Web application.

To log in to the Oracle Ultra Search interface:

1. From the Oracle Collaboration Suite home page of the Applications tier on which Oracle Collaboration Suite Search is hosted, find **Search** in the System Components table. Select the icon in the Administration column. The Single Sign-On page is displayed.
2. Log in using an account with Administrator privileges, such as the `orcladmin` account. The Oracle Ultra Search administration console is displayed.
3. There is a single Oracle Ultra Search default instance `wk_inst`, which hosts Oracle Collaboration Suite Search. Select the instance in the drop-down box, and click **Apply**. You can now make configuration changes using the Oracle Ultra Search menu bar.

Alternatively, you can connect directly to the Oracle Ultra Search administration tool:

`http://<host>:<port>/ultrasearch/admin/index.jsp`

The `<host>` is the Applications tier hosting Oracle Collaboration Suite Search. The default `<port>` is 7777. Log in using an account with administrator privileges, such as `orcladmin`.

Some common tasks that you might wish to perform:

- From the **Queries** tab, select the **Configuration** sub-tab to manage configuration parameters for the Federation engine. You can manage the following parameters:
 - **Timeout Threshold:** The maximum wait time for getting search results from each of the repositories. The unit is in milliseconds.
 - **Maximum Number of Hits:** The larger the number, the slower the search results.
 - **Parallel Query:** Parallel query mode will make the search more efficient, but it also will consume more memory.
 - **Minimum / Maximum Thread Pool Size:** Use a larger number if there are more users running the search application concurrently. A larger pool consumes more resources.
- From the **Queries** tab, select the **Query Statistics** sub-tab to set up query statistics gathering. If you enable this option, you can monitor the queries that your users are performing.
- Select the **Web Access** tab to manage proxy settings for the Web search
- Select the **Schedules** tab to manage how often various data synchronization processes are performed
- From the **Schedules** tab, select the **Index Optimization** sub-tab to manage the index optimization schedule and to set a maximum limit for how long this process may run

- From the **Globalization** tab, select the **Federator Attribute Name** sub-tab to change the translation language used for the federator.
- From the **Users** tab, select the **Privileges** or **Super-Users** sub-tabs to grant administrator privileges or super-user privileges to other users. You can grant privileges to any Oracle Collaboration Suite Single Sign-On user.

See Also: *Oracle Ultra Search Administrator's Guide* for complete information on managing and configuring Oracle Ultra Search

Managing Oracle Contacts

Oracle Collaboration Suite 10g Contacts is a feature of Oracle Collaboration Suite which users can access using Oracle Web Access Client, Oracle WebMail, Oracle Calendar, and Oracle Connector for Outlook. It contains the personal contacts for each user. Oracle Contacts is a schema in the Oracle Internet Directory which is used for storing the personal contacts of all Oracle Collaboration Suite users in the Oracle Collaboration Suite Database.

There are two features of Oracle Contacts which you can manage. This section describes the following tasks:

- [Managing Oracle Contacts Default Categories](#)
- [Managing Oracle Contacts Maximum Entries](#)

Managing Oracle Contacts Default Categories

Users of Oracle Web Access Client and Oracle Connector for Outlook can assign Oracle Contacts entries to various categories. By default, Oracle Collaboration Suite provides a list of default categories to which users can assign their contacts. The default categories behave differently depending on the client used:

- Microsoft Outlook contains its own list of categories, and users can create additional categories of any name. Categories which have the exact same name as a default category stored in Oracle Contacts will map to those categories. For example, if a default category 'Customers' exists in both Oracle Contacts and in a user's Microsoft Outlook Contacts lists, that user will see contacts categorized as Customers in the Customers category when they use Oracle Web Access Client to view their Oracle Contacts.
- Oracle Web Access Client lists only the default categories stored in Oracle Contacts. Users may not create new categories other than the default categories. If a user assigns contacts to a category in Oracle Web Access Client that does not exist in their categories list in Microsoft Outlook, then that contact will appear as uncategorized when they use Microsoft Outlook to view their Oracle Contacts.

You can add, edit, and delete the default categories for all users, by using the Oracle Directory Manager to edit the Oracle Internet Directory.

To add, edit, or delete default categories:

1. Start the Oracle Directory Manager:

Unix:

```
ORACLE_HOME/bin/oidadmin
```

Windows:

```
Start > Programs > Oracle Application Server > OracleHome >  
Integrated Management Tools > Oracle Directory Manager
```

2. When you start Oracle Directory Manager, it will prompt you for connection information. Enter the following information to connect to your Oracle Internet Directory, typically hosted in the Oracle Collaboration Suite Database on your Oracle Collaboration Suite Infrastructure:

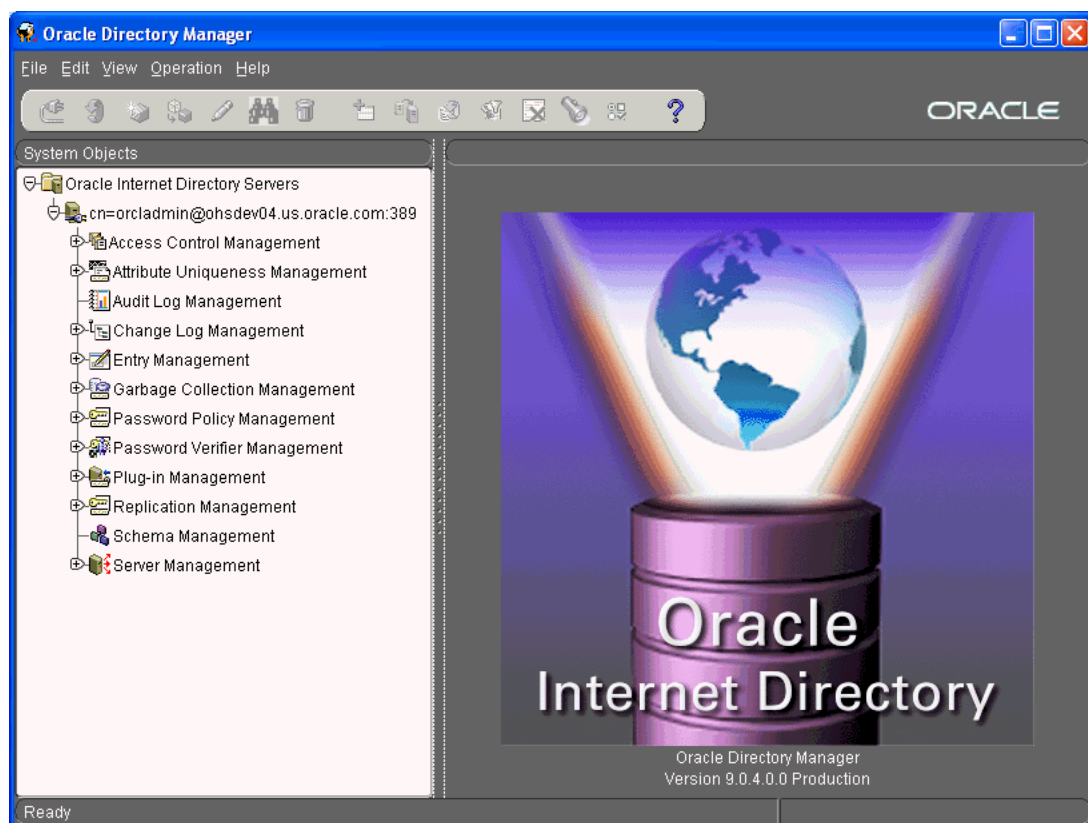
Host: <infrahost.yourdomain.com>
 Port: 389
 Username: cn=orcladmin
 Password: <password>

Port 389 is the default port used by Oracle Internet Directory. You may be using a different port. If so, enter the correct Oracle Internet Directory port.

If you have configured your Oracle Internet Directory to be accessed using Secure Socket Layers (SSL), select the **SSL Enabled** checkbox. Otherwise, leave it blank.

3. Select **Login** to log in to the Oracle Internet Directory. When the connection is successful, the Oracle Internet Directory management screen is displayed. See [Figure 5-2, "Accessing Oracle Internet Directory with Oracle Directory Manager"](#) on page 5-16.

Figure 5-2 Accessing Oracle Internet Directory with Oracle Directory Manager



4. Navigate to the global preferences object of the Common Address Book:
 - a. Select Entry Management
 - b. Select the top level, second level, and additional levels of your domain, in that order. For example, if your domain is `company.us.mydomain.com`, select:


```
dc=com
dc=mydomain
dc=us
dc=company
```

- c. Select cn=OracleContext
- d. Select cn=Products
- e. Select cn=CommonAddressBook
- f. Select cn=Preferences
- g. Select cn=Global
5. Add, edit, or delete the default category entries in the orcladdressbookcategory parameter field
6. When you have finished making changes, select **Apply**. If you wish to revert to the existing values without making changes, select **Revert**.
7. Log in to Oracle Collaboration Suite Control for each Applications tier which hosts Oracle Web Access Client, and restart the OC4J_OCSCClient system component.

Alternatively, you may restart the OC4J_OCSCClient component from the command line:

```
[ORACLE_HOME]/opmn/bin/opmnctl restartproc ias-component=OC4J_OCSCClient
```

Once the process restarts, your changes will take effect.

Note: If you change or delete a default category, users which have already assigned contacts to that category will continue to see the original category name available for use in their address books. If they later remove all of their contacts from that original category, it will disappear from their list of available categories.

Users which have no contacts assigned to the old category will no longer see the old category in their list of available categories.

Managing Oracle Contacts Maximum Entries

By default, Oracle Collaboration Suite sets a maximum number of 2000 Oracle Contacts entries per user. You can change this default value by using the Oracle Directory Manager to edit the Oracle Internet Directory.

To change the maximum address book entries parameter:

1. Start the Oracle Directory Manager:

Unix:

```
ORACLE_HOME/bin/oidadmin
```

Windows:

```
Start > Programs > Oracle Application Server > OracleHome >
Integrated Management Tools > Oracle Directory Manager
```

2. When you start Oracle Directory Manager, it will prompt you for connection information. Enter the following information to connect to your Oracle Internet Directory, typically hosted in the Oracle Collaboration Suite Database on your Oracle Collaboration Suite Infrastructure:

Host: <infrahost.yourdomain.com>
Port: 389
Username: cn=orcladmin
Password: <password>

Port 389 is the default port used by Oracle Internet Directory. You may be using a different port. If so, enter the correct Oracle Internet Directory port.

If you have configured your Oracle Internet Directory to be accessed using Secure Socket Layers (SSL), select the **SSL Enabled** checkbox. Otherwise, leave it blank.

3. Select **Login** to log in to the Oracle Internet Directory. When the connection is successful, the Oracle Internet Directory management screen is displayed. See [Figure 5-2, "Accessing Oracle Internet Directory with Oracle Directory Manager"](#) on page 5-16.
4. Navigate to the global preferences object of the Common Address Book:
 - a. Select Entry Management
 - b. Select the top level, second level, and additional levels of your domain, in that order. For example, if your domain is `company.us.mydomain.com`, select:

```
dc=com
dc=mydomain
dc=us
dc=company
```
 - c. Select `cn=OracleContext`
 - d. Select `cn=Products`
 - e. Select `cn=CommonAddressBook`
 - f. Select `cn=Preferences`
 - g. Select `cn=Global`
5. Edit the `orcladdressbookmaxentries` field to the new maximum entries value
6. When you have finished making changes, select **Apply**. If you wish to revert to the existing values without making changes, select **Revert**.
7. Log in to Oracle Collaboration Suite Control for each Applications tier which hosts Oracle Web Access Client, and restart the `OC4J_OCSCClient` system component.

Alternatively, you may restart the `OC4J_OCSCClient` component from the command line:

```
[ORACLE_HOME]/opmn/bin/opmnctl restartproc ias-component=OC4J_OCSCClient
```

One the process restarts, your changes will take affect.

Note: If you lower the value of the maximum entries parameter and any users already have more than the new number of Oracle Contacts entries allowed, those users will keep all existing entries, but will be unable to create any new entries (unless they delete existing entries to bring their total number of entries down below the new maximum).

Managing Oracle Discussions

Oracle Discussions users can access and interact with discussion forums using various paths: the Oracle Discussions Web user interface, RSS clients, Oracle Mail IMAP

clients, and Oracle Web Access Client. Oracle Discussions provides RSS feeds to access and browse its forums and discussions. When accessing Oracle Discussions through e-mail clients such as Oracle Web Access Client, discussion forums will be visible as Shared Folders.

This section includes the following topics:

- [Introduction to Oracle Discussions](#)
- [Oracle Discussions Access Control](#)
- [Oracle Discussions Administration Tasks](#)
- [Oracle Discussions Forum E-mail Integration](#)
- [Accessing Oracle Discussions with RSS](#)
- [Accessing Oracle Discussions using E-mail](#)
- [Oracle Discussions Message Indexing for Search](#)

Introduction to Oracle Discussions

Oracle Discussions is organized in message forums. Each forum is dedicated to the discussion of a given theme. Forums are grouped under categories; categories can be nested, containing other categories. When a message is posted to a forum, a new message topic is started. Topics are defined as a set of messages stemming out of the same root message. The subject of the root message of a topic defines the name of the topic. The messages of a topic are organized in a tree structure where every reply becomes a child of the message it replies to.

Oracle Discussions Integration with Oracle Mail

Oracle Discussions leverages Oracle Mail for messages storage. Oracle Discussions stores its messages in the Oracle Collaboration Suite Database using the Oracle Mail message store schema. The `ES_MAIL` schema has been enhanced, adding a few Oracle Discussions-specific tables. Oracle Discussions Java SDK relies on Oracle Java Mail APIs to establish and manage connections to both the database and Oracle Internet Directory.

By storing Oracle Discussions messages in the Oracle Mail store, e-mail clients accessing the Oracle Mail IMAP Server have access to the Oracle Discussions forums as shared folders. End users can then read forum messages in an e-mail client application and, through the Oracle Discussions e-mail participation feature, post new topics and replies.

Oracle Discussions uses Oracle Mail Shared Folders for its message storage. An Oracle Discussions category is mapped to a Shared Folder holding other folders. An Oracle Discussions forum is mapped to a Shared Folder holding all the messages posted to that forum. When creating a new category or forum, Oracle Discussions interacts with Oracle Mail to create the corresponding Shared Folder.

At Oracle Discussions installation time, administrators select one Oracle Mail store to be enabled for Oracle Discussions storage. Consequently, a new internal Oracle Mail user will be created and associated with that storage. This internal Discussions user for a mail store whose database SID is `<dbsid>` will be named `discussions_<dbsid>`. This user will be used internally by Oracle Discussions APIs to create and manage all the Shared Folders used by Oracle Discussions in that Oracle Mail store. The corresponding Oracle Internet Directory user has a randomized password, and it is Single Sign-On disabled.

At Oracle Discussions installation time, administrators also select an Oracle Mail domain to be associated to the Oracle Discussions Applications tier. During installation, the `discussions_<dbsid>` user will be provisioned for the selected Oracle Mail domain, thus associating the Applications tier with that Oracle Mail domain. The `discussions_<dbsid>` user is also provisioned as an Oracle Mail System Administrator role, with unlimited quota, and enabled for Oracle Text Indexing of messages.

Multiple Oracle Mail Storage Support Oracle Mail allows for a deployment scenario where e-mail data is stored in different Oracle Mail stores and each Oracle Mail store is associated with a database instance. Oracle Mail stores are partitioned according to users so that all mail messages of one user will be stored in the same Oracle Mail store. The same rule applies to Shared Folders where the e-mails of a Shared Folder will be stored in the same Oracle Mail store of the Shared Folder creator.

Oracle Discussions leverages the deployment scenario of multiple Oracle Mail stores by allowing administrators to select the mail store to be used for Discussions during installation.

Applications Tier Association Each Oracle Discussions Applications tier is associated to an internal Oracle Discussions admin account. Therefore each Oracle Discussions Applications tier is associated with a Oracle Mail store and an e-mail domain. The association between the Oracle Discussions Applications tier and the corresponding admin account is stored in the Oracle Internet Directory Service Registry. The association with an e-mail domain is particularly important as Oracle Mail Shared Folders can only be shared among users provisioned for the same e-mail domain. This means that users connecting to an Oracle Discussions instance must be provisioned for the same e-mail domain associated with that Oracle Discussions instance. Upon user login, Oracle Discussions will check if the user has been provisioned for the e-mail domain associated with this Applications tier.

See Also: For more information about the Oracle Internet Directory 10g Service Registry, see ["Managing the Oracle Internet Directory Service Registry"](#) on page 7-7

Multiple E-mail Domains You can create two Oracle Discussions instances, each of which is associated with a different e-mail domain. When you provision users, you can provision them for both domains, providing them with access to both Oracle Discussions instances. Or, you can provision users for one domain only, limiting them to one or the other Oracle Discussions instance only.

Note: You cannot associate an Oracle Mail store database to more than one Oracle Discussions instance.

Oracle Discussions Access Control

The Oracle Discussions [access control](#) model is based on roles. On a given category or forum, roles can be granted or revoked to Oracle Collaboration Suite users. For a given Discussions instance, grantees must have been provisioned for the same Email domain associated to this instance. The following access control roles defined:

- **Global Administrator** can be granted to Oracle Collaboration Suite users and grants system level administration for the whole Oracle Discussions system
Users granted a Global Administrator role represent the super users of the system. They are granted the permission of executing all tasks on all objects in the system.

Note: Users provisioned for Oracle Mail with the Domain Administrator role will automatically be granted the Oracle Discussions Global Administrator role when they log in to Oracle Discussions.

- **Category Administrator** is the role granted to those users who may administer a given category. Category Administrators have permission to administer only the categories and forums within the assigned category. Category Administrators can post Announcements for the category they administer.
- **Category Creator** can be granted to Oracle Collaboration Suite users. These users can create new categories and forums within the category for which they are granted this role. Category creators are automatically granted category administrator and forum moderator roles for the categories and forums they create.
- **Category Writer** can be granted to Oracle Collaboration Suite users. These users automatically have forum writer privileges for all the forums within the category for which they are granted this role.
- **Forum Creator** roles can be granted to Oracle Collaboration Suite users on a given category. Forum creators on a given category have the privilege of creating forums within that category
- **Forum Moderator** role can be granted to Oracle Collaboration Suite users on a given forum. Users granted this role on a given forum have the authority of managing the content within that forum. Forum moderators can post Announcements for the forum they moderate.
- **Forum Writer** maps to a participant in the Oracle Discussions system. Forum Writers can post new topics or reply to existing ones. They may be able to edit messages that they posted (depending on forum policies), but never messages posted by other users. The forum writer role can be granted to Oracle Collaboration Suite users on a given forum.
- **Forum Reader** can be granted to Oracle Collaboration Suite users on a given forum. Forum readers will only have read access to forums on which they have been granted the role. Forum readers do not have permission to post new messages or reply to existing topics.

Oracle Discussions role resolution is hierarchical, so that a user granted Category Administrator on a given category would also be Category Administrator for all the sub-categories under it. Similarly, Category Administrator on a given category would be Forum Moderator for all the forums under such category or any of its sub-categories. For a given object, the access control granted to a given user would be the most powerful of all the roles granted to him on that object or any of its parents.

For example, consider a forum named 'f1' within a category named 'c1'; assume that a user is granted Category Administrator role for category c1 and Forum Writer for forum f1. The user will actually have Forum Moderator role in for forum f1, because his Category Administrator role grants maximum privileges to all categories, forums, topics, and messages within his assigned categories.

In Oracle Discussions 10g Release 1 (10.1.1), the grantee for a category or forum role can only be a user. There is no support for Oracle Internet Directory 10g groups as grantees for role assignments in this release.

[Table 5–1, "Oracle Discussions Role Permissions"](#) on page 5-22 shows the set of actions each role grants a user to perform on a category or forum.

Table 5–1 Oracle Discussions Role Permissions

Action	Global Admin	Category Admin	Category Creator	Category Writer	Forum Creator	Forum Moderator	Forum Writer	Forum Reader
Create Categories	Yes	Yes	Yes	No	No	No	No	No
Edit Category Settings	Yes	Yes	Yes ¹	No	No	No	No	No
Delete Categories	Yes	Yes	Yes ¹	No	No	No	No	No
View Categories and its Forums	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create Forum	Yes	Yes	Yes	No	Yes	No	No	No
Edit Forum Settings	Yes	Yes	Yes ¹	No	Yes ¹	Yes	No	No
Delete Forums	Yes	Yes	Yes ¹	No	Yes ¹	No	No	No
View Forum	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Post Announcement	Yes	Yes	Yes ¹	No	Yes ¹	Yes	No	No
Post Topic	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Post Reply	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Edit Message	Yes	Yes	Yes	Yes	Yes	Yes	Yes ²	No
Hide Message	Yes	Yes	Yes	No	Yes	Yes	Yes ²	No
Delete Message	Yes	Yes	Yes	No	Yes	Yes	No	No
Move Topics	Yes ³	Yes ³	Yes	No	Yes ³	Yes ³	No	No
Mark as Favorite	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Subscribe	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Search	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

¹ Only for categories/forums they created

² Follows forum policies, defined as a property of each forum

³ Must have ForumWriter permissions in the destination forum

When a user first logs in or first accesses a category or forum, the user's role is cached in the Applications tier for performance reasons. The user's role will be cached while the user is performing read-like operations, and is refreshed before allowing the user to perform any kind of write operation.

For example, if John is granted the Forum Writer role for a forum, the first time he accesses the forum, his Forum Writer role will be cached. While John reads topics and messages of the forum, his role is cached and will show up as forum writer.

If a forum moderator downgrades John to Forum Reader, this will not have an immediate impact on John's active session and his role will still be shown as Forum Writer. However, when John tries to post a message, before executing this operation his role will be refreshed, Oracle Discussions will discover that his role is now Forum Reader, and therefore an error will be reported.

Similarly, when a user logs into Oracle Discussions, the full list of categories and forums he has access to will be fetched and cached in the Applications tier. If, during the lifetime of the user's session, the user is granted access to a new category or forum, the category or forum will not be automatically visible to the user. To access the newly granted category or forum, the user must log out and log back in, allow his session to expire (and then log back in), or force a full refresh of the category or forum list by clicking on the **Last Refresh** link on the top right corner of a category browsing page.

Managing Oracle Discussions roles

When you first install Oracle Discussions, no user is provisioned the Global Administrator role. Using the Provisioning Console, create a new user or provision an existing user as an Oracle Mail Domain Administrator for the e-mail domain used by this Oracle Discussions instance.

See Also: [Chapter 4, "Managing Oracle Collaboration Suite Users and Groups"](#) for instructions on creating and provisioning users.

You can then login into Oracle Discussions using the new administrator account. You will be able to start creating new categories and forums and grant access to other users.

For instructions on assigning roles for categories and forums, see the Oracle Discussions Web Client online help.

Oracle Discussions Administration Tasks

There are a variety of administrative tasks that will be performed in the course of maintaining Oracle Discussions.

The following tasks are described in this section:

- [Oracle Discussions Global Administration](#)
- [Oracle Discussions Category Administration](#)
- [Oracle Discussions Forum Settings](#)
- [Oracle Discussions Web User Interface Defaults](#)
- [Locking Oracle Discussions Message Forums and Topics](#)
- [Moving Oracle Discussions Topics Across Forums](#)
- [Clipping Oracle Discussions Topics](#)
- [Oracle Discussions Announcements](#)

Oracle Discussions Global Administration

Global administrators can execute all tasks on all items in the Oracle Discussions system, including adding and removing other global administrators. Only global

administrators can create root categories in the Oracle Discussions system and post system-level announcements.

Category creators can create new categories and forums within the category for which they are granted this role. Category creators are automatically granted category administrator and forum moderator rights for the categories and forums they create.

1. Select the **Administration** tab from the top of any Oracle Discussions page.
2. Select the **Global Membership** link. A list of the current global administrators is displayed.
3. Click **Change Membership**.
4. Select the **Enable Global Category Creator** check box if you want to allow logged in users to create categories and forums at the root category level.
5. Use the **Add Global Membership** section of the page to add global administrators and category creators:
 - To add a user, enter the user's name in the **User ID** field or search for the user by clicking the **Flashlight** icon. Select a role from the **as** drop-down list and click **Add**.
 - To add a group of users, enter the group name **Users in Group ID** field or search for the group name by clicking the **Flashlight** icon. Select a role from the **as** drop-down list and click **Add**. All the users in the group are granted the same role.
6. Use the **Global Membership** section of the page to change membership or remove members:
 - To change a member's role, select the member from the **Global Membership** column and select the new role from the **Role** drop-down list.
 - To remove a member, select the member and click **Remove**.
7. When you are finished making global membership changes, click **Done**.

Oracle Discussions Category Administration

A category is a container used to group related categories and forums. A category cannot contain messages or attachments. Categories can be used to group discussions based on any hierarchical criteria. For example, in an on-line forum for Oracle products, a category could be defined to contain all forums related to [Java Database Connectivity \(JDBC\)](#) drivers.

Global administrators may create root categories. Category administrators and creators can only create new categories within the categories they administer. During category creation, an administrator can configure the category properties and settings described below, including granting other users access to the category.

Once a category is created, category administrators can edit its properties and settings, including changing the category description. A category administrator is also able to control access to the category by determining which users are granted what roles.

A category administrator may delete a category that he administers. Deleting a category recursively deletes all the contained categories, forums, and messages.

A category has the following properties and settings:

- **Name:** The name of the category as chosen by its creator. In each level of the category hierarchy, category names need to be unique so that there are no two sibling categories with the same name. Upon creation, category names will be

converted to a format where the first letter will be upper case and the following letters will be lower case. Category names are not editable once a category is created. When accessing Oracle Discussions through IMAP, the category name will be used.

- **Display Name:** The display name of the category as chosen by its creator. The display name is used in the Oracle Discussions Web UI and in the RSS feeds. In each level of the category hierarchy, category display names need to be unique so that there are no two sibling categories with the same name. Category display names can be changed after the category is created.
- **Description:** A short description suggesting the theme of the sub-categories and forums that this category contains. Category descriptions are always editable in the lifetime of a category.
- **Access Control List:** the list of users and corresponding roles that have access to this category. See "[Oracle Discussions Access Control](#)" on page 5-20 for details.

Oracle Discussions Forum Settings

Forums resemble physical bulletin forums in the real world. Forums differ from categories in that they contain topics and messages. Forums are generally organized by theme, as all the messages posted to a forum are related to a given subject. Users may post messages into a forum and expect responses, or may just browse existing messages and their replies. In the Internet community, forums are often referred to as forums or on-line forums; other forum products use similar definitions.

When creating a forum, you can specify the following properties and settings:

- **Name:** The name of the forum as chosen by its creator. In each level of the category hierarchy, forum names need to be unique so that there are no two siblings forums with the same name. Upon creation, forum names are converted to a format where the first letter is upper case and the following letters are lower case. Forum names are not editable once a forum is created. When accessing Oracle Discussions through IMAP, the forum names are used.
- **Display Name:** The display name of the forum as chosen by its creator. The display name is used in the Oracle Discussions Web UI and in the RSS feeds. In each level of the category hierarchy, forum display names need to be unique so that there are no two sibling forums with the same name. Forum display names can be changed after the forum is created.
- **Description:** A short description suggesting the theme of messages posted in this forum. Forum descriptions are always editable in the lifetime of a forum.
- **Forum Configuration:** Forum Configuration allows you to set policies used to customize the forum behavior. The following policies can be configured:
 - **Message Attachments:** Controls whether or not users can add attachments to messages they post. If you enable message attachments, you can also set the maximum allowed attachment size.
 - **Message Reply Policy:**
 - * **Reply's subject prefix:** Controls how you want the subject line of message replies to appear.
 - * **Quote original message:** Controls whether you want the original message included in replies, and if so, how the original message is formatted using the following tokens:
 - \$ {msg-sent-date}: Include the date of the quoted message.

`${msg-author}`: Include the name, if available, of the author of the quoted message.

`${msg-from}`: Include the e-mail address of the author of quoted message.

`${msg-subject}`: Include the subject of the quoted message

Forum Access Control ForumModerators have full control of forums in which they have been granted the moderator role. This includes editing and changing all properties and settings for the forum and managing the whole content of the forum. Forums moderators can take different actions to manage the forum content. For example they can:

- Edit or hide inappropriate posts
- Delete old or inappropriate topics and/or messages from the system
- Move topics from one forum to a different more related one
- Clip topics that grow too long or off-topic into separate topic
- Lock a topic or even a full forum

Forum Moderators can also post Announcement messages for the forum they moderate.

Forum writers can post new topics into a forum and reply to existing topics and messages. Forum writers may be able to post and reply via e-mail, depending on the forum e-mail policies. Forum writers may be able to edit and/or delete messages depending on the forum policies.

ForumReaders can browse a forum and its topics. They can see posted messages, search across the forums they have access to and mark categories, forums and topics as favorites. In forums marked as Public, the access control settings are relaxed allowing guest users to act as Forum Readers without having been explicitly granted the role and allowing valid Oracle Internet Directory 10g users logged-in to act as Forum Writers without the explicit role being granted. The same access control rules apply for participation in the Forum through e-mail.

Message Editing and Hiding Policies Once a message is posted in the forum, the message author may or may not be allowed to edit his post, depending on the message editing policies. Any message modified after the original post will be explicitly marked as "edit after the original post" and a message annotation will be used to keep track of the message edit history. Administrators can specify whether forum writers can edit or hide messages.

The default message edit policy will be specified in the global settings. Forum moderators may choose one of the three message editing policies shown in [Table 5–2, "Forum Message Editing and Hiding Policies"](#) for each of the forums they administer to override the default message edit policy.

Table 5–2 Forum Message Editing and Hiding Policies

Policy	Description
Never allow message editing or hiding	Forum writers cannot hide or edit their messages.
Allow editing and hiding only for messages with no replies	Forum writers can only hide or edit their messages if no replies have been received yet.

Table 5–2 (Cont.) Forum Message Editing and Hiding Policies

Policy	Description
Always allow message editing and hiding	Forum writers can hide or edit their messages at any time.

When a message is hidden, forum moderators will be able to see the body of the hidden message as a strike-through, while forum writers and forum readers will instead see a "Message Deleted" message.

Oracle Discussions Web User Interface Defaults

Administrators can configure the defaults settings for the Web UI message editor and the topic view. The following settings are available:

- **Flat View:** Displays all messages within a topic on one page, sorted by date and time. Use this setting if most of your topics contain many short replies. Enter the maximum number of replies allowed per page in the Number of replies per page box
- **Threaded View:** Displays each message in a topic one at a time along with the full thread structure. Use this setting if most of your topics contain a few long replies.
- **Plain Text Editor:** Use this option if you want a plain text editor used by default for posts and replies.
- **Rich Text Editor:** Use this option if you want a rich text editor used by default for posts and replies. This enables users to format the text of the messages.

Locking Oracle Discussions Message Forums and Topics

Locking a message forum or a topic prevents any new messages from being created within that forum or topic. Once a forum or topic is locked, nobody other than moderators can add or change content. This prevents forum writers from posting new topics or replies, or editing or hiding messages. Often a topic is locked because it contains informative posts, which many people will read, and replies by individuals are deemed inappropriate. Sometimes a forum or topic is locked because a new topic or different forum has been created for the same topic, and the older information is considered to be deprecated.

When you lock a forum, the forum will not be shown as locked for users currently connected to the system until they try to post a new message. Similarly, when unlocking a forum, the forum will not be shown as unlocked for other users currently connected to the system until they log out and log back in or their J2EE session expires.

To learn how to lock and unlock message forums and topics, see the Oracle Discussions online help.

Moving Oracle Discussions Topics Across Forums

It is possible to move a topic of messages from one forum to another forum. Commonly this is done because the topic is deemed to contain content that is more appropriate for the topic designated for a different forum. For the operation to be allowed, the connected user must be granted (at least) Forum Moderator role in the source forum and (at least) Forum Writer role in the destination forum.

To learn how to move a topic from one forum to another forum, see the Oracle Discussions online help.

Clipping Oracle Discussions Topics

It is possible to clip a topic, moving one of the topic messages and all its replies into a new topic. Commonly this is done because the topic grew too long, or its replies went off-topic and are therefore more appropriate into a brand new topic.

To learn how to clip a topic from one forum to another forum, see the Oracle Discussions online help.

Oracle Discussions Announcements

Categories and forums have announcements associated with them. Announcements have high visibility in a category or forum page, which makes them useful for highlighting certain topics. For example, you might have an announcement in which the rules for discussion of the forum topic are explained. By posting this announcement, everyone who visits the forum in the future will see this important topic right away. Another common use is to highlight a topic in which frequently asked questions (FAQs) are answered, to prevent new users from asking the same questions.

To learn how to post Announcements, see the Oracle Discussions online help.

Oracle Discussions Forum E-mail Integration

This section contains the following topics:

- [Posting Messages to a Forum Using E-mail](#)
- [Forwarding Messages Posted Using the Oracle Discussions Web UI to E-Mail](#)
- [Forums and Distribution Lists Integration](#)

Posting Messages to a Forum Using E-mail

A forum can be assigned an e-mail address. E-mail messages sent to that e-mail address will be stored in the forum and threaded accordingly. If the sent message does not have any parent message, it will be stored as a new topic; otherwise, it will be correctly stored as a reply of the parent topic. Threading of replies is ensured. Forum e-mail policies will dictate whose e-mails will be stored in the forum, based on the e-mail author.

When enabling a forum for e-mail, the forum e-mail address will be registered as an e-mail alias for the internal account `discussions_<dbid>@<emaildomain>` associated to that Oracle Discussions instance. All e-mails sent to a forum will be initially received in the `discussions_<dbid>@<emaildomain>` INBOX. An E-Mail server-side rule defined for the `discussions_<dbid>@<emaildomain>` will notify the Oracle Discussions Applications tier upon new posts. The notification is achieved through Oracle JMS using a queue in the database and a Message Driven Bean (MDB) deployed as part of the Discussions J2EE application.

Forwarding Messages Posted Using the Oracle Discussions Web UI to E-Mail

There are two ways by which messages posted through the Oracle Discussions Web UI can be forwarded to an e-mail address:

- Users can subscribe to a category, forum, or topic and receive an e-mail notification when new messages are posted. The e-mail notification reply to address will be the forum e-mail address, so that further replies will be posted to the forum. If no forum e-mail address is defined, the message author's e-mail address is used.

- Moderators can set up an e-mail forwarding policy so that all messages posted through the Oracle Discussions Web UI are forwarded to a given e-mail address. The format of the forwarded message is customizable as part of the forum e-mail settings. The reply-to address for forwarded e-mails will be the forwarding e-mail address itself, allowing Distribution List integration.

The following settings can be used to customize the forum e-mail integration:

- **Incoming e-mail policy:**
 - **Ignore all:** Incoming e-mails to the forum are not posted.
 - **Restricted:** Incoming e-mails to the forum are posted only if the sender is a forum writer.
 - **Open:** All incoming e-mails to the forum are posted.
- **E-mail forwarding policy:**
 - **Do not forward any messages:** Select this option if you do not want messages posted to the forum to be forwarded to another e-mail address.
 - **Forward all messages to the following email address:** Select this option if you want messages posted to the forum to be forwarded to a distribution list, and enter the distribution list address in the space provided. Select how you want the message forwarded: **As Original Message** or **As Subscription Notification**. When forwarding a message, the reply-to address of the forward will be the forwarding address itself. This is useful for Distribution List integration.
- **Subscription notification formats:**

Subject Format and **Body Format:** Configure how the subject and body text should be formatted in subscription notifications by using HTML tags, or by using the following tokens:

 - `${msg-forum}`: Include the display name of the forum where the message was posted.
 - `${msg-topic}`: Include the subject of the topic under which the message was posted.
 - `${msg-from}`: Include the e-mail address of the author of the message.
 - `${msg-author}`: Include the name of the author of the message.
 - `${msg-subject}`: Include the subject of the newly posted message.
 - `${msg-sent-date}`: Include the date of the newly posted message.
 - `${msg-body}`: Include the text body part of the newly posted message.
 - `${msg-forum-url}`: Include the URL to access the forum where the message was posted.
 - `${msg-topic-url}`: Include the URL to access the topic where the message was posted.
 - `${msg-url}`: Include the URL to access the newly posted message.

Forums and Distribution Lists Integration

Forums can be easily be configured to archive email Distribution Lists. E-mail messages sent to Distribution Lists will be stored and threaded into a forum and, at the same time, messages posted to that forum from the Oracle Discussions Web UI will be forwarded to the Distribution List.

To integrate a forum with a Distribution List:

1. Create a Distribution List and add the forum e-mail address as a member of the Distribution List. This ensures that all messages sent to the Distribution List will also be stored in the forum.
2. Specify the Distribution List e-mail address as the e-mail forwarding policy for that forum, so that all messages posted to the forum will also be forwarded to the Distribution List. The Oracle Discussions server also makes sure that the messages are never forwarded in an infinite circular loop between the Distribution List and the forum e-mail address.

Accessing Oracle Discussions with RSS

Oracle Discussions exposes RSS newsfeeds for browsing and querying discussion topics. End users can use desktop RSS readers to browse forums and topics. RSS feeds can also be leveraged for basic application integration. Access to the RSS feeds is protected by HTTP Basic Authentication using JAZN/JAAS. The Oracle Discussions Web UI features a small orange XML icon wherever an RSS feed is available. RSS feeds are available for browsing lists of containers, list of topics in a forum, list of messages in a topic, 'popular' topics, 'favorites', 'my posts', replies to 'my posts', and search results.

The URL used for the RSS feed is based on the value of the `labeleduri;rss` attribute of the Oracle Discussions Virtual Service in the Oracle Internet Directory Service Registry. The links in the RSS feed referring back to the Oracle Discussions application are built using the value the `labeleduri;webui` attribute for the Oracle Discussions Virtual Service in the Oracle Internet Directory Service Registry.

See Also: For instructions for editing the Oracle Internet Directory Service Registry, see ["Managing the Oracle Internet Directory Service Registry"](#) on page 7-7

Accessing Oracle Discussions using E-mail

Oracle Discussions users can participate in forum discussions through their desktop e-mail clients. Discussions forums are accessible in desktop e-mail clients as e-mail shared folders. Users can browse the topics and messages of a given forum through Shared Folders. On e-mail clients that support grouping and threading, messages can be threaded and grouped by their topic. Users can post new topics from their e-mail clients by sending an e-mail to the forum e-mail address. Users can reply to existing topics by replying to messages contained in the 'forum' shared folder

Oracle Discussions Message Indexing for Search

Oracle Discussions search functionality leverages the indices provided in the `ES_MAIL` schema. The Discussions internal account `<discussions_<dbid>@<emaildomain>` is enabled for Oracle Text indexing of its messages. The indexing of Oracle Discussions message bodies and attachments is periodically performed by Oracle Text. The index update frequency is a parameter controlled in the Oracle Mail Housekeeper process.

Managing the End-User Documentation Portal

Oracle Collaboration Suite ships with an End-User Documentation Portal that provides an overview of Oracle Collaboration Suite clients as well as instructions on how to download, install, and configure the clients. If you choose to host the End-User

Documentation Portal, you have the ability to customize the information that it contains to suit your business needs. The End-User Documentation Portal comes with an administration panel to facilitate customization.

The End-User Documentation Portal uses PHP (recursive acronym for "PHP: Hypertext Preprocessor"). You must configure PHP in order to use the End-User Documentation Portal.

For information about installing the End-User Documentation Portal, see the chapter "End-User Documentation Portal Installation" in the Oracle Collaboration Suite installation guide of your platform. These instructions include directions for configuring PHP for the End-User Documentation Portal and securing the End-User Documentation Portal administration panel with Apache basic authentication.

If you do not want to use PHP, you may use the static version of the End-User Documentation Portal instead. However, you will not be able to use the administration panel to customize the End-User Documentation Portal; you will have to customize it manually with an HTML or text editor.

This section describes how to manage and customize the End-User Documentation Portal. It contains the following topics:

- [About the End-User Documentation Portal](#)
- [Customizing the End-User Documentation Portal](#)
- [Editing End-User Documentation Portal Views](#)
- [Using Static Version of End-User Documentation Portal](#)
- [Directory Structure of End-User Documentation Portal](#)
- [Editing Content in End-User Documentation Portal](#)

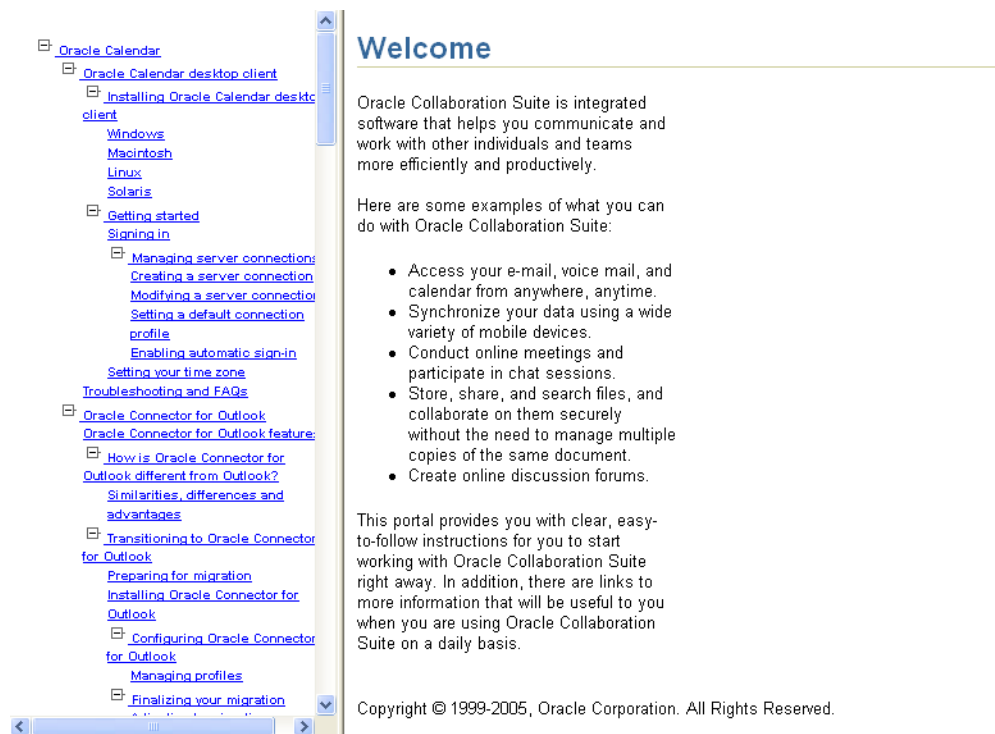
About the End-User Documentation Portal

The End-User Documentation Portal [Figure 5-3](#) displays two panels. In the left panel, a collapsible tree of topics is displayed. In the right panel, documents selected by the user are displayed.

Access the End-User Documentation Portal by navigating to the URL:

`http://<web host>/eupd/index.html`

Where `<web host>` is the Web location where you host the End-User Documentation Portal.

Figure 5–3 The End-User Documentation Portal

Customizing the End-User Documentation Portal

You can customize the End-User Documentation Portal from the Views page. [Figure 5–4](#) shows the End-User Documentation Portal Views page. From this page, you can create one or more Views, which are customized versions of the End-User Documentation Portal.

Access the Views page by navigating to the URL:

`http://<web host>/eupd/admin/view.php`

Where `<web host>` is the Web location where you host the End-User Documentation Portal.

Figure 5–4 End-User Documentation Portal Views page

Views

Original OCS TOC (OCS.xml) Default View			
Edit Title			
Create new view based on this view		Edit view	

OCS Copy (OCS_2.xml)			
Edit Title			
Create new view based on this view	Select as default view	Delete view	Edit view

By default, the End-User Documentation Portal comes with four views. These views correspond to the Oracle Collaboration Suite licensing options:

- Oracle Collaboration Suite (this View contains all of the topics for all of the Oracle Collaboration Suite applications)
- Oracle Unified Messaging
- Oracle Real-Time Collaboration
- Oracle Content Services

If you decide to present a different set of information to your users, you can edit the View to hide various topics, and to add your own custom topics. You may also create one or more custom Views, based on the original View provided with Oracle Collaboration Suite.

Note: The safest practice is to create a copy of the original view, customize it, and then display this new copy. This way the original View remains available, in case you need to revert back to it for any reason.

To create a new View:

1. Select **Create new view based on this view** on an existing view.

The New View page is shown.

2. Enter a title and file name for the new view, and select **Save file**.

The new view is created.

One view is always set to be the Default View. This is the view which users will see when they navigate to the End-User Documentation Portal. [Figure 5–4](#) shows two Views; one has been set to Default View and the other is an inactive copy.

To set any existing View to be the default view, select **Select as default view**. The view is immediately set to be the default view, and will be displayed when users visit the End-User Documentation Portal.

You can delete any View which you have created. You cannot delete any views that were shipped with the End-User Documentation Portal. To delete a View, select **Delete view**. The View is deleted.

Editing End-User Documentation Portal Views

You can customize any View by editing it. To edit a View, select **Edit view**. The Edit View page is displayed, showing a collapsible tree of topics and subtopics. [Figure 5–5](#) shows the Edit View page for a sample View called 'My Company'.

Figure 5–5 *End-User Documentation Portal Edit View page*

Save, and return to view menu Save changes, and continue working

Revert to previously saved view Cancel and return to view menu

My Company view

☐

Oracle Calendar
[Edit](#)

Add section before this one Add section after this one Hide section

☐

[Oracle Calendar desktop client](#)
./content/Calendar/DC/cal_desktop_home.html
[Edit](#)

Add section before this one Add section after this one Hide section

☐

[Installing Oracle Calendar desktop client](#)
./content/Calendar/DC/cal_desktop_install.html?install=#install_w
[Edit](#)

From the Edit View page, you can make all of your desired customizations.

When you are finished making your customizations, select **Save, and return to view menu**.

If you are making many customizations, you may want to periodically save your work. To do so, select **Save changes, and continue working**.

If you made some customizations but decided to revert back to the last saved version of this View, select **Revert to previously saved view**.

If you want to return to the View menu without applying any changes you made, select **Cancel and return to view menu**. Any changes you made since the last time you saved will be lost.

The End-User Documentation Portal lets you make the following customizations:

- Hide any visible section
- Show any hidden section

- Add a new section before or after any existing section
- Edit any section's title or URL
- Delete any custom section you added

Hiding Sections

You can hide one or more topics from view. For example, if your deployment of Oracle Collaboration Suite does not include Oracle Calendar, you might want to hide all of the Oracle Calendar documentation sections.

Sections are hierarchical. If you hide a parent section, it and all of its child sections are hidden from view.

To hide a section:

1. Scroll down through the Edit View window until you find the section you want to hide. If you collapsed any sections (by selecting the minus (-) sign) you may need to expand those sections (by selecting the plus (+) sign) to locate the section you want to hide.
2. Select **Hide section**.

The section and all of that section's child sections (if there are any) are marked as 'hidden'. They will no longer appear on the End-User Documentation Portal.

Showing Sections

If you previously hid any topics from view, you can decide later to show on them on the End-User Documentation Portal.

To show a section:

1. Scroll down through the Edit view window until you find the hidden section you wish to show. If you collapsed any sections (by selecting the minus (-) sign) you may need to expand those sections (by selecting the plus (+) sign) to locate the section you wish to expand.
2. Select **Show section**.

The section and all of that section's child sections (if there are any) are unmarked. They will now appear on the End-User Documentation Portal.

Adding a New Section

You can add custom sections to the End-User Documentation Portal. Once you add a new section, you should give it a title and enter a URL. The content found at the URL will display in the right panel of the End-User Documentation Portal whenever a user selects the title of your custom section in the left panel.

You may add your new section at any point in the topic tree.

To add a new section:

1. Scroll down through the Edit View window until you find the point where you want to add a new section. You can expand or collapse sections to find the exact point where you want to add your new section. Select the minus (-) and plus (+) signs to collapse or expand a section.
2. Select **Add section before this one** or **Add section after this one** from an existing section. A new section will be created before or after the existing section, at the same level of hierarchy as the section.

After you add a new section, you should Edit it to give it a title and URL.

Editing a Section

You can edit any section to change its title (which appears in the hierarchical view of topics in the End-User Documentation Portal) or URL (which determines the content displayed when a user selects the section's title).

To edit a section:

1. Scroll down through the Edit View window until you find the section you want to edit. You can expand or collapse sections to find a child section you want to edit. Select the minus (-) and plus (+) signs to collapse or expand a section.
2. Select **Edit**. The section will expand, providing fields for the Section title and the URL.

Figure 5–6 shows a custom section, called 'Example new section', after selecting **Edit**.

3. Make your desired changes to the Section title and URL. When you finished making changes, select **Submit changes** to apply them. Select **Cancel** to stop editing the section without applying any changes.
4. After you submit changes, the section contracts and the title and URL are saved. Test the new URL by selecting the title of the section; the browser will attempt to access the URL you provided.

Figure 5–6 End-User Documentation Portal - Editing a section

Save, and return to view menu	Save changes, and continue working
Revert to previously saved view	Cancel and return to view menu

My Company view

[Example new section](#)
<http://www.example.com>
Section title:
URL:
 [Cancel](#)

Add section before this one	Add section after this one
Add new subsection	Delete section Hide section

Deleting a Section

You can delete any custom section that you previously added to a View. You cannot delete the default sections. If you need to prevent users from seeing one of the default sections, you may hide it.

Tip: If you need to prevent users from seeing one of the default sections, you may hide it. See ["Hiding Sections"](#) on page 5-35.

To delete a custom section:

1. Scroll down through the Edit View window until you find the section you want to delete. You can expand or collapse sections to find a child section you want to delete. Select the minus (-) and plus (+) signs to collapse or expand a section.

2. Select **Delete section**. The Delete section button is only visible on custom sections that were added to the End-User Documentation Portal. Default sections may not be deleted.
3. A confirmation window will pop up to confirm that you want to delete this section. Select **OK** to delete the section, or select **Cancel**.

The custom section is deleted.

Using Static Version of End-User Documentation Portal

The End-User Documentation Portal uses PHP to generate the table of contents and control the administration panel. You may use the static version of the End-User Documentation Portal if you do not want to use PHP. This version contains all the End-User Documentation Portal content.

Access the static version of the End-User Documentation Portal by navigating to the URL:

`http://<web host>/eupd/index.static.html`

Where `<web host>` is the Web location where you host the End-User Documentation Portal.

You cannot customize the static version of the End-User Documentation Portal with the administration panel. To customize the table of contents of the static version of the End-User Documentation Portal, edit the file `eupd/menu.html` in a text or HTML editor.

Directory Structure of End-User Documentation Portal

This section describes the directory structure of the End-User Documentation Portal and the files that it contains.

The following is the directory structure of the End-User Documentation Portal:

- `eudp`
 - `admin`
 - `content`
 - `temp`
 - `views`

Contents of `eudp`

This directory contains the main entry points of the End-User Documentation Portal, as well as PHP files that contain the code that controls the End-User Documentation Portal and its administration panel.

Do not edit the files in this directory except those that are specified in this section.

This directory includes the following files. **Do not edit these files:**

- `index.html`: The main entry point for the End-User Documentation Portal
- `menu.php`: PHP file that generates the table of contents based on a particular view (which has been chosen from the administration panel)
- `AdminTree.php`: PHP file that contains the code for the End-User Documentation Portal administration panel. It also contains code that parses XML view files.

- `ViewTree.php`: PHP file that contains the code that manages views

This directory includes the following files that you may edit:

- `blank.html`: The first HTML file that users will see when they access the End-User Documentation Portal
- `index.static.html`: The main entry point for the static version of the End-User Documentation Portal. This is for servers that do not have PHP installed. This page will display all the contents of the End-User Documentation Portal; you will not be able to use the End-User Documentation Portal administration panel to edit the contents of this page.
- `menu.html`: The table of contents used by `index.static.html`. This is simply an unordered list of links. Edit this file if you wish to change the table of contents for the static version of the End-User Documentation Portal.

Contents of admin

This directory contains the main entry point of the End-User Documentation Portal administration panel. To restrict users from the administration panel, use Apache's `htpasswd` utility to protect this directory. See Apache's documentation for more information about restricting users access to directories.

Do not edit files in this directory.

This directory includes the following files:

- `view.php`: The main entry point for the End-User Documentation Portal administration panel
- `constants.inc`: Contains text labels used by End-User Documentation Portal administration panel
- `messages.inc`: Contains status, warning, and error text used by End-User Documentation Portal administration panel
- `Configuration.php`: PHP file that contains code that generates the custom table of contents based on a particular view
- `main.php`: PHP file that contains code that manipulates a particular view. Do not access the administration panel with this file; only access the administration file with `view.php`.

Contents of content

This directory contains HTML end-user documentation. You may edit these files depending on your Oracle Collaboration Suite installation. This directory contains directories that correspond to each of Oracle Collaboration Suite's components.

Contents of temp

The End-User Documentation Portal administration panel uses this directory to store temporary changes to the End-User Documentation Portal.

Do not edit files in this directory.

Contents of views

This directory contains Views that come with the End-User Documentation Portal and Views that you have created with the administration panel. Views are stored as XML files.

Do not edit files in this directory.

This directory includes the following files:

- `config.xml`: XML file that contains configuration information pertaining to views
- `masterlist.xml`: XML file that lists all the views
- `ocs.xml`: View that contains all of the topics for all of the Oracle Collaboration Suite applications

Editing Content in End-User Documentation Portal

You may edit content of the End-User Documentation Portal as well as add pages to it. You may add any URL to the End-User Documentation Portal; it will accept any HTML page. You do not even have to store your HTML pages in the `eudp/content` directory.

This section describes the structure of the HTML pages in the End-User Documentation Portal. This information will allow you to create Web pages with a similar look-and-feel to those included in the End-User Documentation Portal.

Structure of HTML Pages

The following is the structure of HTML pages in the End-User Documentation Portal:

```
<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">

<head>
  <title>Title of Your Web Page</title>
  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
  <style type="text/css" media="screen">
    @import url("blafdoc.css");
    <!-- Ensure the location of this style sheet
         is in same directory as this file, or that
         you have the correct path to this style sheet -->
  </style>
</head>

<body>
  <div id="header"><h1>Title of Your Web Page</h1></div>
  <div id="content">
    <p>Insert the content of your Web page here.</p>
    <p class="last">&nbsp;</p> <!-- Do not delete -->
  </div>

  <div id="footer">Enter your copyright statement here.</div>

</body>
</html>
```

The following lists in detail the characteristics of HTML pages in the End-User Documentation Portal:

- These pages use the style sheet `blafdoc.css`. You should be able to find this file in any directory in the `eudp/content` directory. Copy this style sheet in the same directory as your HTML page.

- These pages use three <div> tags:
 - header: This contains the title of your Web page. Wrap the title of your Web page with <h1> tags.
 - content: This contains the content of your Web page. Note that the <div id="content"> tag is embedded in the <div id="header"> tag. Ensure that you add a non-breaking space wrapped with a <p class="last"> tag to the end of your content.
 - footer: This contains the copyright statement of your Web page.

Managing Oracle Application Server Portal and Oracle Collaborative Portlets

Oracle Application Server Portal is a feature of Oracle Application Server. Oracle Collaboration Suite leverages OracleAS Portal by using Oracle Collaborative Portlets, a set of portlets which combine to present users with a summarized version of each Oracle Collaboration Suite application.

OracleAS Portal uses Oracle Application Server Web Cache together with OracleAS Portal's own file-based caching to cache page definitions and content in memory, to boost performance. OracleAS Portal is closely integrated with OracleAS Web Cache to improve Portal's overall availability, scalability, and performance.

This section contains the following topics:

- [Managing Oracle Application Server Portal](#)
- [Managing Oracle Collaborative Portlets](#)

Managing Oracle Application Server Portal

Oracle Collaboration Suite Control Console can be used for monitoring, diagnostics, and for the configuration of OracleAS Portal specific integration and performance settings. The Grid Control Console can be used for monitoring OracleAS Portal, and tracking historical trends, but not for configuration.

To monitor and administer OracleAS Portal, select **Portal:<portal schema name>** in the System Components list on the Oracle Collaboration Suite home page for the Applications tier instance hosting OracleAS Portal. The default portal schema name is **portal**. Note that **OC4J_Portal** is the container for portal servlets, and not the actual portal servlet to monitor.

The main page for monitoring OracleAS Portal that is displayed, is shown in [Figure 5-7, "Oracle Collaboration Suite Control - Main OracleAS Portal Monitoring Page"](#) on page 5-41.

You can also access this page directly from OracleAS Portal. Log in to the portal with an administrator account, click the **Administer** tab on the Portal Builder page and then click **Portal Service Monitoring** (located on the **Portal** sub-tab).

Figure 5–7 Oracle Collaboration Suite Control - Main OracleAS Portal Monitoring Page

ORACLE Enterprise Manager 10g
Application Server Control for Collaboration Suite

[Logs](#) [Topology](#) [Preferences](#) [Help](#)

[Farm](#) > [Application Server: OCS Apps.stanc05.us.oracle.com](#) >
Portal:portal

Page Refreshed Apr 30, 2005 2:08:50 PM

General

Status	Up
Average Page Requests Per Hour	13
Homepage Download (seconds)	0.133
Monitoring Services	Down

OracleAS Metadata Repository Used By Portal

Status	Up
Name	OCSM12DB
Start Time	Apr 22, 2005 3:12:35 PM
Database Version	10.1.0.4.0
Repository Version	10.1.2.0.2 (Build: 6)

Component Status

OracleAS components used by Portal.

Component	Up/Down
HTTP Server	
Parallel Page Engine Services	
Providers	
Ultra Search	

Severity Status

OracleAS components used by Portal that indicate severity status.

Component	Severity
Parallel Page Engine Services	
Providers	

OK Warning Critical Unknown

Administration

[Portal Web Cache Settings](#)
[Portal Cache Settings](#)
[Portal DAD Settings](#)

Related Links

[Portal End User Default Homepage](#)
[All Metrics](#)

[Logs](#) | [Topology](#) | [Preferences](#) | [Help](#)

Copyright © 1996, 2005, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control for Collaboration Suite

From the Oracle Collaboration Suite Control Console, you can specify the OracleAS Web Cache settings that OracleAS Portal should use. Select the **Portal Web Cache Settings** link, under **Administration**, to display the **Portal Web Cache Settings** page. When you set OracleAS Web Cache properties on this page, the Portal Dependency Settings file located on this Applications tier is updated automatically, and the OracleAS Portal schema is also updated

Notes:

- Changing OracleAS Web Cache settings (for example, Listening Port) can change the OracleAS Portal URL. If you do this, your mobile settings need to be updated. For more information, see *Oracle Application Server Portal Configuration Guide*
 - If the invalidation settings change, you must update `cache.xml` with the values of the invalidation host and port number. `cache.xml` is located in `[ORACLE_HOME]/portal/conf` (on UNIX) and `[ORACLE_HOME]\portal\conf` (on Windows).
 - If the OracleAS Web Cache user name or password is changed, you must update `cache.xml` with the changed information. `cache.xml` is located in `[ORACLE_HOME]/portal/conf` (on UNIX) and `[ORACLE_HOME]\portal\conf` (on Windows). For information on obfuscating user name and password, refer to the *Oracle Application Server Portal Developer's Guide*.
-

See Also: *Oracle Application Server Portal Configuration Guide* for information about changing the portal web cache settings of OracleAS Portal

Configuring OracleAS Portal After Installation

During an Applications tier installation that includes OracleAS Portal, you can specify if you want to configure, and automatically start OracleAS Portal at the end of the installation. If you select that option, Oracle Universal Installer will configure OracleAS Portal in two phases:

1. OracleAS Portal Applications tier deployment
2. OracleAS Portal schema configuration in the OracleAS Metadata Repository

If you choose not to configure OracleAS Portal during installation, and want to do this later, you need to:

- Use Oracle Collaboration Suite Control Console to deploy OracleAS Portal on the Applications tier. Refer to ["Adding Applications to your Oracle Collaboration Suite Deployment"](#) on page 5-64 for more information.
- Use the Portal Dependency Settings file and tool, to perform the OracleAS Portal schema configuration in the OracleAS Metadata Repository. You need to perform this step, because OracleAS Metadata Repository configuration is not performed by default, when you use Oracle Collaboration Suite Control Console, so that existing configuration entries in the OracleAS Metadata Repository are not automatically overwritten. Refer to Appendix A of *Oracle Application Server Portal Configuration Guide* for more information.

You can update the OracleAS Metadata Repository with any changes made to the Portal Dependency Settings file `iasconfig.xml`, related to Applications tier component properties, such as OracleAS Web Cache, and Oracle Enterprise Manager 10g.

Portal does not support serving two Applications tiers from a single repository, unless it is front-ended by a load balancing router (LBR). Refer to *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows* for instructions on how to set up OracleAS Portal with an LBR. If you want to add additional Applications tiers to a farm that is already using OracleAS Infrastructure Services, you do not want to overwrite the existing configuration entries during the deployment. In this case, you would install the additional Applications tier without configuring OracleAS Portal, then configure OracleAS Portal, using Oracle Collaboration Suite Control Console, and finally update the Portal Dependency Settings file.

Note: By default, `iasconfig.xml` resides in `ORACLE_HOME/portal/conf`. If the Portal Dependency Settings file is accessible over a network file system, you can share the file across multiple hosts, avoiding the need to manually replicate it every time the file is modified. If the installation is running on an operating system that supports symbolic links, it is recommended that you use this mechanism to reference a shared file. If, however, the Portal Dependency Settings file is not accessible over the network, you must ensure that the file is kept up-to-date with changes to your site topology. Refer to Appendix A of *Oracle Application Server Portal Configuration Guide* for more information.

To use Oracle Collaboration Suite Control Console to deploy OracleAS Portal on the Applications tier, follow the steps outlined in ["Adding Applications to your Oracle Collaboration Suite Deployment"](#) on page 5-64.

At this point, your OracleAS Portal Applications tier components are deployed and configured. The DAD has been created, and the Portal Dependency Settings file `iasconfig.xml` has been updated.

To update the OracleAS Metadata Repository with any changes made to the Portal Dependency Settings file `iasconfig.xml`, run the script `ptlconfig`, located in the directory `ORACLE_HOME/portal/conf`, as follows:

```
ptlconfig -dad portal
```

Additional Applications tiers are often added to production sites, to improve scalability. The two-phased process described in the preceding text allows the flexibility of adding additional Applications tiers, without system downtime.

Managing Oracle Collaborative Portlets

Oracle Collaborative Portlets requires special procedures different than other Oracle Collaboration Suite applications when updating or making changes to its configuration.

This section contains the following topics:

- [Changing the Host or Port on an Applications Tier hosting Oracle Collaborative Portlets](#)
- [Configuring Oracle Collaborative Portlets with Multiple Applications Tiers](#)
- [Using SSL in Oracle Collaborative Portlets](#)

Changing the Host or Port on an Applications Tier hosting Oracle Collaborative Portlets

If the host name or port is changed on the Oracle Collaborative Portlets Applications tier then the Portlet Providers need to be re-registered. This is done by invoking the Oracle Collaborative Portlets Configuration Assistant from the command line, and passing in the new host or port values as parameters.

To run the Oracle Collaborative Portlets Configuration Assistant from the command-line:

```
[ORACLE_HOME]/ocsprovs/bin/ocsprovs_installer.sh -mode complete -ouser <oid_admin_user> -opass <oid_admin_password> -ipass <ias_password> -host <host_name> -clist <listen_port> -cinv <invalidation_port>
```

Set `-host` to the host name that Collaborative Portlets will be accessed through. In a load-balancer (LBR) environment, this is the LBR host name; otherwise it is the Applications tier host name.

Set `-clist` to the web cache listen port. This is the same port that all the applications are accessed on. In a load-balancer (LBR) environment, use the port which the LBR uses for incoming HTTP requests.

Set `-cinv` to the OracleAS Web Cache invalidation port. In a load-balancer (LBR) environment, use the port which the LBR uses for incoming invalidation requests.

Note: Running the Oracle Collaborative Portlets Configuration Assistant will re-generate the OracleAS Portal home page, so if the page has been modified (edited) or users have customized their portlets the changes will be lost, and settings restored back to the default out-of-the-box values.

Configuring Oracle Collaborative Portlets with Multiple Applications Tiers

Oracle Collaboration Suite supports multiple instances of Oracle Collaborative Portlets (on multiple Applications tiers), but only if you use a load-balancer.

See Also: For information on deploying Oracle Collaboration Suite in various High Availability configurations, see *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

During installation of an Oracle Collaboration Suite Applications tier, Collaborative Portlets is always a selectable component.

If you select Collaborative Portlets, the installer checks the OracleAS Metadata Repository to see if a OracleAS Portal has already been configured against it. This might be the case if you have an existing OracleAS Portal and OracleAS Infrastructure which you are installing Oracle Collaboration Suite applications into. If the installer detects that this is the case it will show the following message:

```
The Metadata Repository that you have chosen to use already has an existing
Oracle Portal instance configured against it.  If you would like to continue
to use this Portal instance, select `Yes` and the Oracle Collaborative
Portlets will be configured to use this existing Portal instance.
If you would like to create a new Portal instance during this install instead,
choose `No`
```

NOTE: Choosing to install a new Portal instance during this install will cause any existing Portal instances in this Metadata Repository to stop functioning.

If you select Collaborative Portlets, the installer also checks the OracleAS Metadata Repository to see if BOTH a OracleAS Portal and Collaborative Portlets have been configured against it. This might be the case if you are performing a second Oracle Collaboration Suite Applications tier installation against the same Infrastructure, and you selected Collaborative Portlets in the first Applications tier install (meaning OracleAS Portal and Collaborative Portlets were configured against the OracleAS Metadata Repository in the first Applications tier installation). If so, the installer shows the following message:

```
The installation has detected that Oracle Collaborative Portlets has already
been configured in the Metadata Repository you have selected. Oracle
Collaborative Portlets will be unselected for configuration.
```

No choice is given here. In this case you must use a load balancer (LBR) to support multiple OracleAS Portal and Collaborative Portlets Applications tiers, and you should consult the High Availability documentation.

If you select Collaborative Portlets during the Applications tier install, and neither OracleAS Portal nor Collaborative Portlets are configured against the OracleAS Metadata Repository (as is the case in the first Oracle Collaboration Suite Applications tier installation), then no messages are shown.

In order to set up multiple instances of Oracle Collaborative Portlets for a load-balanced, High Availability deployment, you will have to run the Configuration Assistant.

See Also: For instructions on setting up load-balanced Applications tiers, including load-balancing Collaborative Portlets, see *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

If you choose to host instances of Oracle Collaborative Portlets on different Applications tiers than OracleAS Portal (for example, if OracleAS Portal is configured on apps1 and Oracle Collaborative Portlets is configured on apps2) then the images within the Oracle Collaborative Portlets will break. This is because the images are stored with relative pathnames, on the assumption that OracleAS Portal can find Oracle Collaborative Portlets images on the same machine. To fix this problem, you must edit the pathnames to be fully-qualified; that is, to point to the image file locations on the Oracle Collaborative Portlets host machine (or in a load-balancer environment, the LBR virtual host name).

To correct broken images in this situation:

1. Edit the file `ocsprovs.properties` in the Applications tier Oracle home hosting the OracleAS Portal instance having broken images:


```
[ORACLE_
HOME]/ocsprovs/classes/oracle/webdb/install/resource/ocsprovs.properties
```
2. Change each image path to point to the URL of an Applications tier hosting Oracle Collaborative Portlets
3. Fix the Oracle Collaboration Suite logo from the OracleAS Portal configuration page:

Change the relative URL to an absolute URL of the Applications tier hosting Oracle Collaborative Portlets

Using SSL in Oracle Collaborative Portlets

Oracle Collaborative Portlets uses HTTP internally to communicate with Oracle Collaboration Suite component application Web services (such as Oracle Mail and Oracle Calendar) to obtain application data. The use of SSL is not supported at this level.

In addition, if you configure SSL for Oracle Collaboration Suite and turn off the non-SSL (HTTP) port, then Oracle Collaborative Portlets will stop functioning. In other words, Oracle Collaborative Portlets requires the Web Cache non-SSL (HTTP) port to remain open.

Note: This is applicable for internal HTTP communication only. This *does not* affect external HTTP-based communication between browsers and Oracle Collaboration Suite.

Managing Oracle Web Access Client

Oracle Web Access Client is a browser-based application that looks, feels, and performs like a desktop application. It provides access to various features of Oracle Collaboration Suite, including:

- E-mail with support for HTML editing
- Personal and shared Address Books with Corporate Directory (Global Address Book) integration and support for shared contacts

- TimeBar view of calendar appointments and reminders, with direct access to the Oracle Calendar Web client for creating and editing meetings

Oracle Web Access Client supports standard Web browsers, including Internet Explorer, Mozilla and Mozilla Firefox. Personal preferences are stored on the server.

Oracle Web Access Client makes use of Directory Cache, a component of Oracle Mail that, when enabled, builds an in-memory cached copy of Contacts, enabling faster lookup of user information when using the Oracle Web Access Client.

See Also: Chapter 5, "Directory Cache", in the *Oracle Mail Administrator's Guide*

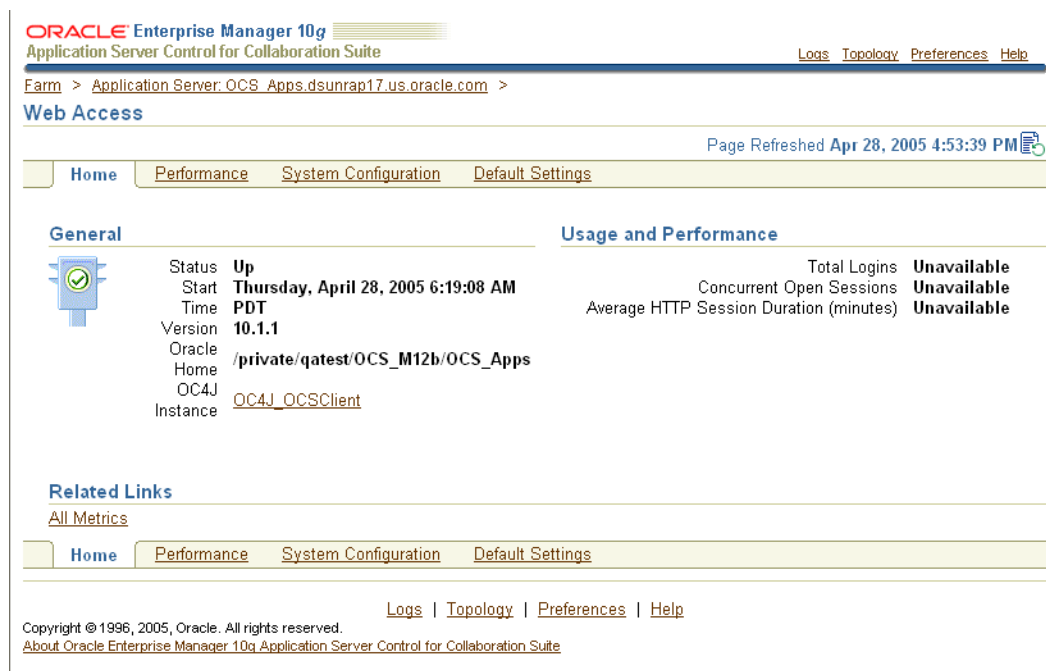
You can perform administration tasks for Oracle Web Access Client using the Oracle Collaboration Suite Control Console.

To view the general monitoring information and performance metrics for Oracle Web Access Client:

1. Log in to the Oracle Collaboration Suite Control Console
2. From the Oracle Collaboration Suite home page, select the Applications server that is hosting Oracle Web Access Client
3. Select Web Access from the System Components list

The Web Access control page opens, showing the Home tab. See [Figure 5–8](#).

Figure 5–8 Oracle Collaboration Suite Control - Oracle Web Access Client Control Page



This section contains the following topics:

- [Viewing Oracle Web Access Client Performance Metrics](#)
- [Managing Oracle Web Access Client System Configuration](#)
- [Managing Oracle Web Access Client Default Settings](#)

- [Configuring Oracle Web Access Client for Non-Single Sign-On IMAP Mode](#)

Viewing Oracle Web Access Client Performance Metrics

You can view in-depth performance metrics for Oracle Web Access Client, by viewing the Oracle Web Access Client Performance tab in the Oracle Collaboration Suite Control Console.

To view in-depth performance metrics for Oracle Web Access Client:

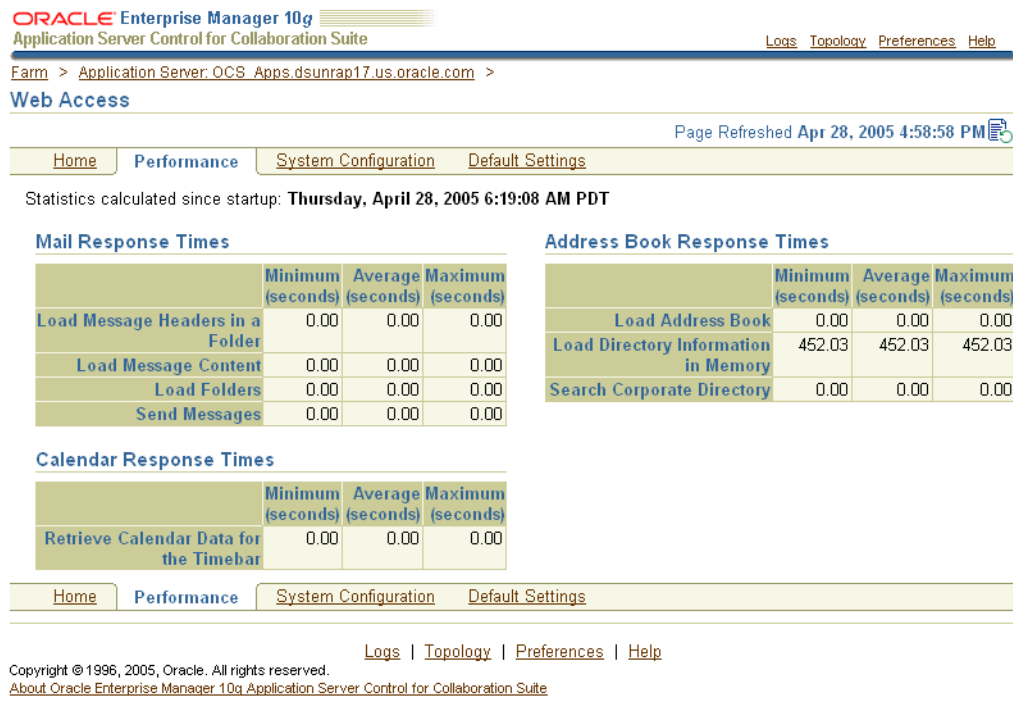
1. Log in to the Oracle Collaboration Suite Control Console
2. From the Oracle Collaboration Suite home page, select the Applications server that is hosting Oracle Web Access Client
3. Select Web Access from the System Components list

The Web Access control page opens, showing the Home tab. See [Figure 5-8](#).

4. Select the Performance tab

The Web Access Performance tab opens, displaying in-depth performance metrics for Oracle Web Access. See [Figure 5-9](#)

Figure 5-9 Oracle Web Access Client Performance Metrics



Managing Oracle Web Access Client System Configuration

You can reconfigure the behavior of Oracle Web Access Client by using the System Configuration tab in the Oracle Collaboration Suite Control Console.

[Table 5-3, "Oracle Web Access Client System Configuration Parameters"](#) shows the parameters which you can modify, their default and available values, and a description of each parameter.

Table 5–3 Oracle Web Access Client System Configuration Parameters

Parameter	Default Value	Available Values	Description
General			
Use GZIP compression for all dynamic and static content	<checked>	<checked>, <unchecked>	Determines whether content should be compressed prior to transmission between the server and the client. Leave this enabled (checked) unless GZIP compression causes compatibility problems with users' browser clients and Oracle Support recommends disabling it.
Logging			
Log Level	INFO	ALL, OFF, FINEST, FINER, FINE, CONFIG, INFO, WARNING, SEVERE	Sets the verbosity of the Oracle Web Access Client log.
Rotation Number	20	1-1000	Sets the maximum number of log files that the system may create.
File Size (MB)	10	0-2000	Sets the maximum size for each log file. Setting this value to zero disables logging.
File Location	ocscient/log	<any valid path>	Sets the location for Oracle Web Access Client log files to be created, relative to the <code>[ORACLE_HOME]</code> .
Directory Cache			
Store directory information in memory	<checked>	<checked>, <unchecked>	Whether to cache directory information in RAM. Doing so improves directory lookup performance at the expense of memory usage. Leave this enabled (checked) unless directory caching results in excessive memory consumption and Oracle Support recommends disabling it.
Update Interval (hours)	24	1-32768	Time elapsed before the Directory Cache is refreshed. If directory caching is enabled, changes in the directory (such as newly-provisioned users or updated user information) will not be visible in Oracle Web Access Client until the next time the directory cache is updated or the <code>OC4J_OCSCient</code> container is restarted. Setting the update interval to a shorter period (e.g. 4 hours) will keep the directory cache more up-to-date, but will incur additional load on the Oracle Internet Directory server. For organizations with tens of thousands of users, Oracle recommends setting the update interval to no fewer than 4 hours.

Table 5–3 (Cont.) Oracle Web Access Client System Configuration Parameters

Parameter	Default Value	Available Values	Description
Search Type	Starts With	Contains, Starts With	Sets the type of directory lookup search users may perform in Oracle Web Access Client. This setting determines whether the directory cache index is optimized for substring or prefix search. For example, if the Search Type is set to "contains," a search for "ter" would match both "Peterson" and "Terry," while if the Search Type is set to "starts with," a search for "ter" would only match "Terry" but not "Peterson." In general, a Search Type of "contains" will result in more matches than a search type of "starts with." In case of East Asian locales (such as Chinese, Japanese, or Korean), Oracle recommends setting Search Type to "contains," while for other locales, the recommended Search Type is "starts with."
Address Book			
Search Results	1000	1-32768	Sets the maximum number of results to return from a directory lookup search. Note: if this value is set to be higher than the internal value of <code>orclsizeLimit</code> in Oracle Internet Directory (default = 1000), then that value is used instead. Oracle recommends setting this value to no more than 10,000; the default value of 1,000 should be sufficient for most deployments.
Messaging			
Send Mail Mode	SMTP	OJMA, SMTP	Sets the protocol to be used for send mail actions.
Message Size (KB)	5120	0-51200	Sets the maximum outgoing message size, including headers, body, and attachments. If you set this value to zero, it will be reset back to the default value.
Signature Size (KB)	128	1-512	Sets the maximum size of a user's signature in outgoing messages

Table 5–3 (Cont.) Oracle Web Access Client System Configuration Parameters

Parameter	Default Value	Available Values	Description
Initial Download	3000	0-32768	Sets the maximum number of messages to attempt to download when a user first connects to Oracle Web Access Client. If this value is set to zero, all headers are downloaded. Since Oracle Web Access Client is a pure thin client with no persistent local storage, it must download e-mail message headers each time the user logs in. This setting can be used to limit the number of message headers fetched by Oracle Web Access Client when a user opens an e-mail folder (such as the Inbox). Message headers are downloaded in most-recent-first order, up to the total number of headers in the folder or this limit, whichever comes first. Older message headers can still be accessed using Mail Search, or users may choose to download all message headers on demand.
Search Results	1000	1-5000	Sets the maximum number of results returned when a user searches for messages. Oracle recommends setting this value to no more than 1,000 (the default). Higher numbers result in much longer response times when there are thousands of results for a search term.
Auto-Complete			
Characters	3	2-10	Sets the minimum number of characters a user must enter before auto-complete shows a drop-down of possible choices. In case of East Asian locales (such as Chinese, Japanese, or Korean), Oracle recommends setting this to the lowest value, 2. For other locales, and for organizations with tens of thousands of users in the directory, Oracle recommends settings of 3 or 4.
Results Limit	30	10-50	Sets the maximum number of results in an auto-complete drop-down list.

To manage system configuration parameters for Oracle Web Access Client:

1. Log in to the Oracle Collaboration Suite Control Console
2. From the Oracle Collaboration Suite home page, select the Applications server that is hosting Oracle Web Access Client
3. Select Web Access from the System Components list
The Web Access control page opens, showing the Home tab. See [Figure 5–8, "Oracle Collaboration Suite Control - Oracle Web Access Client Control Page"](#).
4. Select the System Configuration tab
The Web Access System Configuration tab opens, displaying configuration parameters for Oracle Web Access. See [Figure 5–10, "Oracle Web Access Client System Configuration"](#)

Figure 5–10 Oracle Web Access Client System Configuration

Home Performance **System Configuration** Default Settings

All system configuration changes are persisted in the Collaboration Suite infrastructure database. In order for these changes to take effect, all instances of Oracle Web Access (OC4J_OCSCClient) that share this database need to be restarted. Revert Apply

General

☒ Use Single Sign On (SSO) to authenticate

☒ Use GZIP compression for all dynamic and static content
Reduces network load at the expense of server performance.

Logging

Log Level INFO
Per JDK 1.4 specification.

Rotation Number 20
Maximum number of files created. Valid values: 1-1000.

File Size (MB) 10
Maximum size for each log file. Valid values: 0-2000.

File Location ocscclient/log
Location relative to ORACLE_HOME.

Directory Cache

☒ Store directory information in memory
Increases search speed.

Update Interval (hours) 24
Time elapsed before cache is refreshed.

Search Type Starts With

Address Book

Search Results 1000
Maximum number of items returned in a search. If this number exceeds the Internet Directory maximum, the latter value is used instead.

Messaging

Send Mail Mode OJMA
OJMA mode can be used only when SSO is enabled.

Message Size (KB) 5120
Maximum outgoing message size, including headers, body, attachments, etc. Valid values: 0-51200.

Signature Size (KB) 128
Maximum size. Valid values: 1-512.

Initial Download 10000
Maximum number of messages that will be downloaded initially. 0 means all messages will be downloaded.

Search Results 1000
Maximum number of messages returned in a search. Valid values: 1-5000.

Auto-Complete

Characters 3
Minimum number of characters to enter before auto-complete drop-down appears. Valid values: 2-10.

Results Limit 30
Maximum number of results in an auto-complete drop-down list. Valid values: 10-50.

Home Performance **System Configuration** Default Settings

- Make your desired changes. When you are finished, select **Apply** to save your changes, or select **Revert** to revert to the stored values without applying any changes you have made.
- Restart all instances of Oracle Web Access Client (OC4J_OCSCClient) for your changes to take effect. You can restart Oracle Web Access Client from the Applications tier home page in Oracle Collaboration Suite Control Console, or by running the following command from the *ORACLE_HOME* of your Applications tier:

```
[ORACLE_HOME]/opmn/bin/opmnctl restartproc ias-component=OC4J
process-type=OC4J_OCSCClient
```

See Also:

- To create, edit, and delete the default categories available to users in Oracle Web Access Client, see ["Managing Oracle Contacts Default Categories"](#) on page 5-15
- To change the maximum number of address book entries a user may create, see ["Managing Oracle Contacts Maximum Entries"](#) on page 5-17

Managing Oracle Web Access Client Default Settings

You can set the default values for various user-configurable settings in Oracle Web Access Client. Users can override the default values for these settings, by changing their Preferences from within the Oracle Web Access Client client interface. You can also reset all user's preference selections back to the default values by selecting **Reset**.

Table 5–4, "Oracle Web Access Client Default Settings Parameters" shows the parameters which you can modify, their default and available values, and a description of each parameter.

Note: Note that changing the default folder names as shown in this table only impacts the internal name of the IMAP folder created in the Oracle Mail server. End users will continue to see localized, user-friendly folder names in the Oracle Web Access Client UI. To change how folder names are displayed to end users, you must customize Oracle Web Access Client.

Table 5–4 Oracle Web Access Client Default Settings Parameters

Parameter	Default Value	Available Values	Description
E-mail Folder Names			
Sent Items	Sent Items	<Any text up to 100 characters>	Sets the default name of the folder used to store sent items
Deleted Items	Deleted Items	<Any text up to 100 characters>	Sets the default name of the folder used to store deleted items
Drafts	Drafts	<Any text up to 100 characters>	Sets the default name of the folder used to store drafts
Templates	Templates	<Any text up to 100 characters>	Sets the default name of the folder used to store templates
Character Encoding			
Character Set	Unicode UTF-8	(varies, depending on deployment)	Sets the default character set to use for incoming messages when Oracle Mail cannot determine the correct character set
Messaging			

Table 5–4 (Cont.) Oracle Web Access Client Default Settings Parameters

Parameter	Default Value	Available Values	Description
Show deleted messages	<unchecked>	<checked>, <unchecked>	This option is presented for the purposes of backwards compatibility with older e-mail clients, such as Netscape Messenger and Outlook Express. These older e-mail clients leave deleted messages in their original folder until the user manually compacts the folder. This setting governs whether to show or hide messages such as these. Messages deleted using Oracle Web Access Client will always be moved to the Deleted Items folder immediately, and this setting doesn't affect them.
Automatically check for new messages	<checked>	<checked>, <unchecked>	Sets whether the Oracle Web Access Client client will attempt to check for new messages periodically while it is open
Frequency (minutes)	10	5, 10, 15, 30, 60	Sets the default frequency to check for new messages if 'Automatically check for new messages' is <checked>
Appearance			
Layout	T-Pane	T-Pane, 3-Pane, 2-Pane	Sets the default appearance of the Oracle Web Access Client client interface
Skin	Traditional	Traditional, Custom (Modern, any custom skins added)	Selects the default skin to use for the Oracle Web Access Client client interface.
Menus and Toolbars	Default	Default, Custom (Modern, any custom menus and toolbars added)	Selects the default appearance of menus and toolbars in the Oracle Web Access Client client interface.

To manage Oracle Web Access Client default settings:

1. Log in to the Oracle Collaboration Suite Control Console
2. From the Oracle Collaboration Suite home page, select the Applications server that is hosting Oracle Web Access Client
3. Select Web Access from the System Components list

The Web Access control page opens, showing the Home tab. See [Figure 5–8, "Oracle Collaboration Suite Control - Oracle Web Access Client Control Page"](#).

4. Select the Default Settings tab

The Web Access Default Settings tab opens, displaying default setting parameters for Oracle Web Access. See [Figure 5–11, "Oracle Web Access Client Default Settings"](#)

Figure 5–11 Oracle Web Access Client Default Settings

ORACLE® Enterprise Manager 10g
Application Server Control for Collaboration Suite

Logs Topology Preferences Help

Farm > Application Server: OCS M15 Apps.dsunrdd16.us.oracle.com >

Web Access

Page Refreshed Jul 2, 2005 12:02:25 PM

Home Performance System Configuration **Default Settings**

All changes are saved in the Collaboration Suite infrastructure database. For these changes to take effect, you must restart all instances of Oracle Web Access (OC4J_OCSCClient) that share this database. These changes will only affect newly-provisioned users and users who have not yet used Web Access. Revert Apply

Email Folder Names

Sent Items

Deleted Items

Drafts

☒ **TIP** Folder names must not contain slashes ("/") and must not exceed 100 characters.

Character Encoding

Character Set Used when character set can not be determined.

Messaging

☐ Show deleted messages

☒ Automatically check for new messages

Frequency (minutes)

Appearance

Layout

☒ T-Pane ☐ 3-Pane ☐ 2-Pane

Skin

☒ Traditional ☐ Custom:

Menus and Toolbars

☒ Default ☐ Custom:

Reset All Users to Defaults

The default settings generally affect only newly-provisioned users and those who sign in to Web Access for the first time. To apply default settings to ALL users, do a reset. A reset removes all user-side Web Access preferences stored in the Collaboration Suite database; the next time users log in, their preferences will be based on the default settings. Reset

Home Performance System Configuration **Default Settings**

Logs | Topology | Preferences | Help

Copyright © 1996, 2005, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control for Collaboration Suite

5. Make your desired changes. When you are finished, select **Apply** to save your changes, or select **Revert** to revert to the stored values without applying any changes you have made.
6. Restart all instances of Oracle Web Access Client (OC4J_OCSCClient) for your changes to take effect. You can restart Oracle Web Access Client from the Applications tier home page in Oracle Collaboration Suite Control Console, or by running the following command from the `ORACLE_HOME` of your Applications tier:

```
[ORACLE_HOME]/opmn/bin/opmnctl restartproc ias-component=OC4J_OCSCClient
```

Note: Changing the default settings does not affect current Oracle Web Access Client users. The defaults are only applied when a new user first logs in to Oracle Web Access Client. You can revert all existing users back to the default values by selecting **Reset**.

See Also:

- To create, edit, and delete the default categories available to users in Oracle Web Access Client, see ["Managing Oracle Contacts Default Categories"](#) on page 5-15
- To change the maximum number of address book entries a user may create, see ["Managing Oracle Contacts Maximum Entries"](#) on page 5-17

Configuring Oracle Web Access Client for Non-Single Sign-On IMAP Mode

Under normal operation, Oracle Web Access Client is integrated with Oracle Application Server Single Sign-On for user authentication. This involves making a connection to Oracle Internet Directory. However, it is possible to run Oracle Web Access Client as a stand-alone application, using IMAP protocol to authenticate users. This section describes how to enable and disable IMAP mode for Oracle Web Access Client.

In order to enable IMAP mode, you must set up your own IMAP and SMTP servers.

To enable IMAP mode:

1. Install Oracle Web Access Client, which will be connected to Oracle Internet Directory for SSO by default. For more information about installing Oracle Web Access Client, see the Oracle Collaboration Suite Installation Guide for your platform.
2. Edit the file `[ORACLE_HOME]/j2ee/OC4J_OCSClient/config/oc4j.properties` on the Applications tier where Oracle Web Access Client is installed, to add the properties listed as required, below. For each property, replace values in angle-brackets (such as `<PORT>`) with the appropriate value.

Tip: Before editing the file, you may wish to make a backup copy of it. If you ever need to reverse this procedure (to restore normal Oracle Application Server Single Sign-On operation with Oracle Internet Directory integration), it will be easy to restore the backup copy of the file.

- a. Turn off SSO mode (**Required**):

```
oracle.ocscclient.sso.enable=false
```

- b. Enter host and port values for the IMAP and SMTP servers you will use (**Required**):

```
oracle.ocscclient.imap.host=<IMAP SERVER>
oracle.ocscclient.imap.port=<IMAP PORT>
oracle.ocscclient.smtp.host=<SMTP SERVER>
oracle.ocscclient.smtp.port=<SMTP PORT>
```

- c. Set login user IDs to use a domain name (**Optional**):

```
# If this is set, add "@" + <this> to user's login name if it doesn't
already contain "@" - optional
oracle.ocscclient.imap.defaultlogindomain=<YOUR.DOMAIN.COM>
```

- d. Set the domain name to use for outgoing user mail, if user names do not already include domain names (**Required**):

```
# If this is set, add "@" + <this> to user's login name if it doesn't
already contain "@" when
# setting from address on sent messages - mandatory
oracle.ocscclient.imap.defaultemaildomain=<YOUR.DOMAIN.COM>
```

- e. Set connect information to use to connect to any Oracle database which is storing Oracle Web Access Client user preferences (Optional):

```
# Connect information for an OCS database in which to store user IC
preferences - optional
oracle.ocscclient.db.icsys.pwd=<PASSWORD>
oracle.ocscclient.db.connstr=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=<DATA
BASE HOSTNAME>) (PORT=<DATABASE PORT>)) (CONNECT_
DATA=(SERVER=DEDICATED) (SERVICE_NAME=<DATABASE NAME>))
```

- f. Set connect information to an Oracle calendar server (Optional):

```
# Connect information for an Oracle calendar server - optional
oracle.ocscclient.calendar.sdk.ocalhost=x-oracle-calendar://collabsuite-cal.
oracle.com
oracle.ocscclient.calendar.sdk.ocasurl=http://collabsuite.oracle.com/ocas-bi
n/ocas.fcgi?sub=web
```

- g. Set connect and configuration information for LDAP directory cache support (Optional):

```
# Connect and config information for directory cache support - optional
oracle.ocs.ldappool.host=<LDAP SERVER>
oracle.ocs.ldappool.port=<LDAP SERVER PORT>
oracle.ocs.ldappool.user_dn=<USER DN TO USE WHEN LOGGING IN TO LDAP SERVER
TO SEARCH FOR USERS>
oracle.ocs.ldappool.user_password=<PASSWORD TO USE FOR PERFORMING USER
SEARCH>
oracle.ocscclient.directory.ldap.userSearchBase=<SEARCHBASE UNDER WHICH
USERS WILL BE FOUND>
```

3. Restart the OC4J_OCSCClient process to enable IMAP mode.

Corporate Directory Searches with Oracle Web Access Client

Some Oracle Internet Directory fields (such as `displayname`) are not indexed by default. Because of this, some Corporate Directory searches will appear to return no results in the Oracle Web Access client, or will cause errors. Affected attributes could include:

```
displayname
givenname
middlename
sn
title
departmentnumber
telephonenumber
homephone
facsimiletelephonenumber
mobile
pager
homepostaladdress
c
l
postalcode
st
```



```
street
mail
```

To find out which of these attributes is not being searched, try querying them with a tool such as `ldapsearch` and see which returns an error code 53.

You can either manually index the affected attributes so that they can be searched with the Oracle Web Access client, or silently exclude them from queries so that search errors will no longer occur. Oracle recommends indexing the attributes, since excluding them from searches may lead to confusion for users.

Manually Indexing an Attribute

Before you index attributes, you must shut down Oracle Internet Directory or set it to *Read Only* mode. See *Oracle Internet Directory Administrator's Guide* for more information.

Note: These steps are written with the understanding that the following environment variables are used:

- `ORACLE_HOME`: The Infra `ORACLE_HOME` path
 - `LD_LIBRARY_PATH`: This should include `$ORACLE_HOME/lib32:$ORACLE_HOME/lib`
 - `ORACLE_SID`: The SID of the Infrastructure Oracle Collaboration Suite Database
-

1. Change to the `/ldap/bin` directory as follows:

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

2. Index the attribute as follows:

```
./catalog.sh -connect $ORACLE_SID -add \
            -attr attribute_name
```

Where *attribute_name* is the attribute you want to index; for example, `displayname`.

3. Repeat the previous step for each attribute you want to index.
4. Open `oc4j.properties`; this file can be found at a location similar to the following:

```
$ORACLE_HOME/j2ee/OC4J_OCSCClient/config/oc4j.properties
```

5. For each attribute you indexed (as described in steps 2 and 3), update the appropriate entry in `oc4j.properties` as follows:

```
oracle.ocscclient.directory.capability.search.attr.attribute_name=enabled
```

Where *attribute_name* is the attribute you want to index; for example, `displayname`.

Excluding Attributes from Queries

To exclude attributes from queries, update the appropriate entry in `oc4j.properties` as follows:

```
oracle.ocscclient.directory.capability.search.attr.attribute_name=disabled
```

Where *attribute_name* is the attribute you want to exclude; for example, *displayname*.

Using an Alternate Search Base for Entries Returned by Oracle Web Access Client

On a default installation, web access is able to automatically determine the user and distribution list search base on startup. However, some systems may require a manual configuration of the search bases. There is a configuration for these special cases. In these cases, Oracle recommends that you also view the `objectclass` value for user and distribution list objects to make sure the default value is correct (See ["Placing Constraints on Directory Entries Returned by Oracle Web Access Client"](#) on page 5-58).

Indicators that this configuration might be necessary include:

- The OCS_client log files (in `ORACLE_HOME/ocscclient/log`) contain one of the following strings:

`"Unable to get the user search base from LDAP."`
`"Unable to get the DL search base from LDAP."`
- Users and/or distribution lists are never returned in Oracle Web Access Client searches. Be sure to confirm this by trying the 'All Internet Addresses' search in Oracle Web Access Client using the e-mail address of the user or distribution list.

To override the user and distribution list search bases:

```
# note that dlobjctandcondition and userobjctandcondition may have to be
# revised for such a configuration (see next section).
oracle.ocscclient.directory.ldap.userSearchBase=dc=<your_domain>,dc=com
oracle.ocscclient.directory.ldap.dlSearchBase=cn=dlcontainerOCS,dc=<your_
domain>,dc=com
```

Where `<your_domain>` is the user or distribution list base domain.

Placing Constraints on Directory Entries Returned by Oracle Web Access Client

The Oracle Web Access Client uses a connection pool that connects as the e-mail container entity (`cn=EmailServerContainer,cn=Products,cn=OracleContext`). This means that Corporate Directory queries executed in the Oracle Web Access Client may reveal entries that are normally hidden from end-users. Until this connection method is restructured, a special configuration has been provided so that administrators can define an 'AND' criteria restricting the LDAP objects that are returned. Whenever access controls are added to restrict the visibility of end-user directory data, Oracle Web Access Client administrators should consider overriding these values. (4495854)

Currently, there are only two types of objects returned by the Oracle Web Access Client Corporate Directory:

- Public Users
- Public Distribution Lists

There are two available configurations, one for each data type. They can be overridden in `oc4j.properties` (located in `ORACLE_HOME/j2ee/OC4J_OCSCClient`), and should be formatted as follows:

```
# <dl_condition> and <user_condition> should be replaced by
# RFC 2254-compliant query strings.
oracle.ocscclient.directory.ldap.dlobjctandcondition=dl_condition
oracle.ocscclient.directory.ldap.userobjctandcondition=user_condition
```

The default value of *dl_condition* is (objectclass=orclmailgroup) whereas the default value for *user_condition* is (objectclass=orclUserV2). The value of each of these and conditions determines the constraints that will be placed on each end-user query. When overriding this value, you must always include a condition that ensures a distinct objectclass for the two supported object types (usually composed of the defaults values above).

The following are examples of custom search constraints; notice that objectclass=*condition* is retained for all customized values.

```
# hide all users which have '_hidden@' as part of their e-mail address.
oracle.ocsclient.directory.ldap.userobjectandcondition=(&(objectclass=orclUserV2) (
!(mail=*_hidden*)) )

# hide all users that have been disabled in Oracle Internet Directory
oracle.ocsclient.directory.ldap.userobjectandcondition=(&(objectclass=orclUserV2) (
!(orclisenabled=DISABLED)))

# use an objectclass other than 'orclmailgroup' for DLs
# (to support older Oracle Internet Directory setups).
oracle.ocsclient.directory.ldap.dlobjectandcondition=(objectclass=mailgroups)
```

For more information on LDAP or LDAP query strings, see *Oracle Internet Directory Administrator's Guide*.

Managing Oracle Workspaces

Oracle Workspaces is an online application that enables groups of users to:

- Manage complex projects using workspace containers.
- Share, organize and collaborate on documents in a secure environment.
- Communicate easily and securely in a number of different ways: meetings, discussion forums and e-mail messages.
- Collaborate in real time through Web conferencing and instant messaging.
- Track the timeline and progress of a project using the workspace calendar and tasklist.
- Manage content access using workspace roles.

By assembling together relevant content for a project, including documents, tasks, meetings and forums, workspace members have a powerful framework within which they can organize their collaborative efforts. To assist users in managing this content, Oracle Workspaces uses a role-based access control model that provides read-only, write, or administrative access.

In addition, workspace administration is user-driven with minimal involvement by the global system administrator. Essentially, workspace creators are the workspace administrators, managing all workspace configuration issues such as membership and resource configuration directly. A user can create a workspace, add members with the appropriate roles, connect to all required services and start collaborating without the need for intervention by a system administrator.

See Also: For instructions on using all of the features of the Oracle Workspaces Web UI, see the Oracle Workspaces online help.

For instructions on sizing and tuning Oracle Workspaces, see "[Tuning Oracle Workspaces](#)" on page 10-15

This section contains the following topics:

- [Introduction to Oracle Workspaces](#)
- [Oracle Workspaces Access Control](#)
- [Oracle Workspaces Management Tasks](#)

Introduction to Oracle Workspaces

Oracle Workspaces provides a common interface for using other Oracle Collaboration Suite components (Oracle Mail, Oracle Content Services, Oracle Calendar, Oracle Messenger, Oracle Web Conferencing, and Oracle Discussions). It provides operations to help integrate these components, known as services (or resources), smoothly:

- Registration of newly deployed components to workspace applications.
For example, you might initially deploy Oracle Collaboration Suite with only Oracle Workspaces, Oracle Content Services, and Oracle Discussions. Later on, if you choose to deploy Oracle Calendar as well, users can immediately choose to add calendaring functionalities to existing and new workspaces with minimal configuration.
- Tolerance to component down time.
For example, if the Oracle Content Services server is unavailable because of scheduled downtime or unexpected server issues, Oracle Workspaces will continue to operate smoothly, with a message indicating that the Oracle Content Services resource is temporarily unavailable.

Oracle Workspaces content (files, meetings, discussions, and so on) is stored in each native application repository. For example, when a file is added to a workspace, it is stored in the Oracle Content Services repository.

Users can access Oracle Workspaces content using the Oracle Workspaces Web UI, or directly by using Oracle Collaboration Suite Web user interfaces (Oracle Discussions Web UI, Oracle Calendar Web client, and so on).

Privileges and roles are honored across the Oracle Collaboration Suite Web clients. For example, if a user has read-only access to a file through the Oracle Workspaces interface, they will also have read-only access through the Oracle Content Services interface.

See also: For more information on using Oracle Collaboration Suite Web clients to access Oracle Workspaces content, see [Table 5-12](#), "[Oracle Workspaces Support for Oracle Collaboration Suite Web Client Access](#)" on page 5-63

All user **authentication** and **authorization** is performed using Oracle Internet Directory.

Oracle Workspaces Access Control

There are two categories of roles used in Oracle Workspaces. The application level role applies to a user's privileges in the Oracle Workspaces system, defining the actions a user can perform at the application level. The workspace level role applies to a user's privileges within one workspace, defining the user's access to content within the workspace.

There are two application level roles:

- **Application Administrator:** Users granted this role can manage the entire Oracle Workspaces application. Some functions include granting/revoking application level roles, setting application level configuration properties and template management. Application Administrators can also perform any operation in any workspace; they can proxy as workspace administrators for any workspace.
- **Workspace Creator:** Users granted this role can create workspaces. If the workspace creation policy is Restricted, then only users with the Workspace Creator role can create workspaces. If the workspace creation policy is Public, then any user can create workspaces.

When Workspace Creators create workspaces, they are granted Workspace Administrator privileges for that workspace. Workspace Creators do not have Administrator privileges over workspaces which they did not create.

There are three workspace level roles:

- **Reader:** Users granted this role have read-only access to the workspace. They cannot add new content or edit existing content.
- **Writer:** Users granted this role have both read and write access to the workspace. They can create new folders, upload files, schedule meetings, create tasks, participate in discussions and manage relationships.
- **Administrator:** Users granted this role can do everything that workspace writers can do as well as manage workspace configuration and membership.

The following tables describe the possible roles a user may have and the corresponding actions permitted in Oracle Workspaces:

Table 5–5 Oracle Workspaces Workspace Management

Action	Workspace Reader	Workspace Writer	Workspace Administrator	Application Administrator	Workspace Creator
List my workspaces View workspace	Yes	Yes	Yes	Yes ¹	No
Customization of workspace	No	No	Yes	Yes ¹	No
Creation of root workspace	No	No	No	Yes ¹	Yes
Deletion of root workspace	No	No	Yes	Yes ¹	No
List all workspaces	No	No	No	Yes	No

¹ An Application Administrator can proxy as the workspace owner to perform this action

Table 5–6 Oracle Workspaces Membership Management

Action	Workspace Reader	Workspace Writer	Workspace Administrator	Application Administrator	Workspace Creator
Add, remove, and change workspace membership and roles	No	No	Yes	Yes ¹	No
List members of a workspace	Yes	Yes	Yes	Yes ¹	No
Retrieve membership information of a member					

¹ An Application Administrator can proxy as the workspace owner to perform this action

Table 5–7 Oracle Workspaces Template Management

Action	Workspace Reader	Workspace Writer	Workspace Administrator	Application Administrator	Workspace Creator
Generate a template from an existing workspace	No	No	Yes	Yes	No
Store/Delete templates in/from the repository	No	No	No	Yes	No
View and list templates	No	No	No	Yes	Yes

Table 5–8 Oracle Workspaces Application Management

Action	Workspace Reader	Workspace Writer	Workspace Administrator	Application Administrator	Workspace Creator
Change workspace application configuration and policy	No	No	No	Yes	No
Change owner of workspace	No	No	Yes	Yes	No

Table 5–9 Oracle Content Services Access in Oracle Workspaces

Action	Workspace Reader	Workspace Writer	Workspace Administrator	Application Administrator
Read a file	Yes	Yes	Yes	Yes ¹
Create a file or folder	No	Yes	Yes	Yes ¹
Delete or edit a file or folder	No	Yes	Yes	Yes ¹

¹ An Application Administrator can proxy as the workspace owner to perform this action

Table 5–10 Oracle Calendar Access in Oracle Workspaces

Action	Workspace Reader	Workspace Writer	Workspace Administrator	Application Administrator
Read meeting details	Yes.	Yes.	Yes	Yes ¹
Create a meeting	No	Yes	Yes	Yes ¹
Delete a meeting or edit meeting details	No	Yes	Yes	Yes ¹

¹ An Application Administrator can proxy as the workspace owner to perform this action

Table 5–11 Oracle Discussions Access in Oracle Workspaces

Action	Workspace Reader	Workspace Writer	Workspace Administrator	Application Administrator
Create a discussion board	No	Yes	Yes	Yes ¹
Create a discussion message	No	Yes	Yes	Yes ¹
Read a discussion message	Yes	Yes	Yes	Yes ¹
Delete discussion board	No	Yes.	Yes	Yes ¹

¹ An Application Administrator can proxy as the workspace owner to perform this action

[Table 5–12, "Oracle Workspaces Support for Oracle Collaboration Suite Web Client Access"](#) on page 5-63 shows how users can access various Oracle Workspaces contents using various clients of their choice, in addition to the Oracle Workspaces client.

Table 5–12 Oracle Workspaces Support for Oracle Collaboration Suite Web Client Access

Resource or Resource Item	Web Clients	Exposed as	Actions Supported
Document Library: Oracle Content Services files and folders	Oracle Content Services Web client WebDAV	A document library is seen as a Oracle Content Services shared folder identified by the workspace name under the path <code>/oracle/workspaces</code> .	All typical actions, including read, update, create, delete and version files and folders. It is possible to perform some actions that the Oracle Workspaces client would disallow. Oracle Workspaces makes a best effort to recover from them.
Oracle Discussions forums and messages	Oracle Discussions Web client	Workspace discussion forums are categorized in the Oracle Discussions application under the Facility <code>Workspaces.forums</code> . (Similarly, workspace Inboxes are categorized under the <code>Workspaces.inbox</code> facility). They are identified by the workspace name.	All typical message actions, including view, create, and reply messages. Creation and deletion of forums.
Oracle Discussions forums and messages	Oracle Mail IMAP mail clients	A workspace forum is seen as an IMAP shared folder under a shared folder with the same name of the workspace.	All typical message actions, including view, create, and reply messages.
Oracle Calendar meetings	Oracle Calendar Web client Oracle Connector for Outlook Oracle Calendar desktop client	Any Oracle Workspaces meetings that an individual is invited to are displayed in the user's personal calendar, along with the user's personal events and meetings.	View the details of the meetings.

Oracle Workspaces Management Tasks

Generally, Oracle Workspaces requires little administration, because individual users manage the configuration of their own workspaces.

You can monitor the performance and usage statistics of Oracle Workspaces from the Oracle Collaboration Suite Control.

As the Oracle Workspaces top-level administrator, you may need to perform one or more of the following tasks:

- Set application-level policies and properties:
 - Set the workspace creation policy to Restricted or Public.
If the workspace creation policy is set to Restricted, then only users with the Workspace Creator role can create new workspaces. If it is set to Public, than any Oracle Collaboration Suite user can create new workspaces.
- Manage connection information of the dependent Oracle Collaboration Suite components, such as the server of the Oracle Content Services application, SMTP server location, and so on.
- Set default user interface preferences.
- Set the default template to be used for workspace creation
- Enable and disable e-mail notification
- Set templates for e-mail notification messages

See the online help for instructions on performing all of the above tasks in Oracle Workspaces.

Adding Applications to your Oracle Collaboration Suite Deployment

You can configure any Oracle Collaboration Suite application which you have not already configured, at any time, to add it to your running Oracle Collaboration Suite deployment. For example, you might have selected only Oracle Mail and Oracle Content Services during installation, and now you would like to add Oracle Real-Time Collaboration to your deployment.

Note: Do not use the Deploy Ear File or Deploy War File options in Oracle Collaboration Suite Control to deploy a new J2EE application on your Oracle Collaboration Suite OC4J instances.

Deploying a new application could cause problems with the Oracle Collaboration Suite JVM or Oracle Collaboration Suite environment, including introducing incompatibility problems with the Oracle Collaboration Suite user applications.

To add an application to your Oracle Collaboration Suite deployment, you must first decide whether to configure the new application on an existing Applications tier, or to create a new Applications tier to host the new application. There are trade-offs for either of these options. For information about deployment scenarios and the trade-offs made, see the *Oracle Collaboration Suite Deployment Guide*

Configuring a New Application on a New Applications Tier

If you choose to create a new Applications tier, you can configure the new application by using the Oracle Collaboration Suite installation CD. Use the Oracle Universal

Installer to create a new Applications tier, and configure the desired applications on that tier. Provide the connection information for your Infrastructure tier(s) when prompted, and the new applications will be properly configured by the installer.

See also: *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows* for instructions on installing and configuring an Oracle Collaboration Suite Applications tier.

Configuring a New Application on an Existing Applications Tier

To configure a new application (one which you have not configured on any Applications tier in your deployment):

1. Open the Oracle Collaboration Suite Control Console and select the Applications tier on which you wish to configure the new application.
2. From the Applications tier home page, select **Configure Component**.
The Configure Component page displays the components which have not been configured on this Applications tier.
3. From the Components table, select the application you wish to configure, and select **Continue**.
4. Enter the connection passwords and other information requested by the Configuration Assistant. The information required differs for each Oracle Collaboration Suite application.
5. If you are configuring an application which affects an existing Oracle Calendar instance (such as Oracle Real-Time Collaboration, Oracle Mobile Collaboration, or Oracle Mail), you must restart the Oracle Calendar server in order to import new configuration information into unison.ini.
6. If you are configuring Oracle Application Server Portal using Oracle Enterprise Manager, you must perform some additional steps to complete the configuration. These are described in "Configuring OracleAS Portal After Installation" in *Oracle Application Server Administrator's Guide*.
7. You must restart the OC4J_OCSCClient and HTTP_Server processes. From the Oracle Collaboration Suite home page, select each of these processes and click **Start**.
8. After you configure an Oracle Collaboration Suite component using the Oracle Collaboration Suite Control, click the **Refresh Data** icon in the upper right corner of the Oracle Collaboration Suite home page. This causes the Administration URL for the configured component to appear in the Administration column of the System Components table.

When the configuration process is complete, you have finished adding the new application to your deployment.

Note: If you are setting up additional OracleAS Portal instances, you must perform additional steps after running the Configuration Assistant. See ["Configuring OracleAS Portal After Installation"](#) on page 5-42.

Managing Oracle Collaboration Suite Databases

This chapter describes how to manage the Oracle Collaboration Suite Database. Oracle Collaboration Suite uses one or more Oracle Database 10g databases to store messages, files, and other data for users.

Generally, a single Oracle Collaboration Suite Database resides on the same computer hosting the Infrastructure, in a separate Oracle Home. Other configuration options include separating the OracleAS Metadata Repository, the Oracle Internet Directory 10g, or application data into one or more distributed databases hosted on separate computers.

You should be sure you have a good understanding of the architecture of your specific Oracle Collaboration Suite deployment, so that you can apply a comprehensive database management methodology.

Note: In addition to the Oracle Collaboration Suite Database, Oracle Calendar uses its own separate database to store Calendar information. The Oracle Calendar database periodically synchronizes user information with the Oracle Internet Directory. You can force this synchronization using the UNIDSSYNC utility. See "UNIDSSYNC" in Chapter 6 of *Oracle Calendar Reference Manual*

For more information about maintaining the Oracle Calendar database, see "Server Maintenance Procedures" in Chapter 14 of *Oracle Calendar Administrator's Guide*

This chapter contains the following sections:

- [Administering Database Users](#)
- [Granting Database Control Administrative Privileges](#)
- [Setting Up Database Control Preferences](#)
- [SQL Statements and Other Management Tools: SQL*Plus and iSQL*Plus](#)
- [Starting and Stopping the Oracle Collaboration Suite Database](#)
- [Viewing Listener Configuration](#)
- [Managing Oracle Collaboration Suite Database Structures](#)
- [Viewing and Modifying Initialization Parameters](#)
- [Managing Memory Parameters](#)

- [Managing the OracleAS Metadata Repository](#)
- [Changing Oracle Collaboration Suite Schema Passwords](#)

Using the Oracle Enterprise Manager 10g Database Control Console

When you install Oracle Collaboration Suite, the Oracle Universal Installer also installs the Database Control Console. The Web-based Database Control serves as the primary tool for managing your Oracle database and sets a new standard in ease-of-use.

If you have installed and deployed Oracle Enterprise Manager 10g Grid Control, you can also use the Grid Control Console to manage the Oracle Collaboration Suite Database.

See Also: ["Using Grid Control to Manage Oracle Collaboration Suite"](#) on page 3-16

The following topics introduce you to the Database Control:

- [Database Management Features](#)
- [Database Control Console Online Help](#)
- [Database Control Console Navigational Features](#)

Database Management Features

From the Database Control Console, you can perform administrative tasks such as creating schema objects (tablespaces, tables, and indexes), managing user security, backing up and recovering your database, and importing and exporting data. You can also view performance and status information about your database instance.

Database Control Console Online Help

You can access context sensitive online Help by clicking **Help** displayed on every page. In addition to viewing the help specific to the task at hand, there is a **View Contents** link that takes you to top level Help where you can view a table of contents and link to topics. A search facility enables you to search the contents of Help.

Database Control Console Navigational Features

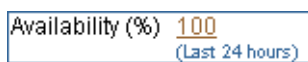
Navigational features of Oracle Enterprise Manager include the following:

- Property pages on each home page help you organize management tasks into distinct categories; for example, click Maintenance to perform tasks associated with backing up and maintaining your data.

Figure 6–1 Database Home Page Navigational Property Pages



- Drill down links that provide increasing levels of detail.

Figure 6–2 Database Home Page Drill Down Link

Clicking the 100 link shown in [Figure 6–2](#) provides additional levels of detail about the database’s availability.

- Suggested related links for more information.

Figure 6–3 Database Home Page Related Links

Related Links		
Advisor Central	Alert History	Alert Log Content
All Metrics	Blackouts	iSQL*Plus
Jobs	Manage Metrics	Metric Collection Errors
Monitoring Configuration		

Starting the Database Control Console

To access the Database Control Console from a client browser, the `dbconsole` process needs to be running on the server. This process is automatically started after installation.

However, if the process is not running because of a system restart or other event, you can manually start it at the command line.

To start the `dbconsole` process:

1. Navigate into your Oracle Collaboration Suite Database `$ORACLE_HOME/bin` directory
2. Run the following statement:

```
./emctl start dbconsole
```

Additionally, you can stop the process and view its status.

To stop the `dbconsole` process:

```
./emctl stop dbconsole
```

To view the status of the `dbconsole` process:

```
./emctl status dbconsole
```

Starting dbconsole in Windows

In Windows, in addition to using the command line, you can start the `dbconsole` process as a service.

To start `dbconsole` as a service:

1. Click Start->Control Panel->Administrative Tools->Services. The Services page appears.
2. Oracle services begin with **Oracle**. The `dbconsole` service is listed as **Oracle<oracle_home><SID>DBConsole**. The status of this process is listed in the Status column, either Started or Stopped. Double click the service. The property page appears.

3. In the properties page, ensure that the Startup Type is either Manual or Automatic and not Disabled. Click **Start**, if the process is not already started. Click **OK**.

You can also use the Services page to stop the process.

Accessing the Database Control Console

At the end of a successful database creation, Database Control is automatically launched and the database is started. At other times, provided the `dbconsole` process is running on the server, you can navigate to your Database Control from your client browser as follows:

1. Point your Web browser to the following URL:

```
http://hostname:portnumber/em
```

For example, if you installed the database on a host computer named `comp42`, and the installer indicated that your Database Control Console HTTP port number is 5500 (also recorded in the `$ORACLE_HOME/install/portlist.ini` file), enter the following URL:

```
http://comp42:5500/em
```

If the database is up, Enterprise Manager displays the Database Control Login page.

If the database is down and needs to be re-started, Enterprise Manager displays the Startup/Shutdown and Perform Recovery page. If this is the case, click Startup/Shutdown. You are then prompted for the host and target database login user names and passwords, which you must enter. For the database user and password, use `SYS` and the password you specified during installation.

Click **OK** to start the database. In the Confirmation screen, click **YES** to start the database in open mode.

2. Log in to the database using a username that is authorized to access the Database Control. This initially could be `SYS` or `SYSTEM`. Use the password you specified for the account during the database installation.

Enterprise Manager displays the Database Home page ([Figure 6-4](#)).

The property pages across the top of the page enable you to access performance, administration, and maintenance pages for managing your database. The functionality provided by these pages is discussed in other chapters of this book.

The various sections of the Database Home page, and related links, provide a wealth of information about the database's environment and health. For example, the **Alerts**, **Related Alerts**, and **Performance Analysis** sections warn you of errors and performance problems that are impacting the operation of your database. You can click the provided links to see more detail about the problem area, and even to obtain recommendations for resolving the problem. For more information, see [Chapter 10, "Monitoring and Tuning Oracle Collaboration Suite Performance"](#).

Figure 6–4 Database Home Page



Administering Database Users

To create new database users or administer existing ones select the **Administration** property page on the Database Home page (Figure 6–4, "Database Home Page").

From the Database Administration page, under the Security heading, click **Users**.

Security

Users

Roles

Profiles

The Users page shown in Figure 6–5, "Database Users Page" is displayed. From this page you can view, add, edit, or delete database users.

Figure 6–5 Database Users Page

ORACLE Enterprise Manager 10g Database Control

Setup Preferences Help Logout Database

Database: OCSM14DB.us.oracle.com > Users Logged in As SYS

Users

Search

Name

To run an exact match search or to run a case sensitive search, double quote the search criteria. The wildcard (%) symbol can still be used in a double quoted search string.

Results

Actions Create Like

Previous 1-25 of 64 Next 25

Select	UserName	Account Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	Created
☒	ANONYMOUS	EXPIRED & LOCKED	2005-06-09 12:47:19	SYSAUX	TEMP	DEFAULT	2005-05-15 02:22:06
☐	B2B	OPEN		B2B_RT	TEMP	DEFAULT	2005-06-03 03:22:38
☐	BAM	OPEN		USERS	TEMP	DEFAULT	2005-06-03 03:40:12
☐	CALENDAR	OPEN		USERS	TEMP	DEFAULT	2005-06-08 02:54:18
☐	CTXSYS	EXPIRED & LOCKED	2005-06-09 12:47:19	SYSAUX	TEMP	DEFAULT	2005-05-15 02:20:29
☐	CWSYS	OPEN		CWSYS_MAIN_TBS	CWSYS_TEMP_TBS	DEFAULT	2005-06-08 07:59:58

Creating Database Users

In this section, you create a user named MYUSER, set the password, and assign MYUSER to the USERS tablespace. This enables MYUSER to log in to the database

Later, you will learn how to edit and assign roles to this user.

To create a database user, do the following as user SYS or SYSTEM:

1. Click **Create** on the right hand side of the Users page. The Create Users General page shown in Figure 6–6 is displayed.

The General page is one of a series of pages in the Users property page.

Figure 6–6 Create User General Page

ORACLE Enterprise Manager 10g Database Control

Setup Preferences Help Logout

Database

Database: OCSM14DB.us.oracle.com > Users > Create User

Logged in As SYS

Create User

Show SQL Cancel OK

General Roles System Privileges Object Privileges Quotas Consumer Groups Proxy Users

* Name

Profile DEFAULT

Authentication Password

* Enter Password

* Confirm Password

☐ Expire Password now

Default Tablespace

Temporary Tablespace

Status ☐ Locked ☒ Unlocked

General Roles System Privileges Object Privileges Quotas Consumer Groups Proxy Users

Show SQL Cancel OK

Database | Setup | Preferences | Help | Logout

Copyright © 1996, 2005, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Database Control

2. Enter a user **Name**. For example: MYUSER
3. Leave Profile set to **DEFAULT**. The profile specifies the resource limit
Note that this profile does not allow the user to log in to Database Control. To do so, the user needs to be assigned the DBA role.
4. Leave Authentication set to **password**. For advanced authentication schemes, see *Oracle Database Security Guide*.
5. Enter the password of your choice in the **Enter Password** and **Confirm Password** boxes.
6. Do not check **Expire Password** now. If the account status is set to expired, then the user or the **Database Administrator** must change the password before the user can log in to the database.
7. For the **Default Tablespace** field, click the browse button (flashlight) and select the **USERS** tablespace. While users can specify different defaults for each user, it is easiest to define a default permanent tablespace and a default temporary tablespace at the database level, instead of the user level. For more information on the **USERS** tablespace, see "[Some Tablespaces in the Database](#)" on page 6-28.
8. For the **Temporary Tablespace** field, click the browse button (flashlight) and select the **TEMP** tablespace. For more information on the **TEMP** tablespace, see "[Some Tablespaces in the Database](#)" on page 6-28.
9. For **Status**, select **Unlocked**. Note that you can later lock an account to keep a user out of the database. Locking an account is preferable to deleting a user which deletes all associated tables and data.

10. Click **OK**. The Users page is displayed, and you can now see an entry for the new user, MYUSER.

The Users General page has links to several other property pages. For example, you can specify user roles, privileges, quotas, consumer groups, and proxy users. Consumer groups are groups of users, or sessions, that are grouped together based on their processing needs.

Note: This section creates a regular database user. If you want to grant the user system administrator privileges, you need to complete additional steps described in ["Granting Database Control Administrative Privileges"](#) on page 6-10

See Also: *Oracle Database Administrator's Guide* and *Oracle Database Security Guide* for more information on roles, privileges, quotas, consumer groups and proxy authentication

Using a Shortcut to Create Database Users

If you later want to create other database users similar to user MYUSER, or another existing database user, Oracle provides a shortcut for doing so. On the Users page, you can create a user with the same attributes as another user as follows:

1. Select the user that you want to duplicate.
2. From the Actions menu, select **Create Like**.
3. Click **Go**. The Create User General page appears for a new user with the same attributes as the duplicated user.

The **Actions** box also provides shortcuts for other actions, as well as providing a means to display the SQL DDL used to create a user.

Editing Database Users

You can change the attributes of database users by clicking **Edit** on the Users page (Figure 6-5, "Database Users Page") and selecting the properties page with the attributes that you want to change. The following procedure changes the tablespace quotas assigned to user MYUSER.

1. From the Users page, select MYUSER in the results list, then click **Edit**. The Edit User General page is displayed.
2. Click the Quotas property page to display the Quotas page.

You can see that this user has 0 MB quota on all tablespaces. This means that MYUSER has no quota in any tablespace. Since MYUSER belongs to the `users` tablespace, he must have quota to create tables and other schema objects in this tablespace.

3. In the Quota column for tablespace `users`, click the drop-down list and select **Value**.
4. In the corresponding **Value** column, enter 100.
5. Click **Apply**.

User MYUSER can now create objects in the `users` tablespace.

6. Click the **Database** property page to return to the Administration home page.

Unlocking Database Accounts and Resetting Passwords

Locked database accounts cannot be accessed by the database user. During installation, you can unlock and reset the Oracle supplied database user accounts. If you did not choose to unlock those accounts at that time, you can do so now as follows:

1. From the Users page shown in [Figure 6-5, "Database Users Page"](#), in the **Select** column of the table, mark a user whose **Account Status** is shown as `EXPIRED AND LOCKED` and that you want to unlock and reset.

2. From the pull down menu in the **Actions** pull-down menu, select **Unlock User** and click **Go**. Click **Yes** to confirm that you want to unlock the user.

This unlocks the user account (the **Account Status** is now `EXPIRED`), but does not reset the password. The user still is unable to log in to the database.

3. From the Users page, again mark the user in the **Select** column, then click **Edit**.

The Edit User General page is displayed. You can also display this page for a user by clicking the user name in the **UserName** column.

4. Use the General page to change the password for the account. Note that you can also use this page to unlock the account.

You must follow the preceding steps individually for each account that you want to unlock and reset.

Locking an account is similar. You select the user and then choose **Lock User** from the **Actions** pull-down menu. Locking an account denies access to the account.

To better understand the ramifications of unlocking and resetting accounts, see the other property pages available on the Edit user page. Specifically, explore the **Roles**, **System Privileges**, and **Object Privileges** property pages to see the privileges of the user whose account you are enabling.

Granting Database Roles

As a system administrator, you can use Database Control to grant roles to database users. For example, you can grant a user the DBA role, which allows the user to administer the database. You can also grant user-created roles.

To grant the DBA role to MYUSER:

1. From the Administration Page, under the Security heading, click **Users**.
2. From the list of users, select MYUSER and click **Edit**. The Edit User: MYUSER page appears.
3. In the top navigation bar, click **Roles**. A page appears with the list of roles for MYUSER.
4. Click **Modify** on the right hand side of the page. The Modify Roles page appears.
5. In the Available Roles list, select the DBA role and click **Move** to make it part of the Selected Roles list. You can also select the APDEV role you created earlier in this chapter.
6. Click **OK**. Then click **Apply**.

Revoking Database Roles

You can also revoke roles from database users. To revoke the DBA role from MYUSER:

1. From the Administration page, click **Users** under the Security heading.

2. From the list of users, select **MYUSER** and click **Edit**. The Edit User: MYUSER page appears.
3. In the top navigation bar, click **Roles**. A page appears with the list of roles for MYUSER.
4. Click **Modify** on the right hand side of the page. The Modify Roles page appears.
5. In the Available Roles list, select the **DBA** role and click **Remove** to make it part of the Available Roles list.
6. Click **OK**. Then click **Apply**.

Dropping Database Users

Database Control enables you to drop users. However, you must exercise caution when doing so, since dropping a database user will drop all schema objects owned by the user including tables and indexes. If you want to deny a database user access to the database, it is better to lock the user account or expire the user password.

To drop a database user such as MYUSER:

1. From the Administration page, under the Security heading, click **Users**.
2. Select the **MYUSER** user, and click **Delete**. At the confirmation page, click **Yes**.

Granting Database Control Administrative Privileges

When you log in to the Database Control Console using the **SYS** or **SYSTEM** user account, you are logging in as the Oracle Enterprise Manager super user. These are the only accounts that are automatically granted the roles and privileges required to access all the management functionality provided the Database Control.

To grant management access to other database users, use the following procedure:

1. Start your Web browser and log in to the Database Control as the **SYS** or **SYSTEM** database user.
2. Click **Setup** at the top of the Database Home page.
3. Click **Administrators** in the left navigation bar.

If you need to create a new administrator, you must first create the user and then assign administrative privileges as described in this section. To create a new user, see ["Administering Database Users"](#) on page 6-5.

4. Click **Create** to create a new Enterprise Manager user by assigning the management privileges to an existing database user.
5. Click the flashlight icon next to the Name field and select an existing database user from the pop-up window.
6. Enter the password for the selected user and click **Finish**.

Enterprise Manager assigns the management privileges to the selected user. The selected database user is now included in the list of management users on the Setup Administrators page. All the users shown on this page can log in to the Database Control and perform database management tasks.

Setting Up Database Control Preferences

Enterprise Manager enables you to set up preferences that help you manage the database. These include the following:

- **Notification**—These are settings that enable Oracle to e-mail you alert notifications. Alerts are notifications of when a database is in an undesirable state and needs your attention. By default, the Database Control Console home page lists all alerts. However, set up is required for e-mail notification. For more information about alerts and setting up notifications, see ["Setting up Notification"](#) on page 10-25.
- **Blackout Administration**—When you have planned downtime for database maintenance, you can indicate to Oracle that you do not want false alerts to be sent to you. To do so, you define a blackout period. See ["Defining Database Alert Blackout Time Periods"](#) on page 6-11.
- **Preferred Credentials**—Enterprise Manager can automatically execute many routine administrative tasks, such as backups, on your behalf. This is done using sophisticated job scheduling system built into the Enterprise. To keep your environment secure, setting up tasks for automatic execution in Enterprise Manager requires you to provide login information for the machine and database. To avoid having to enter this information every time you create a job or task, Enterprise Manager enables you to save this information as preferred credentials. Preferred credentials are stored in the database in encrypted mode to protect it from unauthorized use. See ["Setting Database Preferred Credentials"](#) on page 6-11.

Defining Database Alert Blackout Time Periods

When you plan to bring your database down for maintenance, you can indicate that you do not want alert notifications to be sent to you. Alerts are notifications of when the database is in an undesirable state and needs your attention. For more information about alerts, see ["Alerts"](#) on page 10-19.

To define a blackout time period, follow these steps

1. From the Database Control Console home page, click **Setup** at the top of the page. The Setup page appears.
2. Click **Blackouts** in the left hand pane. The Blackouts page appears.
3. Click **Create**. This starts the Create Blackout wizard. On the Properties page, name your blackout, and select the target that has planned downtime. Click **Next**.
4. On the Schedule page, enter the start time of your planned blackout, or choose immediately if you are bringing the database down now. Also select the duration of the blackout, either as indefinite, as a length or time, or until a time in the future. Under Repeating, accept the default of Do Not Repeat. If you want to repeat the blackout periodically, you can select a repeat frequency in the pull down menu. Click **Next**.
5. The review page appears. Review what you have entered, and if satisfied, click **Finish**. If not, you can click Back to change a setting.

Setting Database Preferred Credentials

You can have Enterprise Manager automatically fill in host and database login credentials for you, such as when you schedule jobs and tasks to perform administrative operations like backup and recovery. For security, Oracle stores preferred credentials in encrypted mode.

To set preferred credentials for the database, do the following:

1. From the home page, click **Preferences** at the top of the page. The Preferences page appears.

2. Click **Preferred Credentials** in the left hand pane. The Preferred Credentials page appears. For the Database target, click the icon under Set Credentials. The Database Preferred Credentials page appears.
3. For your database, enter the credentials for Normal Username/Password, SYSDBA Username/Password, and Host Username/Password.
4. Click **Test** to test your credentials. You should get a confirmation message if your credentials can be verified.
5. Click **Apply** to apply the changes.

SQL Statements and Other Management Tools: SQL*Plus and iSQL*Plus

Database Control is a Web-based graphical interface that enables you to perform management operations on the database like startup and shutdown, object creation, and schema management.

When you use Database Control to perform database management tasks, the underlying operations are performed using Structured Query Language (SQL) statements. SQL is an English-like computer programming language for accessing and manipulating data contained in a database. It is an industry-standard language for accessing databases, including those provided by vendors other than Oracle.

The following is an example of a SQL query:

```
SELECT COUNTRY_ID, COUNTRY_NAME FROM HR.COUNTRIES;
```

SQL is a powerful language and can be used to perform a variety of database administrative tasks. While performing these tasks, you can click Show SQL to see the underlying SQL statements being issued.

For more details on this language, see *Oracle Database SQL Reference*.

In addition to Database Control and Grid Control, you can use other Oracle tools to issue SQL statements such as SQL*Plus and its Web version iSQL*Plus. These tools enable you to perform the same database management operations, as well as to query, insert, update or delete data directly in the database.

Starting SQL*Plus

SQL*Plus is a command line program you use to issue SQL statements to an Oracle database. You can issue these statements interactively or in batch. SQL*Plus comes with your Oracle installation and is located in your Oracle Collaboration Suite Database \$ORACLE_HOME/bin directory.

To start SQL*Plus, enter the following at the command line on all platforms:

```
sqlplus username/password
```

You can use the SYS administrative user and password you set up during installation. SQL*Plus starts and connects you to the default database. At the SQL prompt, you can enter statements that perform administrative tasks such as database startup and shutdown. You can also query, insert, update and delete data.

On Windows, you can use the SQL*Plus Windows GUI. To start this, select Start->Programs->Oracle-OraHomeName->Application Development->SQL*Plus.

For more information about SQL*Plus, see *SQL*Plus User's Guide and Reference*.

For more information about SQL statements, see *Oracle Database SQL Reference*.

Starting iSQL*Plus

iSQL*Plus is the Web version of SQL*Plus. Before you can connect to it with a URL, you must start the iSQL*Plus application server. To do so, enter the following at the command line:

```
isqlplusctl start
```

After the server is started, you can connect to iSQL*Plus with a URL such as

```
http://machine_name:5560/isqlplus
```

Alternatively, you can connect to iSQL*Plus using Enterprise Manager. To do so from the home page, click **iSQL*Plus** under Related Links.

For more information about iSQL*Plus, see *SQL*Plus User's Guide and Reference*.

Starting and Stopping the Oracle Collaboration Suite Database

The Oracle Collaboration Suite Database must be running in order for Oracle Collaboration Suite to operate.

Many typical Oracle Collaboration Suite configurations include a single instance of the Collaboration Suite Database, installed on the Infrastructure tier. In these scenarios, you can start up and shut down the Collaboration Suite Database automatically when you start up or shut down the Infrastructure, by using an automatic script. The most simple method for starting the Collaboration Suite Database manually is also listed in the instructions for manually starting the Infrastructure.

See Also:

- To start the Infrastructure and Collaboration Suite Database by using a script, follow the instructions provided in "[Starting the Infrastructure Tier](#)" on page 2-4.
- To stop the Infrastructure and Collaboration Suite Database by using a script, follow the instructions provided in "[Stopping the Infrastructure Tier](#)" on page 2-6.

In other deployment scenarios, you may be hosting the Collaboration Suite Database on a separate computer, or you may have multiple instances of the Collaboration Suite Database. If you upgraded from a previous version of Oracle Collaboration Suite to Oracle Collaboration Suite 10g Release 1 (10.1.1), your OracleAS Metadata Repository may be in a separate database from the Collaboration Suite Database. In these scenarios, you will have to start and stop your database instances directly (or write a specialized script for your particular environment).

This section describes all of the options for manually starting and stopping the Collaboration Suite Database.

Note: You can also start and stop the Oracle Collaboration Suite Database using Database Control or Grid Control. For more information about using Database Control, see "[Using the Oracle Enterprise Manager 10g Database Control Console](#)" on page 6-2.

When you start up a database, you create an instance of that database and you determine the state of the database. Normally, you start up an instance by mounting and opening the database. Doing so makes the database available for any valid user to

connect to and perform typical data access operations. Other options exist, and these are also discussed in this section.

This section contains the following topics relating to starting up an instance of any Oracle Database 10g:

- [Options for Starting Up Oracle Collaboration Suite Database](#)
- [Preparing to Start an Oracle Collaboration Suite Database Instance](#)
- [Using SQL*Plus to Start Up an Oracle Collaboration Suite Database](#)
- [Scenarios for Starting a Oracle Collaboration Suite Database Instance](#)
- [Options for Shutting Down an Oracle Collaboration Suite Database](#)
- [Shutting Down an Oracle Collaboration Suite Database with the NORMAL Clause](#)
- [Shutting Down an Oracle Collaboration Suite Database with the IMMEDIATE Clause](#)
- [Shutting Down an Oracle Collaboration Suite Database with the TRANSACTIONAL Clause](#)
- [Shutting Down an Oracle Collaboration Suite Database with the ABORT Clause](#)

Options for Starting Up Oracle Collaboration Suite Database

You can start up and administer a database instance in several ways, as described in the sections that follow.

Starting Up a Database Using Grid Control

You can use Oracle Enterprise Manager Grid Control 10g (Grid Control) to administer your database, including starting it up and shutting it down. Grid Control is a separate Oracle product that combines a GUI console, agents, common services, and tools to provide an integrated and comprehensive systems management platform for managing Oracle products. Grid Control enables you to start a database using a GUI interface, rather than command line operations.

See Also:

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Managing Oracle Collaboration Suite*

Starting Up a Database using the Database Control Console

You can use the Database Control Console to administer your database, including starting it up and shutting it down. If you are using Grid Control, there is no need to also use Database Control (although you may do so if you want to). The Database Control Console allows you to use a graphical user interface (GUI) to manage the Oracle Collaboration Suite Database.

For more information about using Database Control, see "[Using the Oracle Enterprise Manager 10g Database Control Console](#)" on page 6-2

Starting Up a Database Using SQL*Plus

To start up a database using a SQL*Plus session, connect to Oracle Application Server 10g with administrator privileges, and then issue the `STARTUP` command. Using SQL*Plus in this way is the only method described in detail in this section.

Starting Up a Database Using Recovery Manager

You can also use Recovery Manager (RMAN) to execute `STARTUP` and `SHUTDOWN` commands. You may prefer to do this if you are within the RMAN environment and do not want to invoke SQL*Plus.

See Also: *Oracle Database Backup and Recovery Basics* for information on starting up the database using RMAN

Preparing to Start an Oracle Collaboration Suite Database Instance

You must perform some preliminary steps before attempting to start an instance of your database using SQL*Plus.

1. Start SQL*Plus without connecting to the database:

```
SQLPLUS /NOLOG
```

2. Connect to Oracle Collaboration Suite Database as SYSDBA:

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

Now you are connected to the database and ready to start up an instance of your database.

See Also: *SQL*Plus User's Guide and Reference* for descriptions and syntax for the `CONNECT`, `STARTUP`, and `SHUTDOWN` commands. These are SQL*Plus commands.

Using SQL*Plus to Start Up an Oracle Collaboration Suite Database

You use the SQL*Plus `STARTUP` command to start up a Oracle Collaboration Suite Database instance. To start an instance, the database must read instance configuration parameters (the initialization parameters) from either a server parameter file or a traditional text initialization parameter file.

When you issue the `STARTUP` command, by default, the database reads the initialization parameters from a server parameter file (`SPFILE`) in a platform-specific default location. When you install Oracle Collaboration Suite, the server parameter file is automatically created. If you wish to use a traditional text parameter file instead, you must specify the `PFILE` clause of the `STARTUP` command to identify the initialization parameter file.

Note: For UNIX, the platform-specific default location (directory) for the server parameter file (or text initialization parameter file) is:

```
ORACLE_HOME/dbs
```

For Windows the location is:

```
ORACLE_HOME\database
```

In the platform-specific default location, Oracle Database locates your initialization parameter file by examining filenames in the following order:

1. `spfile$ORACLE_SID.ora`
2. `spfile.ora`
3. `init$ORACLE_SID.ora`

Note: The `spfile.ora` file is included in this search path because in a Real Application Clusters environment one server parameter file is used to store the initialization parameter settings for all instances. There is no instance-specific location for storing a server parameter file.

For more information about the server parameter file for a Real Application Clusters environment, see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*.

You can direct the database to read initialization parameters from a traditional text initialization parameter file, by using the `PFILE` clause of the `STARTUP` command. For example:

```
STARTUP PFILE = /u01/oracle/dbs/init.ora
```

It is not usually necessary to start an instance with a non-default server parameter file. However, should such a need arise, you can use this `PFILE` clause to start an instance with a non-default server parameter file as follows:

1. Create a one-line text initialization parameter file that contains only the `SPFILE` parameter. The value of the parameter is the non-default server parameter file location.

For example, create a text initialization parameter file `/u01/oracle/dbs/spf_init.ora` that contains only the following parameter:

```
SPFILE = /u01/oracle/dbs/test_spfile.ora
```

Note: You cannot use the `IFILE` initialization parameter within a text initialization parameter file to point to a server parameter file. In this context, you must use the `SPFILE` initialization parameter.

2. Start up the instance pointing to this initialization parameter file.

```
STARTUP PFILE = /u01/oracle/dbs/spf_init.ora
```

The server parameter file must reside on the machine running the database server. Therefore, the preceding method also provides a means for a client machine to start a database that uses a server parameter file. It also eliminates the need for a client machine to maintain a client-side initialization parameter file. When the client machine reads the initialization parameter file containing the `SPFILE` parameter, it passes the value to the server where the specified server parameter file is read.

You can start an instance in various modes:

- Start the instance without mounting a database. This does not allow access to the database and usually would be done only for database creation or the re-creation of control files.

- Start the instance and mount the database, but leave it closed. This state allows for certain DBA activities, but does not allow general access to the database.
- Start the instance, and mount and open the database. This can be done in unrestricted mode, allowing access to all users, or in restricted mode, allowing access for database administrators only.

Note: You cannot start a database instance if you are connected to the database through a shared server process.

In addition, you can force the instance to start, or start the instance and have complete media recovery begin immediately. The `STARTUP` command clauses that you specify to achieve these states are described in "[Scenarios for Starting a Oracle Collaboration Suite Database Instance](#)" on page 6-17.

Scenarios for Starting a Oracle Collaboration Suite Database Instance

The following scenarios describe and illustrate the various states in which you can start up a Oracle Collaboration Suite Database instance. Some restrictions apply when combining clauses of the `STARTUP` command.

Note: It is possible to encounter problems starting up an instance if control files, database files, or redo log files are not available. If one or more of the files specified by the `CONTROL_FILES` initialization parameter does not exist or cannot be opened when you attempt to mount a database, Oracle Database returns a warning message and does not mount the database. If one or more of the datafiles or redo log files is not available or cannot be opened when attempting to open a database, the database returns a warning message and does not open the database.

See Also: *SQL*Plus User's Guide and Reference* for information about the restrictions that apply when combining clauses of the `STARTUP` command

Starting an Instance, and Mounting and Opening a Database

Normal database operation means that an instance is started and the database is mounted and open. This mode allows any valid user to connect to the database and perform typical data access operations.

Start an instance, read the initialization parameters from the default server parameter file location, and then mount and open the database by using the `STARTUP` command by itself (you can, of course, optionally specify the `PFILE` clause):

```
STARTUP
```

Starting an Instance Without Mounting a Database

You can start an instance without mounting a database. Typically, you do so only during database creation.

Note: Generally, you should use the Oracle Universal Installer from the Oracle Collaboration Suite CD to create Oracle Collaboration Suite Database instances, rather than creating them manually. The Oracle Universal Installer will create an Oracle Database instance, and seed it with all of the necessary Oracle Collaboration Suite schemas, automatically.

For more information about creating Oracle Collaboration Suite Database instances, see the *Oracle Collaboration Suite Installation Guide for Microsoft Windows* or *Oracle Collaboration Suite Installation Guide for Solaris Operating System*.

Use the `STARTUP` command with the `NOMOUNT` clause:

```
STARTUP NOMOUNT
```

Starting an Instance and Mounting a Database

You can start an instance and mount a database without opening it, allowing you to perform specific maintenance operations. For example, the database must be mounted but not open during the following tasks:

- Enabling and disabling redo log archiving options. For more information, see ["Redo Log Files"](#) on page 6-26
- Performing full database recovery. For more information, see *Oracle Database Backup and Recovery Basics*

Start an instance and mount the database, but leave it closed by using the `STARTUP` command with the `MOUNT` clause:

```
STARTUP MOUNT
```

Restricting Access to an Instance at Startup

You can start an instance, and optionally mount and open a database, in restricted mode so that the instance is available only to administrative personnel (not general database users). Use this mode of instance startup when you need to accomplish one of the following tasks:

- Perform an export or import of database data
- Perform a data load (with SQL*Loader)
- Temporarily prevent typical users from using data
- Perform certain migration and upgrade operations

Typically, all users with the `CREATE SESSION` system privilege can connect to an open database. Opening a database in restricted mode allows database access only to users with both the `CREATE SESSION` and `RESTRICTED SESSION` system privilege. Only database administrators should have the `RESTRICTED SESSION` system privilege. Further, when the instance is in restricted mode, a Database Administrator cannot access the instance remotely through an Oracle Net listener, but can only access the instance locally from the machine that the instance is running on.

Start an instance (and, optionally, mount and open the database) in restricted mode by using the `STARTUP` command with the `RESTRICT` clause:

```
STARTUP RESTRICT
```

Later, use the `ALTER SYSTEM` statement to disable the `RESTRICTED SESSION` feature:

```
ALTER SYSTEM DISABLE RESTRICTED SESSION;
```

If you open the database in nonrestricted mode and later find you need to restrict access, you can use the `ALTER SYSTEM` statement to do so, as described in ["Restricting Access to an Open Database"](#) on page 6-21.

See Also: *Oracle Database SQL Reference* for more information on the `ALTER SYSTEM` statement

Forcing an Instance to Start

In unusual circumstances, you might experience problems when attempting to start a database instance. You should not force a database to start unless you are faced with the following:

- You cannot shut down the current instance with the `SHUTDOWN NORMAL`, `SHUTDOWN IMMEDIATE`, or `SHUTDOWN TRANSACTIONAL` commands.
- You experience problems when starting an instance.

If one of these situations arises, you can usually solve the problem by starting a new instance (and optionally mounting and opening the database) using the `STARTUP` command with the `FORCE` clause:

```
STARTUP FORCE
```

If an instance is running, `STARTUP FORCE` shuts it down with mode `ABORT` before restarting it.

See Also: ["Shutting Down an Oracle Collaboration Suite Database with the ABORT Clause"](#) on page 6-23 to understand the side effects of aborting the current instance

Starting an Instance, Mounting a Database, and Starting Complete Media Recovery

If you know that media recovery is required, you can start an instance, mount a database to the instance, and have the recovery process automatically start by using the `STARTUP` command with the `RECOVER` clause:

```
STARTUP OPEN RECOVER
```

If you attempt to perform recovery when no recovery is required, Oracle Database issues an error message.

Automatic Database Startup at Operating System Start

Many sites use procedures to enable automatic startup of one or more Oracle Database instances immediately following a system start. The procedures for performing this task are specific to each operating system. For information about automatic startup, see your operating system specific Oracle documentation.

Starting Remote Instances

If your local Oracle Database server is part of a distributed database, you might want to start a remote instance and database. Procedures for starting and stopping remote instances vary widely depending on communication protocol and operating system.

Altering Oracle Collaboration Suite Database Availability

You can alter the availability of a database. You may want to do this in order to restrict access for maintenance reasons or to make the database read only. The following sections explain how to alter the availability of a database:

- [Mounting a Database to an Instance](#)
- [Opening a Closed Database](#)
- [Opening a Database in Read-Only Mode](#)
- [Restricting Access to an Open Database](#)

Mounting a Database to an Instance

When you need to perform specific administrative operations, the database must be started and mounted to an instance, but closed. You can achieve this scenario by starting the instance and mounting the database.

To mount a database to a previously started, but not opened instance, use the SQL statement `ALTER DATABASE` with the `MOUNT` clause as follows:

```
ALTER DATABASE MOUNT;
```

See Also: ["Starting an Instance and Mounting a Database"](#) on page 6-18 for a list of operations that require the database to be mounted and closed (and procedures to start an instance and mount a database in one step)

Opening a Closed Database

You can make a mounted but closed database available for general use by opening the database. To open a mounted database, use the `ALTER DATABASE` statement with the `OPEN` clause:

```
ALTER DATABASE OPEN;
```

After executing this statement, any valid Oracle9i Application Server user with the `CREATE SESSION` system privilege can connect to the database.

Opening a Database in Read-Only Mode

Opening a database in read-only mode enables you to query an open database while eliminating any potential for online data content changes. While opening a database in read-only mode guarantees that datafile and redo log files are not written to, it does not restrict database recovery or operations that change the state of the database without generating redo. For example, you can take datafiles offline or bring them online since these operations do not affect data content.

If a query against a database in read-only mode uses temporary tablespace, for example to do disk sorts, then the issuer of the query must have a locally managed tablespace assigned as the default temporary tablespace. Otherwise, the query will fail.

Ideally, you open a database in read-only mode when you alternate a standby database between read-only and recovery mode. Be aware that these are mutually exclusive modes.

The following statement opens a database in read-only mode:

```
ALTER DATABASE OPEN READ ONLY;
```

You can also open a database in read/write mode as follows:

```
ALTER DATABASE OPEN READ WRITE;
```

However, read/write is the default mode.

Note: You cannot use the RESETLOGS clause with a READ ONLY clause.

See Also: *Oracle Database SQL Reference* for more information about the ALTER DATABASE statement

Restricting Access to an Open Database

To place an instance in restricted mode, where only users with administrative privileges can access it, use the SQL statement ALTER SYSTEM with the ENABLE RESTRICTED SESSION clause. After placing an instance in restricted mode, you should consider killing all current user sessions before performing any administrative tasks.

To lift an instance from restricted mode, use ALTER SYSTEM with the DISABLE RESTRICTED SESSION clause.

See Also:

- *Oracle Database Administrator's Guide* for directions for killing user sessions
- ["Restricting Access to an Instance at Startup"](#) on page 6-18 to learn some reasons for placing an instance in restricted mode

Options for Shutting Down an Oracle Collaboration Suite Database

You can shut down an instance of your database in several ways, as described in the sections that follow.

Shutting Down a Database Using Grid Control

You can use Grid Control to administer your database, including starting it up and shutting it down. Grid Control is a separate Oracle product that combines a GUI console, agents, common services, and tools to provide an integrated and comprehensive systems management platform for managing Oracle products. Grid Control enables you to start a database using a GUI interface, rather than command line operations.

See Also:

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*

Shutting Down a Database using the Database Control Console

You can use the Database Control Console to administer your database, including starting it up and shutting it down. If you are using Grid Control, there is no need to also use Database Control (although you may do so if you want to). The Database Control Console allows you to use a GUID interface to manage the Oracle Collaboration Suite Database.

For more information about using Database Control, see ["Using the Oracle Enterprise Manager 10g Database Control Console"](#) on page 6-2

Shutting Down a Database Using Recovery Manager

You can also use Recovery Manager (RMAN) to execute `STARTUP` and `SHUTDOWN` commands. You may prefer to do this if you are within the RMAN environment and do not want to invoke SQL*Plus.

See Also: *Oracle Database Backup and Recovery Basics* for information on starting up the database using RMAN

Shutting Down a Database Using SQL*Plus

You can start a SQL*Plus session, connect to Oracle Database with administrator privileges, and then issue the `SHUTDOWN` command. Using SQL*Plus in this way is the only method described in detail in this section.

To initiate database shutdown, use the SQL*Plus `SHUTDOWN` command. Control is not returned to the session that initiates a database shutdown until shutdown is complete. Users who attempt connections while a shutdown is in progress receive a message like the following:

```
ORA-01090: shutdown in progress - connection is not permitted
```

Note: You cannot shut down a database if you are connected to the database through a shared server process.

To shut down a database and instance, you must first connect as `SYSOPER` or `SYSDBA`. There are several modes for shutting down a database. These are discussed in the following sections.

Shutting Down an Oracle Collaboration Suite Database with the NORMAL Clause

To shut down a database in normal situations, first connect as `SYSOPER` or `SYSDBA`. Then use the `SHUTDOWN` command with the `NORMAL` clause:

```
SHUTDOWN NORMAL
```

Normal database shutdown proceeds with the following conditions:

- No new connections are allowed after the statement is issued.
- Before the database is shut down, the database waits for all currently connected users to disconnect from the database.

The next startup of the database will not require any instance recovery procedures.

Shutting Down an Oracle Collaboration Suite Database with the IMMEDIATE Clause

Use immediate database shutdown only in the following situations:

- To initiate an automated and unattended backup
- When a power shutdown is going to occur soon
- When the database or one of its applications is functioning irregularly and you cannot contact users to ask them to log off or they are unable to log off

To shut down a database immediately, first connect as SYSOPER or SYSDBA. Then use the SHUTDOWN command with the IMMEDIATE clause:

```
SHUTDOWN IMMEDIATE
```

Immediate database shutdown proceeds with the following conditions:

- No new connections are allowed, nor are new transactions allowed to be started, after the statement is issued.
- Any uncommitted transactions are rolled back. (If long uncommitted transactions exist, this method of shutdown might not complete quickly, despite its name.)
- Oracle Database does not wait for users currently connected to the database to disconnect. The database implicitly rolls back active transactions and disconnects all connected users.

The next startup of the database will not require any instance recovery procedures.

Shutting Down an Oracle Collaboration Suite Database with the TRANSACTIONAL Clause

When you want to perform a planned shutdown of an instance while allowing active transactions to complete first, first connect as SYSOPER or SYSDBA. Then use the SHUTDOWN command with the TRANSACTIONAL clause:

```
SHUTDOWN TRANSACTIONAL
```

Transactional database shutdown proceeds with the following conditions:

- No new connections are allowed, nor are new transactions allowed to be started, after the statement is issued.
- After all transactions have completed, any client still connected to the instance is disconnected.
- At this point, the instance shuts down just as it would when a SHUTDOWN IMMEDIATE statement is submitted.

The next startup of the database will not require any instance recovery procedures.

A transactional shutdown prevents clients from losing work, and at the same time, does not require all users to log off.

Shutting Down an Oracle Collaboration Suite Database with the ABORT Clause

You can shut down a database instantaneously by aborting the database instance. If possible, perform this type of shutdown *only* in the following situations:

The database or one of its applications is functioning irregularly *and* none of the other types of shutdown works.

- You need to shut down the database instantaneously (for example, if you know a power shutdown is going to occur in one minute).
- You experience problems when starting a database instance.

When you must do a database shutdown by aborting transactions and user connections, first connect as SYSOPER or SYSDBA. Then issue the SHUTDOWN command with the ABORT clause:

```
SHUTDOWN ABORT
```

An aborted database shutdown proceeds with the following conditions:

- No new connections are allowed, nor are new transactions allowed to be started, after the statement is issued.
- Current client SQL statements being processed by Oracle Database are immediately terminated.
- Uncommitted transactions are not rolled back.
- Oracle Database does not wait for users currently connected to the database to disconnect. The database implicitly disconnects all connected users.

The next startup of the database *will* require instance recovery procedures.

Viewing Listener Configuration

The listener runs on your database server machine and brokers incoming client requests. With the Database Control Console, you can view the status of the listener.

To view the status of the listener, navigate to the Oracle Collaboration Suite Database home page. Under General, click **Listener**. The Listener: *listener_name* page appears. Under General, note the listener status, which is either Up or Down.

This page also gives the listener version, its net address, and start time.

You can additionally view the listener status at the command line using

```
lsnrctl status
```

Starting up and Shutting Down the Listener

You can start and stop the Oracle listener at the command line. To start the listener, use the following:

```
lsnrctl start
```

You can also stop it at the command line using the following:

```
lsnrctl stop
```

You can use the Database Control Console to stop the listener. To do so, navigate to the Listener: *listener_name* page by clicking **Listener** on the Oracle Collaboration Suite Database Home page. To shut down the listener, click **Stop**.

Managing Oracle Collaboration Suite Database Structures

This section discusses using the Database Control Console to explore and manage the storage structures of your database. This section contains the following topics:

- [Exploring the Storage Structure of Your Database](#)
- [Common DBA Tasks for Managing Database Storage](#)
- [Managing Undo for Your Database](#)

Exploring the Storage Structure of Your Database

An Oracle database is comprised of physical and logical structures, which you, as a DBA, are responsible for managing. Physical structures are those that can be seen and

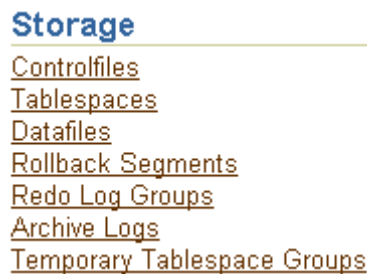
operated upon from the operating system, such as the physical files that store data on disk.

Logical structures are created and recognized by the Oracle database server, and are not known to the operating system. The primary logical structure in a database, a tablespace, contains physical files. The applications developer or end user may be aware of the logical structure, but is not usually aware of this physical structure. The DBA must understand the correlation between the physical and logical structures of a database and control the mapping of the logical structure of the database to the physical structure.

Oracle has functionality within the database server to automate the management of its structure. Further, the Database Control Console provides a Web-based graphical user interface to enable easy management and monitoring of your database.

You view database storage structure by clicking the links shown under the **Storage** heading on the Administration Home page (see [Figure 6–8, "Database Administration Page"](#) on page 6-37). [Figure 6–7, "Storage Options"](#) shows these links.

Figure 6–7 Storage Options



The following sections provide a closer look at the database storage structure:

Control File

A control file tracks the physical components of the database and other control information. It is essential to the functioning of the database. Because of this, Oracle recommends that the control file be multiplexed. In other words, it should have multiple identical copies. For databases created using DBCA, three copies of the control file are automatically created.

If any control file fails, then your database becomes unavailable. But as long as you still have any of the control file copies intact, you can shut down your database and re-create the failed control file from one of the other control files, then restart your database. Another option is to delete the failed control file from the `CONTROL_FILES` initialization parameter and restart your database with the remaining control files. There are other options, depending upon circumstances. See *Oracle Database Administrator's Guide* for detailed information about control files.

Click the **Controlfiles** link. The Controlfiles General page shows that your database has a multiplexed control file. There are two other property pages, in addition to the General page, for viewing control file information. The Advanced and Record Section pages give you more detailed information about your control file. Explanations of this information are contained in the online help.

Redo Log Files

Every Oracle database has a set of two or more redo log files. The set of redo log files is collectively known as the redo log for the database. A redo log is made up of redo entries (also called redo records). The primary function of the redo log is to record all changes made to data. If a failure prevents modified data from being permanently written to the datafiles, then the changes can be obtained from the redo log, so work is never lost. To protect against a failure involving the redo log itself, Oracle allows a multiplexed redo log so that two or more copies of the redo log can be maintained on different disks.

Your database's redo log consists of groups of redo log files. A group consists of a redo log file, and its multiplexed copies. Each identical copy is said to be a member of that group, and each group is defined by a number, such as group 1. The database log writer process writes redo records from the memory buffer to a redo log group until the group fills up, or a log switch operation is requested, then it writes to the next group. This is done in a circular fashion, where the oldest group is overwritten by the most recent redo records.

Click **Redo Log Groups**. The Redo Log Groups page appears, showing the attributes of the redo log groups for your database. A database typically consists of three groups. Note the status attribute for the redo log groups. The `CURRENT` status group is the one currently being written to disk by the log writer process.

You can see that each group contains only one member. This is because the database does not have a multiplexed redo log. Select a redo log group and click **View** to see information about the redo log group members.

Multiplexing the Redo Log While not multiplexing redo log groups is acceptable in a small database environment, you should consider adding multiplexing as your database grows in users and applications. This provides better protection for data in the case of instance or media failure.

To multiplex your redo log, you must add members to each redo log group. This example will add one member to each redo log group. It is not required that redo log groups be symmetrical (all have the same number of members), but in practice it is recommended that this be the case. It *is* required that a database have a minimum of two redo log groups.

To create a multiplexed redo log for your database, follow these steps:

1. Navigate to the Redo Log Groups page.
2. Select a group and click **Edit**, or click the group number link.

The Edit Redo Log Group page appears.

3. In the **Redo Log Members** section, click **Add**.

The Add Redo Log Member page appears.

4. Enter the file name. For example, if your existing member file name is `REDO01`, you might name this member `REDO01a`. Enter the file directory. Click **OK**.

You can create this file in the same directory, but it is recommended that you store members on separate drives. That way, if there is a drive failure, you still have access to one member.

5. Repeat these steps for every existing group.

When you add the redo log member to a group, the group's status is marked `INVALID`. This is a normal state because there is a member that has not been written to

yet. When a log switch occurs, and the invalid group becomes the current group, then its status is marked `CURRENT`.

To see the status change on a log switch:

1. Navigate to the Redo Log Groups page.
2. From the Actions pull down menu, select **Switch logfile**. Click **Go**.

You can see that the next groups status changes from `INVALID` to `CURRENT`.

Archive Log Files

When you archive your redo log, you write redo log files to another medium location prior to their being overwritten. This location is called the archive log. You can archive to multiple locations, including a standby database.

These copies of redo log files extend the amount of redo information that can be saved and used for recovery. Archiving can be either enabled or disabled for the database, but Oracle recommends you enable archiving. The status of a log group that is actively being archived is `ACTIVE`.

Click **Archive Logs**. The Archive Logs page is displayed. This page lets you view archive log files and their attributes.

For placing the database into archive log mode, or adding archive log locations, see [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#).

Rollback Segments

In earlier releases of the Oracle database, rollback segments were database structures used to track undo information for the database. Now, Oracle's preferred way of managing undo is with the undo tablespace. For more information, see ["Managing Undo for Your Database"](#) on page 6-32.

Click **Rollback Segments**. You see the attributes of the system rollback segment. The system rollback segment is self managing.

Tablespaces

A database consists of one or more tablespaces. A tablespace is a logical structure, or container, created by and known only to the Oracle database server in which database objects are stored. A tablespace consists of one or more datafiles or tempfiles.

There are various types of tablespaces, including undo tablespaces, temporary tablespaces, and permanent tablespaces.

A database running in automatic undo management mode transparently creates and manages undo segments. You can create an undo tablespace and determine the maximum retention time for undo data kept in that tablespace.

Temporary tablespaces improve the concurrence of multiple sort operations, reduce their overhead, or avoid Oracle space management operations altogether. Temporary tablespaces are the most efficient tablespaces for disk sorts. Space management (extent allocation and deallocation) is locally managed.

After temporary tablespaces, tablespaces of type `TEMPORARY` are the next best tablespaces to use for sort operations. Space management is dictionary managed. Permanent tablespaces (which are not of type `TEMPORARY`) are least efficient for performance of disk sorts.

See Also: *Oracle Database Administrator's Guide*

Tablespaces Page Click **Tablespaces**. The Tablespaces page provides high level information about tablespace structure and space usage. You can see how much space is allocated for the tablespace and what portion of it is used. Select a tablespace and click **View** to see the underlying datafile attributes.

Some Tablespaces in the Database [Table 6–1, "Tablespaces and Descriptions"](#) provides a description some of the tablespaces included in the database.

Table 6–1 Tablespaces and Descriptions

Tablespace	Description
SYSAUX	This is an auxiliary tablespace to the <code>SYSTEM</code> tablespace. Some components and products that prior to Oracle Database 10g used the <code>SYSTEM</code> tablespace or their own tablespaces now use the <code>SYSAUX</code> tablespace. This reduces the load on the <code>SYSTEM</code> tablespace and reduces maintenance because there are fewer tablespaces to monitor and maintain. Every Oracle Database 10g or higher level database must have a <code>SYSAUX</code> tablespace. Components that use this as their default tablespace during installation include Automatic Workload Repository, Oracle Streams, Oracle Text, and Enterprise Manager Repository. For more information, see the <i>Oracle Database Administrator's Guide</i>.
SYSTEM	The <code>SYSTEM</code> tablespace is always created at database creation. Oracle uses it to manage the database. It contains the data dictionary, which is the central set of tables and views used as a read-only reference for a particular database. It also contains various tables and views that contain administrative information about the database. These are all contained in the <code>SYS</code> schema, and can only be accessed by user <code>SYS</code> or other administrative users with the required privilege.
TEMP	This tablespace stores temporary data generated when processing SQL statements. It would, for example, be used for sort work space. Every database should have a temporary tablespace that is assigned to users as their temporary tablespace. In the preconfigured database, the <code>TEMP</code> tablespace is specified as the default temporary tablespace. This means that if no temporary tablespace is specified when a user account is created, then Oracle assigns this tablespace to the user.
UNDOTBS1	This is the undo tablespace used by the database server to store undo information. See "Managing Undo for Your Database" on page 6-32 to understand Oracle's use of the undo tablespace. Every database must have an undo tablespace that can be created at database creation.
EXAMPLE	This tablespace contains the sample schemas that Oracle includes with the database. The sample schemas provide a common platform for examples. Oracle documentation and educational materials contain examples based on the sample schemas.
USERS	This tablespace is used to store permanent user objects and data. Like the <code>TEMP</code> tablespace, every database should have a tablespace for permanent user data that is assigned to users. Otherwise, their objects will be created in the <code>SYSTEM</code> tablespace, and this is not good practice. In the preconfigured database, <code>USERS</code> is assigned the default tablespace, and space for all objects created by non-system users comes from this tablespace. For system users, the default permanent tablespace remains <code>SYSTEM</code>.

Temporary Tablespace Groups Temporary tablespace groups let users consume temporary space from multiple tablespaces. Using a tablespace group, rather than a single temporary tablespace, can alleviate problems caused when one tablespace is inadequate to hold the results of a sort, particularly on a table that has many partitions. A tablespace group enables parallel execution servers in a single parallel operation to use multiple temporary tablespaces.

You can assign a tablespace group name as a default temporary tablespace for the database or as a temporary tablespace for a user.

Click the **Temporary Tablespace Groups** link. You see the temporary tablespace groups that are defined for your database. Initially, there are none.

See Also: *Oracle Database Administrator's Guide* for details on using tablespace groups

Datafiles

Datafiles are the operating system files that hold the data within the database. The data is written to these files in an Oracle proprietary format that cannot be read by programs other than the database server. Tempfiles are a special class of datafiles that are associated only with temporary tablespaces.

Datafiles can be broken down into the following components:

- Segments and extents

A segment contains a specific type of database object. For example, tables are stored in data segments, and indexes are stored in index segments.

An extent is a contiguous set of data blocks within a segment. Oracle initially allocates an extent of a specified size for a segment, but if that extent fills, then more extents can be allocated.

- Data block

Data blocks, also called database blocks, are the smallest unit of I/O to database storage. An extent consists of several contiguous data blocks. The default database block size is specified by a DBA at database creation or defaulted by Oracle.

After the database has been created, it is not possible to change the default block size without re-creating the database. However, it is possible to create tablespace with a block size different than the default block size. For details on how to create tablespaces with non-default (or non-standard) block size, see *Oracle Database Administrator's Guide*.

To view more information about your database datafiles, click **Datafiles**. Your database datafiles are displayed. Select a datafile and click **View** to see more attributes for the datafile, or select a tablespace link to see the attributes of the owning tablespace.

Other Storage Structures

Other storage structures that can exist in an Oracle database include the following:

Initialization Parameter File Initialization parameters are used by the database server at startup to determine the runtime resources for the database. They are actively monitored by the database and can be set or modified while the database is running.

Initialization parameters and the initialization parameter file are discussed in "[Viewing and Modifying Initialization Parameters](#)" on page 6-36.

Password File A database might use a password file to authenticate administrative users who can have SYSDBA connect privileges. SYSDBA connect privileges enable a DBA to start up and shut down the database and perform other high level administrative tasks. This password file is outside of the database itself, because it must sometimes be referenced when the database is not yet running.

This is not the only form of administrator authentication, so not all databases require a password file.

Backup Files Backup files are technically not database files, but rather copies of the database in some form that can be used to recover the database should a failure causing loss of data occur.

Backup files are discussed in [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#).

Common DBA Tasks for Managing Database Storage

The remainder of this section presents examples of some common database administration tasks relating to the storage structure:

- [Viewing Tablespaces in Your Database](#)
- [Modifying a Tablespace](#)
- [Dropping a Tablespace](#)
- [Reclaiming Wasted Space](#)

Viewing Tablespaces in Your Database

You can see all tablespaces in your database. From the Database Control Console Administration page, click **Tablespaces** under Storage. This takes you to the Tablespaces page.

The Results page shows all tablespaces, including the following information about each: type of tablespace, type of extent management, type of segment management, status, size, and percent used. Click the tablespace name for more information.

Modifying a Tablespace

With Database Control Console, you can modify a tablespace, such as extend it, set it to automatically extend, change its space thresholds, or change its status to offline. A tablespace might need extending when you get a critical and warning alert. You might need to offline a tablespace to perform recovery operations on it.

This section shows you how to set a tablespace to automatically extend when it reaches its limit. To enable autoextend tablespace, do the following:

1. From the Database Control Console Administration page, click **Tablespaces** under Storage. This takes you to the Tablespaces page.
2. Select a tablespace to autoextend, such as `USERS`, and click **Edit**. The Edit Tablespace:USERS General property page appears.
3. Select the datafile associated with the tablespace, and click **Edit**. The Edit Datafile page appears.
4. Check **Automatically extend datafile when full (AUTOEXTEND)**. Set a suitable increment, such as 1 M. You can optionally set a maximum file size or set file size to unlimited depending on your resources.

You can use SQL statements to add datafiles and associate them with a tablespace. You can either specify the file specifications for the datafiles being created, or you can use the Oracle Managed Files feature to create files that are managed by the database server.

You can also use SQL statements to manually resize a datafile. This lets you add space to your database without adding datafiles, if you are concerned about reaching the maximum number of datafiles allowed in your database. Manually reducing the sizes of datafiles lets you reclaim unused space in the database. This is useful for correcting errors in estimates of space requirements. For more information on managing datafiles, see the *Oracle Database Administrator's Guide*.

5. Click **Continue**. This brings you back to the Edit Tablespace page. Click **Apply**. A confirmation message appears.

Similarly, you can change tablespace thresholds by selecting a tablespace on the Tablespaces page and navigating to the Threshold property page. Here you can alter your space thresholds that generate the warning and critical alerts. For more information about thresholds and alerts, see [Chapter 10, "Monitoring and Tuning Oracle Collaboration Suite Performance"](#).

To take a tablespace offline, on the Edit Tablespace page, under Status, select **Offline** and click **Apply**.

Dropping a Tablespace

After a tablespace has been dropped, the objects and data in it will no longer be available. To recover them can be a time consuming process. Oracle recommends performing a backup before and after dropping a tablespace. Oracle Collaboration Suite applications will stop functioning properly if any of their required tablespaces have been dropped.

1. From the Administration page, click **Tablespaces** under Storage. This takes you to the Tablespaces page.
2. Select the tablespace that you want to drop, and click **Delete**. Enterprise Manager will ask for confirmation that you want to delete the tablespace and associated datafiles from the operating system.

Reclaiming Wasted Space

Over time, inserts, updates, and deletes (DML operations) to objects within a tablespace can create pockets of empty space that individually are not big enough to be reused. Collectively these pockets can constitute large amounts of wasted space.

Oracle lets you reclaim wasted space through a shrink operation. In a shrink operation, data is compacted to the front of the table. Free space can either be given back to the tablespace or kept in the table for future inserts. A shrink operation on a table does not affect DML operations to the table during the operation.

Using the Segment Advisor The Segment Advisor performs growth trend analysis on individual objects to determine if there will be any additional space left in the object in 7 days. It then uses the reclaim space target to select candidate objects to shrink. The Segment Advisor can be invoked in the comprehensive mode. In this mode, in addition to using the pre-computed statistics in the workload repository, the Segment Advisor samples the objects under consideration to refine the statistics for the objects. Although this operation is more resource intensive, it may be used to perform a more accurate analysis, when desired.

You can run the advisor at the tablespace or object level. To run the advisor from the tablespace level do the following:

1. From the Database Control Console Administration page under Storage, click **Tablespaces**. This takes you to the Tablespaces page.
2. On the Tablespaces page, select a tablespace and select **Run Segment Advisor** from the Actions menu. Note the used space before the operation for later comparison. Click **Go**. Note that the Segment Advisor can also be launched from the Advisor Central page.
3. The Segment Advisor: Advisor Mode page appears. On this page, accept the default **Complete Analysis of All Segments (Comprehensive)** mode. Click **Continue**.
4. The Segment Advisor: Options page appears. Accept **Unlimited** as the time limit for Analysis. Click **Next**.
5. The Segment Advisor: Schedule page appears. Select Standard as the Schedule Type and accept **Immediately** as the Start time. Otherwise, you can schedule the task to run later. Click **Next**.
6. The Segment Advisor: Review page appears summarizing the task and selected objects. Verify that the task will run as you want, and click **Submit**.
7. The Advisor Central page appears listing the advisor related tasks that have run. Select the Segment Advisor task that you submitted, and click **View Result**.
8. The Segment Advisor Task page appears showing the recommendations for the selected table. To implement one or more recommendations, select the recommendations to implement. This will launch the shrink wizard, which is described in the following section.

Shrinking Database Objects Over time, it is common for segment space to become fragmented or for a segment to acquire a lot of free space as the result of update and delete operations. The resulting sparsely populated objects can suffer performance degradation during queries and DML operations.

The Segment Advisor provides advice on whether an object has space available for reclamation based on the level of space fragmentation within an object.

1. Select **Shrink Options** at the bottom of the page. You can choose to Compact Segments and Release Space, which releases freed space to the tablespace, or you can Compact Segments only. Click **Schedule Implementation** to run the shrink operation.
2. The Schedule Implementation page appears. Accept a start time of **Immediately**, and click **Submit**.
3. The scheduler Jobs page appears showing the status of the job. Click **Refresh** to update the page until the status of the job is Completed. On successful completion, you can navigate back to the Tablespace page and compare the current used space with the previous.

Managing Undo for Your Database

This section discusses undo management which involves storing the changes of database transactions long enough to accommodate rollback, read consistency, and flashback features.

When you install the database, Oracle automatically enables auto-tuning of the undo retention period. (This parameter is discussed in ["Undo Tablespace Size and Retention"](#))

[Time"](#) on page 6-33.) Auto-tuning of undo retention enables you to start running Oracle Collaboration Suite without immediately managing undo. Later, as your database activity and transaction rate increase, understanding how to manage undo will become more useful to you.

About Undo

Undo data stores changes made to the database by transactions. Undo is necessary for the following:

- To undo any uncommitted changes made to the database in the event that a rollback operation is necessary. A rollback operation can be the result of a user (application) specifically issuing a rollback statement to undo the changes of a misguided or unintentional transaction, or it can be part of a recovery operation.
- To provide read consistency. This means that each user can get a consistent view of data, even while other uncommitted changes may be occurring against the data. For example, if a user issues a query at 10:00 a.m. and the query lasts for 15 minutes, the query results should reflect the entire state of the data at 10:00 a.m. regardless of any updates or inserts by other users during the 15 minute query.
- To enable Oracle's flashback features, which enables you to view or recover data to a previous point in time. These features include Flashback Query and Flashback Table.

See Also: "Recovering Messages with Oracle Flashback Query" in Chapter 10 of *Oracle Mail Administrator's Guide*

Undo Tablespace Size and Retention Time

In order for changes to be rolled back or undone, Oracle makes a copy of the original data before modifying it. The original copy of the modified data is called undo data. Undo data is stored in a logical database structure called an undo tablespace.

The undo tablespace is of a finite size. Space usage within the tablespace is such that records can be overwritten. The undo data needs to be saved at least until the transaction has been committed. Until then the undo data is said to be in the active state. The amount of space available in the undo tablespace should, therefore, be at least large enough to hold the active undo data generated by currently active transactions. Otherwise some of these transactions may fail. After the active undo data is stored in the undo tablespace, Oracle automatically ensures that it is never overwritten until the corresponding transaction has been committed.

Even after the transaction has been committed, the undo data still cannot be overwritten immediately. It is important to the success of flashback functionality, and for read consistency for long running transactions, that records not be overwritten too soon. For example, if your longest query takes 15 minutes, the undo tablespace should be big enough to hold 15 minutes worth of undo information.

To control the retention of undo records, Oracle maintains an undo retention period, which in turn affects the size of the undo tablespace; the longer the retention period, the bigger the tablespace. The undo retention period should be at least as long as your longest running query. In addition, if you plan to use flashback features to recover from human errors such as unintentional changes, the undo retention should be set equal to the amount of time in the past you want to go back. For more details on Flashback features, see *Oracle Database Administrator's Guide*.

Automatic Undo Management

Oracle Database automatically determines how long undo data should be preserved after the transaction has been committed based on queries running against the database. During this time, the undo data is said to be in the unexpired state. Oracle will keep the undo data in the unexpired state as long as needed by queries currently running against the database or as long as any low undo retention threshold (whichever is longer). After this time, the state of undo data changes to expired. Undo data is a good candidate for overwriting only when it is in the expired state.

If the undo tablespace does not have adequate free or expired space to store active undo data generated by current transactions, Oracle may be forced to overwrite the unexpired undo data. As this may cause your queries to fail, this is not a desirable situation. In order to avoid this, Oracle recommends you allow the size of the undo tablespace to be automatically increased by enabling auto-extend. See ["Extending the Undo Tablespace"](#) on page 6-35.

If you cannot enable auto extension for any reason and choose to adjust the size of the undo tablespace manually, Oracle Database includes an undo advisor to help you determine the optimal size. See ["Using the Undo Advisor"](#) on page 6-35.

Undo Management with Database Control

With Database Control, you can access the Undo Management page from the database Administration page by selecting **Undo Management** under the **Instance** heading.

You can use the Undo Management page to view undo configuration, including the auto-tuned undo retention period, the low threshold retention period, and the name and size of the undo tablespace. Auto-tuning of undo retention cannot be disabled.

You can also use this page to set the low threshold retention or to extend your tablespace. While Oracle automatically tunes the undo retention period, low threshold undo retention lets you define the floor value under which Oracle should never bring down the undo retention. When Oracle Collaboration Suite Database is installed, the low threshold undo retention is set to a default value. You may need to alter this value only when you need to build a recovery strategy using Flashback Query.

To change the low threshold, click its value. The Undo Advisor page appears, which can help you determine a better setting. See ["Using the Undo Advisor"](#) on page 6-35 for more information.

The Configuration section also shows if auto-extending the tablespace is enabled, which is the default. When auto-extend tablespace is enabled, Oracle automatically increases the size of the undo tablespace when more space is needed. By combining automatic extension of the undo tablespace with automatically tuned undo retention, you can ensure that long-running queries will succeed by guaranteeing the undo required for such queries.

The methods for determining the undo retention period are described in the following sections:

- [Using Oracle Recommendations for Managing Undo](#)
- [Using the Undo Advisor](#)

See Also: *Oracle Database Administrator's Guide* for more information about Automatic Undo Management and undo tablespaces.

Using Oracle Recommendations for Managing Undo

In the **Recommendations** section of the Undo Management page, you can specify a past time period for Oracle to analyze system activity. The current recommendations for your undo configuration are summarized. To update the analysis, click **Update Analysis**.

If Oracle recommends that you extend the undo tablespace, you can do so. See ["Extending the Undo Tablespace"](#) on page 6-35 for more information.

To obtain more detailed information about the recommendations, click **Undo Advisor**. See also ["Using the Undo Advisor"](#) on page 6-35.

Extending the Undo Tablespace When auto-extend tablespace is enabled, the system will automatically extend the undo tablespace if it is under space pressure.

However, when the auto-extend tablespace feature is disabled, you might need to manually extend the undo tablespace. You might discover this ahead of time while planning with the Undo Advisor. See ["Using the Undo Advisor"](#) on page 6-35.

You might also need to extend the undo tablespace when you get an undo tablespace alert (warning or critical), or when you get "query too long" alert or "snapshot too old" error.

To resize the tablespace, click **Edit Undo Tablespace**. The Edit Tablespace page appears. To extend the tablespace, select a datafile and click **Edit**. Enter the new size in the File Size field. You can also opt to have the system automatically extend the datafile by enabling **Automatically extend datafile when full** under Storage and specifying an increment size.

Click **Continue**. Click **Apply**. A confirmation message should appear.

Using the Undo Advisor

You can use the undo advisor to advise on the undo tablespace size and the low threshold undo retention setting. To navigate to the Undo Advisor page, navigate to the Undo Management page and do one of the following:

- Click **Undo Advisor**.
- Click the value adjacent to **Low Threshold Undo Retention**.

The top of the page shows the current auto-tuned undo retention time and undo tablespace size.

The Undo Advisor helps you answer the following questions about your undo configuration:

1. **What is the maximum undo retention time required to guarantee successful query?** This time period corresponds to the duration of your longest running query. You can find **Longest Running Query** on the Undo Management page under System Activity and Tablespace Usage.
2. **Does my database have enough space to accommodate the maximum undo retention given the current tablespace configuration?** To figure this out, note the **Best Possible Undo Retention** under analysis on the Undo Advisor page. If this time period is longer than your longest running query, your undo tablespace is adequately configured.
3. **What if the best possible retention time is less than my longest running query?** If this is the case, your undo tablespace is too small. You need to either set your tablespace to auto-extend or manually extend it. To figure out the required new size of your tablespace, on the Undo Advisor page **New Undo Retention** field,

plug in the value of your longest running query. Enter an appropriate Analysis Time Period and click **Update Analysis and Graph**. Under Analysis, note the Required Tablespace size for New Undo Retention. To learn how to alter your tablespace, see ["Extending the Undo Tablespace"](#) on page 6-35.

4. **How do I configure undo to accommodate Flashback operations?** If you are interested in using flashback features such as Flashback Query or Flashback Table, you can use the Undo Advisor to advise on how to configure your tablespace and undo retention. In order for flashback operations to go back in time, the database must ensure that undo data is not overwritten. To build a flashback recovery strategy, you can set the low threshold parameter, which determines the lowest value for automatic undo tuning. For example, if the low threshold is set to 15 minutes, Oracle never lowers the undo retention time to less than 15 minutes. Consequently, if your flashback recovery strategy requires you to go back 8 hours to recover from human errors, set the low threshold to 8 hours. To learn how to set a new retention time, see ["Setting New Threshold Undo Retention Time"](#) on page 6-36.

The **Required Tablespace Size by Undo Retention Length** graph shows the relationship between retention period and undo tablespace size, highlighting key data points, such as the Auto-tuned and Best Possible Retention.

Setting New Threshold Undo Retention Time To set a new low threshold retention time from the Undo Advisor page, enter the value in New Undo Retention and click **OK**.

Alternatively, you can set this parameter as you do for other system parameters by navigating to the All Initialization Parameters page. The parameter is called `undo_retention`. For more information about this page, see ["Viewing and Modifying Initialization Parameters"](#) on page 6-36.

Viewing and Modifying Initialization Parameters

When you install the Oracle Collaboration Suite Database, the initialization parameters are optimized for normal use in the environment. It is not necessary for you to alter any initialization parameters at this time. The steps described in this section will familiarize you with the initial parameter setting for your database and indicate how to modify parameters.

To view or modify the initialization parameters for your database:

1. From the Database Control Console Database Home page, click the **Administration** property page. The next page that you see is the Administration home page shown in [Figure 6-8](#).

Figure 6–8 Database Administration Page

ORACLE Enterprise Manager 10g Database Control

Setup Preferences Help Logout

Database

Logged in As SYS

Database: OCSM14DB.us.oracle.com

Home Performance Administration Maintenance

Instance

- Memory Parameters
- Undo Management
- All Initialization Parameters

Storage

- Controlfiles
- Tablespaces
- Datafiles
- Rollback Segments
- Redo Log Groups
- Archive Logs
- Temporary Tablespace Groups

Security

- Users
- Roles
- Profiles

Enterprise Manager Administration

- Administrators
- Notification Schedule
- Blackouts

Schema

- Tables
- Indexes
- Views
- Synonyms
- Sequences
- Database Links

Warehouse

- Cubes
- OLAP Dimensions
- Measure Folders
- Dimensions
- Materialized Views
- Materialized View Logs
- Refresh Groups

Configuration Management

- Last Collected Configuration
- Database Usage Statistics

Workload

- Automatic Workload Repository
- SQL Tuning Sets

Resource Manager

- Resource Monitors
- Resource Consumer Group Mappings
- Resource Consumer Groups
- Resource Plans

Scheduler

- Jobs
- Schedules
- Programs
- Job Classes
- Windows
- Window Groups
- Global Attributes

2. Click **All Initialization Parameters** under the **Instance** heading.

Enterprise Manager displays the Initialization Parameters page comprised of a table listing the current value of each initialization parameter as seen by the database instance. You can also use this page to alter initialization parameter values, using the **Show SQL**, **Revert**, and **Apply** buttons.

There are two property pages shown on the Initialization Parameters page:

- **Current**—The table on this property page displays all of the initialization parameter values currently seen by the database instance (in memory).
You can use this page to make dynamic changes to parameters in the current running instance. Only parameters marked dynamic can be changed. To do so, enter a new value and click **Apply**.
- **SPFile**—This property page is present when you are using a server parameter file, whose location is displayed at the top of the table. This property page shows parameter settings in the server parameter file.

Changes to parameter settings in this file are persistent across instance startup and shutdown. To make persistent changes to an initialization parameter, enter the new value and click **Apply**. You can optionally apply changes to the current running instance by checking **Apply changes in SPFile to the current running instance**. If you do not check this box, your changes will not take effect until the database is shut down and restarted.

Parameters marked as **Basic** represent a small subset of all initialization parameters, and are considered necessary to keeping the database running smoothly.

As the number of database users grows and workload increases, you might need to alter some initialization parameters. You can make these changes directly using the Initialization Parameter page as described, or indirectly using one of the advisors provided by Oracle. One such advisor, the memory advisor, is described in ["Managing Memory Parameters"](#) on page 6-38.

Managing Memory Parameters

Some initialization parameters, referred to here as memory parameters, determine the total size of the system global area (SGA) and the program global area (PGA), and of the subcomponents of the SGA. The settings of memory parameters can affect the performance of your database. When you install your database, these parameters are tuned to meet the requirements of the environment that you specify.

If you enabled Automatic Shared Memory Configuration when you configured your database, Oracle automatically sizes the subcomponents of the SGA, which include the shared pool and buffer cache. Oracle recommends that you enable memory auto tuning.

If Automatic Shared Memory Management is disabled, you can enable it on the Memory Parameters page. You can navigate to this page from the Administration page by clicking **Memory Parameters** under the Instance heading. From this page you can enable or disable Automatic Shared Memory Management and view your SGA and PGA memory settings from their property pages.

Modifying Memory Parameters

To modify the size of an SGA subcomponent without shutting down your instance, you can disable Automatic Shared Memory Management on the Memory Parameters page. With the Advice button on the Memory Parameters page, the Memory Advisor (discussed in ["Using the Memory Advisor"](#) on page 10-30) gives you advice on optimal memory settings. If you choose to modify your memory settings manually, you can enter new sizes and apply changes dynamically while the instance is up. You can also do so from the Current property page on the Initialization Parameters page. However, there are some restrictions on dynamic modification of memory parameters. For more information, see *Oracle Database Administrator's Guide*.

To make changes to memory parameters persistent across instance startup and shutdown, you must alter your parameter file. You can do so by navigating to SPFile property page from the Memory Parameters page and making your changes there.

See Also: *Oracle Database Performance Tuning Guide* for more information about memory parameters and their tuning

Managing the OracleAS Metadata Repository

The OracleAS Metadata Repository stores schemas used by Oracle Collaboration Suite components for organizing data in the database. These schemas are automatically pre-seeded with appropriate values during installation. This section describes how to manage the OracleAS Metadata Repository, primarily using Grid Control.

This section contains the following topics:

- [Frequently Asked Questions About OracleAS Metadata Repository](#)

- [Viewing OracleAS Metadata Repository Schema Passwords](#)
- [Changing OracleAS Metadata Repository Schema Passwords](#)
- [Changing the Character Set of OracleAS Metadata Repository](#)
- [Renaming and Relocating OracleAS Metadata Repository Datafiles](#)

Frequently Asked Questions About OracleAS Metadata Repository

OracleAS Metadata Repository is an Oracle Database 10g database and can be managed using standard database procedures and tools. However, there are some considerations for managing OracleAS Metadata Repository within the Oracle Collaboration Suite environment. This section answers frequently asked questions about managing the OracleAS Metadata Repository.

- **What is the OracleAS Metadata Repository?**

The OracleAS Metadata Repository is a database. It is pre-seeded with schemas to support Oracle Collaboration Suite components and services.

See Also: {X-REF?} for information on the schemas that are pre-seeded in the OracleAS Metadata Repository

- **When is the OracleAS Metadata Repository required?**

The OracleAS Metadata Repository is an optional component of Oracle Application Server, but it is required for all Oracle Collaboration Suite installations. All of the Oracle Collaboration Suite applications require the OracleAS Metadata Repository.

- **How can I create an OracleAS Metadata Repository?**

The OracleAS Metadata Repository is a part of any Oracle Collaboration Suite Infrastructure installation. The Oracle Universal Installer installs the OracleAS Metadata Repository from scratch. Under the most common deployment scenarios, the OracleAS Metadata Repository is created as part of a single Oracle Collaboration Suite Database. However, in some scenarios you might have several Oracle Collaboration Suite Databases, one of which contains the OracleAS Metadata Repository.

See Also: *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

- **Are there any tools for managing the OracleAS Metadata Repository?**

You can use Database Control to manage the OracleAS Metadata Repository. Refer to "[Using the Oracle Enterprise Manager 10g Database Control Console](#)" on page 6-2.

- **Can I use the OracleAS Metadata Repository to deploy applications?**

No. The Metadata Repository is not supported for deploying applications.

- **Are there any database features that are not supported by the OracleAS Metadata Repository?**

The following tablespace management features are not supported:

- Using `ALTER TABLESPACE` to assign a different default tablespace to a user

- Using `ALTER TABLESPACE` to reduce the number of tablespaces that were created when you initially created the OracleAS Metadata Repository
- Renaming a tablespace

It is, however, possible to use `ALTER TABLESPACE` to do segment management using `autoextend` or any other feature.

■ **Can a OracleAS Metadata Repository coexist on a host with other databases?**

Yes. When you install Oracle Collaboration Suite, the OracleAS Metadata Repository is created within the Oracle Collaboration Suite Database. However you can host the OracleAS Metadata Repository as a separate database in its own Oracle Home, on the same host as other databases, as long as each database has a unique SID and global database identifier. The databases may be able to share a Net listener as follows:

- Multiple Oracle9i and Oracle 10g databases can share the same Net listener port. If the other databases on your host are Oracle9i or Oracle 10g databases, the OracleAS Metadata Repository can use the same Net listener port (for example, 1521) as the other databases.
- If the other databases on your system are Oracle 8i databases running Oracle Net8 listener, then the OracleAS Metadata Repository must use a different port for its Net listener.

■ **Can I change the OracleAS Metadata Repository Net listener port after installation?**

Yes. Refer to ["Changing the OracleAS Metadata Repository Net Listener Port"](#) on page 14-22.

■ **Can I change the OracleAS Metadata Repository SID and global database name after installation?**

No. This is not supported.

■ **Can I change the character set of the OracleAS Metadata Repository?**

Yes. Follow the instructions for changing the character set in the database documentation, then refer to ["Changing the Character Set of OracleAS Metadata Repository"](#) on page 6-46 for updates you need to make to Oracle Application Server.

■ **Can I tune the OracleAS Metadata Repository?**

Yes, you can apply database tuning strategies to the OracleAS Metadata Repository.

One important point to be aware of is that the processes and sessions parameters in the Oracle `init$SID.ora` configuration file should be tuned to allow the OracleAS Metadata Repository to handle the maximum number of database sessions used by Oracle Collaboration Suite Applications tier installations.

The primary consumers of database sessions are OracleAS Portal and Oracle Mobile Collaboration. An `init$SID.ora` setting of `processes=150` should support four Applications tier installations that include these components. Note that an OracleAS Portal best practice recommendation is to relocate the Portal instance out of the Infrastructure, which would reduce the database connections requirement.

See Also: *Oracle Application Server Performance Guide* for a detailed description of the database connection usage of `mod_plsql` in an OracleAS Portal installation

- **Can I change OracleAS Metadata Repository schema passwords?**

Yes. However, you must make sure to use the correct procedure. Some schemas store their passwords in Oracle Internet Directory and you must change their passwords using the Oracle Collaboration Suite Control so the password is updated in Oracle Internet Directory and the database.

See Also: ["Changing OracleAS Metadata Repository Schema Passwords"](#) on page 6-42

- **Can I delete schemas from the OracleAS Metadata Repository that I am not using?**

No. You should never delete any of the schemas that come with the OracleAS Metadata Repository.

- **Can I rename or relocate OracleAS Metadata Repository datafiles after installation?**

Yes.

See Also: ["Renaming and Relocating OracleAS Metadata Repository Datafiles"](#) on page 6-47

- **How can I backup and recover the OracleAS Metadata Repository?**

Oracle provides a backup and recovery strategy for your entire Oracle Collaboration Suite environment, including the OracleAS Metadata Repository.

See Also: [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#)

Viewing OracleAS Metadata Repository Schema Passwords

If a OracleAS Metadata Repository is registered with Oracle Internet Directory, then some schema passwords are stored in the directory and you can view them using Oracle Internet Directory tools.

You can view the passwords using the following procedures:

- [Viewing OracleAS Metadata Repository Schema Passwords using Oracle Directory Manager](#)
- [Viewing OracleAS Metadata Repository Schema Passwords using ldapsearch](#)

Viewing OracleAS Metadata Repository Schema Passwords using Oracle Directory Manager

You can view OracleAS Metadata Repository schema passwords using Oracle Directory Manager as follows:

1. Start Oracle Directory Manager with the following command:

Unix:

```
ORACLE_HOME/bin/oidadmin
```

Windows:

```
Start > Programs > Oracle Application Server > OracleHome >  
Integrated Management Tools > Oracle Directory Manager
```

2. Log in to Oracle Directory Manager as the `orcladmin` user.
3. In the System Objects frame, expand **Entry Management**, expand **cn=OracleContext**, expand **cn=Products**, expand **cn=IAS**, expand **cn=IAS Infrastructure Databases**, and expand the `orclReferenceName` for the OracleAS Metadata Repository.
4. Select the `OrclResourceName` entry for the schema whose password you want to view.
5. In the Properties tab, you can view the password in the `orclpasswordattribute` field.

Viewing OracleAS Metadata Repository Schema Passwords using `ldapsearch`

You can view OracleAS Metadata Repository schema passwords using `ldapsearch`, a command-line tool, as follows:

```
ORACLE_HOME/bin/ldapsearch -p oid_port -h oid_hostname -D "cn=orcladmin"  
-w orcladmin_password -b "orclresourcename=schema_name,  
orclreferencename=metadata_rep_global_db_name, cn=ias infrastructure databases,  
cn=ias, cn=products, cn=oraclecontext" -s base "objectclass=*"   
orclpasswordattribute
```

The command returns several lines of output. The password is listed in the following line:

```
orclpasswordattribute=password
```

The following is an example for viewing the ORASSO schema password. In this example, the ORASSO schema password is `Og23NI78`.

```
ORACLE_HOME/bin/ldapsearch -p 3060 -h myhost -D "cn=orcladmin"  
-w mypassword -b "orclresourcename=ORASSO,  
orclreferencename=orcl.mycompany.com,  
cn=ias infrastructure databases, cn=ias, cn=products,  
cn=oraclecontext" -s base "objectclass=*" orclpasswordattribute
```

```
OrclResourceName=ORASSO,orclReferenceName=orcl.mycompany.com  
cn=IAS Infrastructure Databases,cn=IAS,cn=Products,cn=OracleContext  
orclpasswordattribute=Og23NI78
```

Changing OracleAS Metadata Repository Schema Passwords

The method for changing schema passwords in the OracleAS Metadata Repository varies by schema. Some schemas store their passwords in Oracle Internet Directory; you must change their passwords using the Oracle Collaboration Suite Control so that both Oracle Internet Directory and the database are updated. Other schemas do not store their passwords in Oracle Internet Directory; you can change their passwords in the database using SQL*Plus. A few schemas require special steps for changing their passwords.

See ["Changing Oracle Collaboration Suite Schema Passwords"](#) on page 6-49 for special instructions for changing the Oracle Collaboration Suite Application schema passwords.

Table 6–2 lists the appropriate method for changing some OracleAS Metadata Repository schema passwords.

Table 6–2 Methods for Changing OracleAS Metadata Repository Schema Passwords

Schema	Method for Changing Password
B2B	You must change the password in two places: ■ Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45. ■ Manually change the password in Oracle Internet Directory. Refer to "Changing Schema Passwords in Oracle Internet Directory" on page 6-46.
DCM	If the OracleAS Metadata Repository is registered with Oracle Internet Directory, you must change the password in two places: ■ Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45. ■ Manually change the password in Oracle Internet Directory. Refer to "Changing Schema Passwords in Oracle Internet Directory" on page 6-46. If the OracleAS Metadata Repository is not registered with Oracle Internet Directory, you only need to change the password directly in the database using SQL*Plus.
DISCOVERER5	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
DSGATEWAY ¹	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
IP ²	You must change the password in two places: ■ Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45. ■ Manually change the password in Oracle Internet Directory. Refer to "Changing Schema Passwords in Oracle Internet Directory" on page 6-46.
OCA	This schema requires special steps. Refer to <i>Oracle Application Server Certificate Authority Administrator's Guide</i> for advanced topics in administration.
ODS	This schema requires special steps. Refer to <i>Oracle Internet Directory Administrator's Guide</i> for information on resetting the default password for the database.
ORAOCA_PUBLIC	This schema requires special steps. Refer to <i>Oracle Application Server Certificate Authority Administrator's Guide</i> for advanced topics in administration.
ORASSO	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Infrastructure (Identity Management) installation and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45. After you change the password, restart Oracle HTTP Server: <pre>opmnctl stopproc ias-component=HTTP_Server opmnctl startproc ias-component=HTTP_Server</pre>
ORASSO_DS	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Infrastructure (Identity Management) installation and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
ORASSO_PA	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Infrastructure (Identity Management) installation and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.

Table 6–2 (Cont.) Methods for Changing OracleAS Metadata Repository Schema Passwords

Schema	Method for Changing Password
ORASSO_PS	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Infrastructure (Identity Management) installation and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45. Changing the ORASSO_PS password requires that the database link from all Portal schemas to the ORASSO_PS schema be re-created. To do this, run the following command for each affected Portal instance: <pre>ORACLE_HOME/portal/conf/ptlconfig -dad dad_name -site [-pw PORTAL_schema_password]</pre> Refer to <i>Oracle Application Server Portal Configuration Guide</i>.
ORASSO_PUBLIC	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Infrastructure (Identity Management) installation and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
OWF_MGR	You must change the password in two places: ■ Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45. ■ Manually change the password in Oracle Internet Directory. Refer to "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
PORTAL	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45. After you change the password, restart Oracle HTTP Server: <pre>opmnctl stopproc ias-component=HTTP_Server opmnctl startproc ias-component=HTTP_Server</pre>
PORTAL_APP	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
PORTAL_DEMO	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
PORTAL_PUBLIC	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
SCOTT	Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45.
SYS	Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45.
SYSTEM	Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45.
UDDISYS	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.

Table 6–2 (Cont.) Methods for Changing OracleAS Metadata Repository Schema Passwords

Schema	Method for Changing Password
WCERSYS	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
WIRELESS	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
WK_TEST	Use SQL*Plus to change the password directly in the database. Refer to "Changing Schema Passwords using SQL*Plus" on page 6-45.
WKPROXY	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.
WKSYS	Use the Oracle Collaboration Suite Control. Navigate to the Application Server Home Page for the Applications tier instance that uses this schema and follow the instructions in "Changing Schema Passwords using the Oracle Collaboration Suite Control" on page 6-45.

¹ Beginning with Oracle Application Server 10g Release 2 (10.1.2), the DSGATEWAY schema is not used. It is provided for backward compatibility.

² Beginning with Oracle Application Server 10g Release 2 (10.1.2), the IP schema does not contain any data. It has been replaced by the B2B schema and is provided only for backward compatibility.

Changing Schema Passwords using the Oracle Collaboration Suite Control

Some schemas store their passwords in Oracle Internet Directory. You must change their passwords using the Oracle Collaboration Suite Control so the password is updated in both the database and Oracle Internet Directory.

To change a schema password using the Oracle Collaboration Suite Control:

1. Depending on the schema, navigate to the home page for the Applications tier instance or the Infrastructure. Refer to [Table 6–2](#) to determine which home page to use.
2. On the home page, click **Infrastructure**.
3. On the Infrastructure page, click **Change Schema Password**.
4. On the Change Schema Password page, select the schema. Enter the new password in the **Password** and **Confirm Password** fields. Click **OK**.

Changing Schema Passwords using SQL*Plus

You can change some schema passwords directly in the database using SQL*Plus. To do so, connect to the database as a user with SYSDBA privileges and issue the following command:

```
SQL> ALTER USER schema identified by new_password;
```

For example, to change the SCOTT schema password to "abc123":

```
SQL> ALTER USER SCOTT IDENTIFIED BY abc123;
```

Changing Schema Passwords in Oracle Internet Directory

A few schemas (DCM, B2B, OWF_MGR) require you to manually update the password in the OracleAS Metadata Repository and in Oracle Internet Directory. You can use this procedure to change these passwords.

1. Start Oracle Directory Manager with the following command:

```
(UNIX) ORACLE_HOME/bin/oidadmin  
(Windows) Start > Programs > Oracle Application Server - OracleHome >  
Integrated Management Tools > Oracle Directory Manager
```
2. Log in to Oracle Directory Manager as the `orcladmin` user.
3. In the System Objects frame, expand **Entry Management**, expand **cn=OracleContext**, expand **cn=Products**, expand **cn=IAS**, expand **cn=IAS Infrastructure Databases**, and expand the `orclReferenceName` for the OracleAS Metadata Repository
4. Select the `OrclResourceName` entry for the schema whose password you want to change.
5. In the Properties tab, update the password in the `orclpasswordattribute` field.
6. Click **Apply**.

Changing the Character Set of OracleAS Metadata Repository

To configure the Applications tier and Infrastructure to work with OracleAS Metadata Repository after its character set has been changed:

1. Modify the character set of all Database Access Descriptors (DADs) accessing the OracleAS Metadata Repository to the new database character set.
 - a. Using the Oracle Collaboration Suite Control, navigate to the Applications tier instance home page.
 - b. In the System Components section, click **HTTP_Server**.
 - c. On the HTTP_Server home page, click **Administration**.
 - d. On the HTTP_Server Administration page, select **PL/SQL Properties**. This opens the `mod_plsql` Services page.
 - e. Scroll to the DADs section and click the name of the DAD that you want to configure. This opens the Edit DAD page.
 - f. In the **NLS Language** field, type in a `NLS_LANG` value whose character set is the same as the new character set for OracleAS Metadata Repository.
 - g. Click **OK**.
 - h. Repeat steps e to g for all DADs accessing OracleAS Metadata Repository.
2. Reconfigure the Oracle Ultra Search index as follows:
 - a. Connect to OracleAS Metadata Repository as `WKSYS` and invoke the following SQL script to reconfigure the default cache character set and index preference:

```
ORACLE_HOME/ultrasearch/admin/wk0prefcheck.sql
```
 - b. Connect to OracleAS Metadata Repository as the default user (`WKTEST`) and invoke the following SQL script:

```
ORACLE_HOME/ultrasearch/admin/wk0idxcheck.sql
```


The script requests you to enter the instance name (WK_INST). Enter "y" when prompted to go ahead with the change.

This script re-configures the instance (in this case, the default instance). It also truncates the Oracle Text index used by Oracle Ultra Search and you must force a recrawl to rebuild the index.

- c. Repeat step b for all Oracle Ultra Search instances that were created before you changed the database character set. Invoke the script as the instance owner, and then force a recrawl of all data sources, if necessary.

Renaming and Relocating OracleAS Metadata Repository Datafiles

When you install OracleAS Metadata Repository, you can choose the location for its datafiles. The default location is `ORACLE_HOME/oradata/SID`. After installation, you may want to relocate datafiles to a different directory. For example, you may want to move them to a directory on a file system with more space. Or, you may want to move them to a directory on a different disk for performance reasons. Another thing you may want to do is keep the datafiles in the same directory, but rename them.

If have kept datafiles in an Oracle home from an Oracle Collaboration Suite Release 1 (9.0.3) or Release 2 (9.0.4), you can use this procedure to move the datafiles. The upgrade process described in the *Oracle Collaboration Suite Upgrade Guide* does not move them from their original location.

This section provides a procedure for renaming or relocating datafiles. You can use this procedure on one or more datafiles, and the datafiles may be in multiple tablespaces.

This procedure applies to:

- The datafiles associated with Oracle Collaboration Suite schemas and tablespaces.
- The following standard Oracle database datafiles:
 - `drsys01.dbf`
 - `system01.dbf`
 - `temp01.dbf`
 - `users01.dbf`

The following example shows how to relocate two datafiles in two different tablespaces, as follows:

- Relocate the `oca.dbf` datafile in the OCATS tablespace from `/infra_home/oradata/orcl/oca.dbf` to `/new_directory/oca.dbf`
- Relocate the `dcm.dbf` datafile in the DCM schema from `/infra_home/oradata/orcl/dcm.dbf` to `/new_directory/dcm.dbf`

Before you start the procedure:

- Make sure you have a complete cold backup of OracleAS Metadata Repository.

See Also: [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#)

- Connect to OracleAS Metadata Repository as a user with administrator privileges. You must have the `ALTER DATABASE` system privilege to relocate datafiles.
- Read through the entire procedure before you start.

The procedure is as follows:

1. Verify the location of your datafiles.

You can verify the location of datafiles in a particular tablespace by querying the [data dictionary](#) view `DBA_DATA_FILES`.

For example, to query the location of datafiles in the OCATS and DCM tablespaces:

```
SQL> SELECT FILE_NAME, BYTES FROM DBA_DATA_FILES
WHERE TABLESPACE_NAME = 'OCATS' OR TABLESPACE_NAME = 'DCM';
```

FILE_NAME	BYTES
-----	-----
/infra_home/oradata/orcl/oca.dbf	78643200
/infra_home/oradata/orcl/dcm.dbf	96993280

2. Shut down all Applications tier instances that use OracleAS Metadata Repository. (All Oracle Collaboration Suite applications use the OracleAS Metadata Repository.)
3. Stop the Infrastructure that contains OracleAS Metadata Repository, then start an OracleAS Metadata Repository instance and mount the database without opening it, as follows:

- a. Stop the Oracle Collaboration Suite Control and OPMN-managed processes:

```
emctl stop iasconsole
opmnctl stopall
```

- b. Leave the OracleAS Metadata Repository listener running.

- c. Stop the OracleAS Metadata Repository instance (make sure the `ORACLE_HOME` environment variable is set):

```
sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> SHUTDOWN
```

- d. Start an OracleAS Metadata Repository instance and mount the database without opening it:

```
SQL> STARTUP MOUNT
```

4. Move the datafiles to their new location using the operating system. For example:

```
(UNIX)
mv /infra_home/oradata/orcl/oca.dbf /new_directory/oca.dbf
mv /infra_home/oradata/orcl/dcm.dbf /new_directory/dcm.dbf
```

```
(Windows)
rename C:\infra_home\oradata\orcl\oca.dbf D:\new_directory\oca.dbf
rename C:\infra_home\oradata\orcl\dcm.dbf D:\new_directory\dcm.dbf
```

Note: You can execute an operating system command to copy a file by using the SQL*Plus `HOST` command.

5. Use `ALTER DATABASE` to rename the file pointers in the database's control file:

```
SQL> ALTER DATABASE
RENAME FILE ' /infra_home/oradata/orcl/oca.dbf',
```

```

TO
        '/infra_home/oradata/orcl/dcm.dbf'
        '/new_directory/oca.dbf',
        '/new_directory/dcm.dbf';

```

The new files must already exist; this statement does not create the files. Also, always provide complete filenames (including their full paths) to properly identify the old and new datafiles. In particular, specify the old datafile name exactly as it appears in the DBA_DATA_FILES view of the data dictionary.

6. Shut down OracleAS Metadata Repository, then perform a normal startup of the Infrastructure:

- a. Leave the OracleAS Metadata Repository listener running.
- b. Shut down OracleAS Metadata Repository:

```
SQL> SHUTDOWN
```

- c. Start OracleAS Metadata Repository:

```
SQL> STARTUP
```

- d. Start OPMN-managed processes and the Oracle Collaboration Suite Control:

```
opmnctl startall
emctl start iasconsole
```

7. Start the Applications tier instances that use the Infrastructure. (All Oracle Collaboration Suite applications use the Infrastructure.)

8. Verify the new location of your datafiles.

```
SQL> SELECT FILE_NAME, BYTES FROM DBA_DATA_FILES
WHERE TABLESPACE_NAME = 'OCATS' OR TABLESPACE_NAME = 'DCM';
```

FILE_NAME	BYTES
/new_directory/oca.dbf	78643200
/new_directory/dcm.dbf	96993280

9. Perform a complete cold backup of OracleAS Metadata Repository. After making any structural changes to a database, always perform an immediate and complete backup.

See Also: [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#)

Changing Oracle Collaboration Suite Schema Passwords

[As a part of your routine security procedures, you may want to change the passwords used by Oracle Collaboration Suite components to access the application schemas.

Each of the following sections describes how to update the Oracle Collaboration Suite applications when you make a change to an application schema password. Generally, to change a schema password, see ["Changing OracleAS Metadata Repository Schema Passwords"](#) on page 6-42, and then follow the specific instructions for each affected application.

This section contains the following topics:

- [Changing the Oracle Calendar Schema Password](#)
- [Changing the Oracle Content Services Schema Password](#)

- [Changing the Oracle Mail Schema Password](#)
- [Changing the Oracle Real-Time Collaboration Schema Password](#)

Changing the Oracle Calendar Schema Password

Follow these steps to change the Oracle Calendar schema password:

1. Change the schema password for the Calendar database user.
2. Once the database schema password has been changed run the following command-line utility from the `$ORACLE_HOME/ocal/bin` directory:

```
unioiconf -setschemapassword <dbglobalname> -D <bindDN>
```

Where `<bindDN>` is typically `'cn=orcladmin'` and `<dbglobalname>` is the fully-qualified database name `<$ORACLE_SID><$DOMAIN_NAME>`, such as `'ASDB.ca.oracle.com'`.

See Also: For more information on the `unioiconf` utility, refer to Chapter 6, "Calendar Server Utilities" in the *Oracle Calendar Reference Manual*

Changing the Oracle Content Services Schema Password

You can use the Application Server Control for Collaboration Suite to change the Oracle Content Services schema password. The password will be changed in Oracle Internet Directory, as well as:

- On the current Applications tier, if you are running repository metrics on this Applications tier
- In the Oracle Database, if you select **Change in Database**

You should only change the schema password from the Applications tier on which repository metrics are being collected. If you are collecting repository metrics on more than one Applications tier, you must change the schema password on all Applications tiers where repository metrics are collected. If you are not collecting any repository metrics, it does not matter which Applications tier you choose to use. See *Oracle Content Services Administrator's Guide* for more information about repository metrics.

To change the Oracle Content Services schema password:

1. Connect to the Application Server Control for Collaboration Suite from the Applications tier where you want to change the schema password.
2. Navigate to the Content Services Home page.
3. Click **Stop Domain**.
4. Click **Change Schema Password** in the Administration section. You will not be able to access the Change Schema Password page unless all Oracle Content Services processes have been stopped.
5. Provide the new password and confirm it in the **Password** and **Confirm Password** fields.
6. If the schema password has not yet been changed in the database, you can choose to change the database schema password at this time. To do this, select **Change in Database** and provide the database SYS password.
7. Click **OK**.

8. Return to the Content Services Home page and click **Start Domain**.

Changing the Oracle Mail Schema Password

Follow these steps to change the Oracle Mail schema password (for the ES_MAIL schema):

1. Stop all Oracle Mail processes on every Applications tier:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=email
```

2. Connect to the Oracle Collaboration Suite Database as SYSDBA and change the password for ES_MAIL:

```
SQL> alter user es_mail identified by <new_password>;
```

where <new_password> is the clear text password to be changed.

3. Launch Oracle Directory Manager (oidadmin) and connect to the OracleAS Metadata Repository. Navigate to the following location under Entry Management:

```
cn=<ocs_db_global_name>,cn=MailStores,cn=um_  
system,cn=EEmailServerContainer,cn=Products,cn=OracleContext
```

where <ocs_db_global_name> is the global name of the Oracle Collaboration Suite Database <\${ORACLE_SID}><\${DOMAIN_NAME}>, such as 'ASDB.ca.oracle.com'.

4. Change the value of the attribute orclpasswordattribute to the new password, and click **Apply**.
5. On each Applications tier on which Oracle Mail is configured, run the following command:

```
% $ORACLE_HOME/jdk/jre/bin/java -classpath $ORACLE_  
HOME/jlib/esinstall.jar:$ORACLE_HOME/jlib/esldap.jar:$ORACLE_  
HOME/lib/mail.jar:$ORACLE_HOME/jlib/esadmin.jar:$ORACLE_  
HOME/jlib/escommon.jar:$ORACLE_HOME/jlib/repository.jar:$ORACLE_  
HOME/jlib/emConfigInstall.jar oracle.mail.install.EMConfig $ORACLE_HOME
```

6. If you are using Grid Control to manage Oracle Mail, you also need to update Grid Control with the new schema password.
 - a. From the Grid Control Console, select the **Targets** tab.
 - b. Select the **All Targets** tab.
 - c. Search for the target type "". Click on the target name in the results page to view the target home page.
 - d. Click **Monitoring configuration**.
 - e. Type in the new schema password as the value of **Administration Store Password**.

7. Restart the Oracle Mail processes on all Applications tiers:

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=email
```

8. Restart the Oracle Collaboration Suite Control on all tiers:

```
ORACLE_HOME/bin/emctl stop iasconsole  
ORACLE_HOME/bin/emctl start iasconsole
```

Changing the Oracle Real-Time Collaboration Schema Password

Follow these steps to change the Oracle Real-Time Collaboration schema password:

1. Stop the Oracle Real-Time Collaboration Applications tier:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=RTC
```

2. Stop OC4J_imeeting (Oracle Real-Time Collaboration Application for J2EE):

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J process-type=OC4J_imeeting
```

3. Change the database schema password.

4. For each Applications tier, enter the following command:

```
$ORACLE_HOME/imeeting/bin/rtcctl  
rtcctl> updateDatabaseInfo -dbpassword <newpassword>
```

Where *<newpassword>* is the new schema password.

5. Start the Oracle Real-Time Collaboration Applications tier:

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=RTC
```

6. Start OC4J_imeeting (Oracle Real-Time Collaboration Application for J2EE):

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OC4J process-type=OC4J_imeeting
```

Managing Oracle Collaboration Suite Infrastructure

The Infrastructure component of Oracle Collaboration Suite is the Oracle Application Server 10g instance(s), which host the centralized databases, and services utilized by most or all of the Oracle Collaboration Suite applications.

These components and databases include:

- Identity Management Services (IM)
- OracleAS Metadata Repository (MR)
- Delegated Administration Services (DAS)
- Single Sign-On service (SSO)
- Oracle Directory and Integration Provisioning Server (DIP)
- Oracle Internet Directory (OID)

This chapter describes how to manage various parts of the Oracle Collaboration Suite Infrastructure. You will perform most of these management tasks using Enterprise Manager Application Server Control Console for Oracle Collaboration Suite (OCS Control).

This chapter does not address topics about managing the actual databases that reside on the Infrastructure. For information about managing your Oracle Collaboration Suite databases, see [Chapter 6, "Managing Oracle Collaboration Suite Databases"](#).

This chapter contains the following topics:

- [Setting Up and Enabling Multiple Realms](#)
- [Managing the Oracle Internet Directory Service Registry](#)

Setting Up and Enabling Multiple Realms

This section explains how to enable the single sign-on server to support multiple realms within one instance of the Oracle Identity Management infrastructure. You may use different realms, or namespaces, within one instance of the Oracle Identity Management infrastructure to set and store Oracle configuration information unique to different sets of users.

Realm configuration is a three-part process that consists of the following:

- Creating realms in Oracle Internet Directory
- "Turning on" multiple realms in OracleAS Single Sign-On

- Making Oracle Collaboration Suite applications aware of identity management realms

This section contains the following topics:

- [How the Single Sign-On Server Enables Authentication to Multiple Realms](#)
- [Configuring the Single Sign-On Server for Multiple Realms](#)
- [Granting Administrative Privileges for Multiple Realms](#)

How the Single Sign-On Server Enables Authentication to Multiple Realms

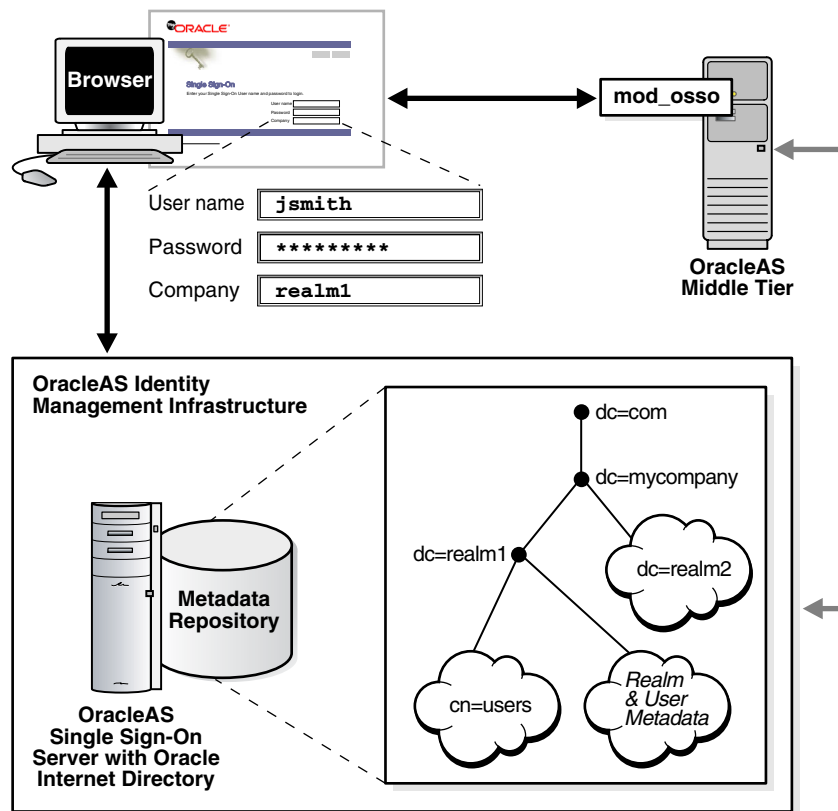
The authentication sequence for single sign-on to multiple realms is much the same as it is for single sign-on in a single, default realm. The only difference from the user's perspective is that, when the user affiliated with the first type of realm is presented with the login screen (see [Figure 7-1](#) on page 7-3), he or she must enter not only a user name and password but also a new credential: the realm nickname. The value entered can be case insensitive.

This section covers the following topics:

- [Locating Realms in Oracle Internet Directory](#)
- [Validating Realm-Affiliated Users to Partner Applications](#)

Locating Realms in Oracle Internet Directory

Once a user has entered his credentials, both his realm nickname and user name are mapped to entries in Oracle Internet Directory. More specifically, the single sign-on server uses directory metadata to find the realm entry in the directory. Once it finds this entry, the single sign-on server uses realm metadata to locate the user. Once the user's entry is found, his password, an attribute of his entry, is validated. And once his password is validated, he is authenticated.

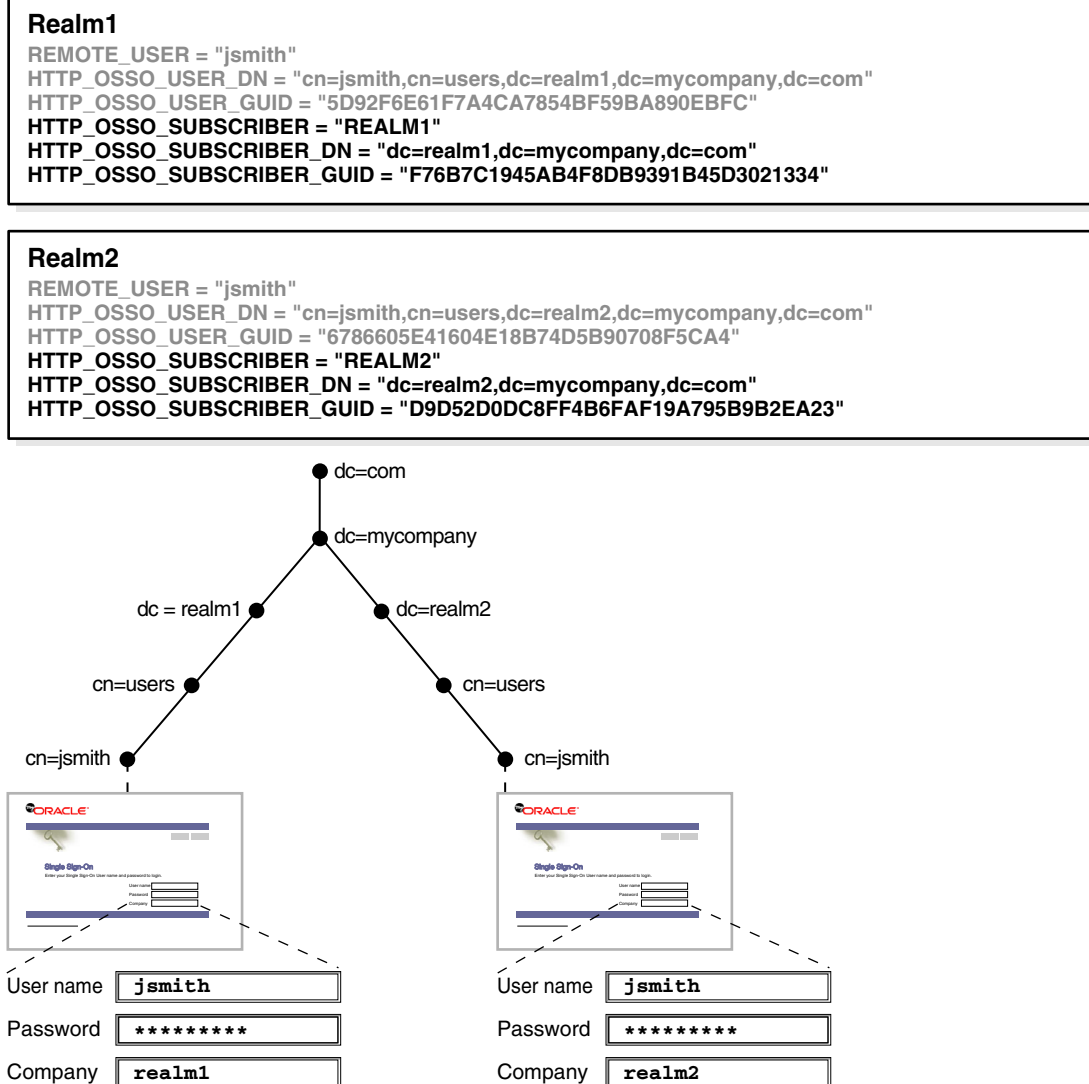
Figure 7-1 The Big Picture: Single Sign-On in Multiple Realms

Validating Realm-Affiliated Users to Partner Applications

Presented with two users, both with the same nickname but affiliated with different realms, a partner application requires some mechanism for distinguishing between these users. The application requires such a mechanism because it must be able to adapt content—an OracleAS Portal page with stock news and stock listings, for instance—to match the needs of the realm requesting it. Accordingly, OracleAS release 9.0.4 adds the realm nickname, realm DN, and realm GUID as attributes passed to **mod_osso**. Recall that **mod_osso** sets a cookie, storing the retrieved attributes as HTTP headers. When deciding what content to offer up, the application may use function calls to retrieve any one of these attributes from **mod_osso** headers.

For detailed information about **mod_osso** headers and the methods used to access them, see the chapter about **mod_osso** in *Oracle Identity Management Application Developer's Guide*.

[Figure 7-2](#) on page 7-4 shows how applications running in **mod_osso** see HTTP headers for two users with the same nickname who are affiliated with two different realms. The application uses the headers that appear in bold face to distinguish between the two users. The host, or default realm, in this case is **mycompany.com**.

Figure 7-2 *mod_osso Headers for Users with the Same Name*

Configuring the Single Sign-On Server for Multiple Realms

Configuring the single sign-on server for multiple realms involves creating an entry for each realm in the single sign-on schema. Every realm that you create in Oracle Internet Directory must have a corresponding entry in the single sign-on schema.

Note:

- Create the realm in the directory before creating it in the single sign-on schema.
- The configuration scripts that follow work only on UNIX platforms. They cannot be run on Windows platforms.

To configure the single sign-on server for multiple realms, complete the steps that follow. Steps 1, 2, and 5 must be completed only once because these steps enable the

server for multiple realms. Steps 3 and 4 must be completed each time you add a realm.

1. Ensure that you have installed the OracleAS infrastructure and the single sign-on server.
2. Go to `ORACLE_HOME/sso/admin/plsql/wwhost`.

Run the `enblhstg.csh` script using the syntax that follows. See [Table 7-1](#) on page 7-6 for an explanation of script parameters:

```
enblhstg.csh -mode sso
              -sc sso_schema_connect_string
              -ss orasso
              -sw sso_schema_password
              -h oid_host_name
              -p oid_port
              -d "cn=orcladmin"
              -w oid_bind_password
```

Note: If the single sign-on server is part of a distributed deployment, make sure that you run the script on the computer that contains the metadata repository for OracleAS.

Here is an example:

```
enblhstg.csh -mode sso
              -sc webdbsvr2:1521:s901dev3
              -ss orasso
              -sw xyz
              -h dlsun670.us.oracle.com
              -p 389
              -d "cn=orcladmin"
              -w welcome123
```

3. Add realms to Oracle Internet Directory:
 - a. Login into the Oracle Internet Directory Provisioning Console as the `orcladmin` super-user:


```
http://<fully_qualified_oid_instance>:<port_no>/oiddas
```
 - b. Click on Realm Management
 - c. Enter value for "Realm Management"
 - d. Click Submit
4. Create an entry for the realm in the single sign-on database. Use the script `ORACLE_HOME/sso/admin/plsql/wwhost/addsub.csh`. Again, if your single sign-on server is part of a distributed deployment, run the script on the computer that contains the metadata repository for OracleAS.

Use the following syntax to execute the script:

```
addsub.csh -name realm_nickname
            -id realm_ID
            -mode sso
            -sc sso_schema_connect_string
            -ss sso_schema_name
            -sw sso_schema_password
            -h oid_host_name
```

```
-p oid_port
-d oid_bind_dn
-w oid_bind_dn_password
-sp sys_schema_password
```

Table 7-1 on page 7-6 defines parameters for both `enblhstg.csh` and `addsub.csh`.

Table 7-1 Parameters for `enblhstg.csh` and `addsub.csh`

Parameter	Description
-mode	The value here must be <code>sso</code> .
-sc	The connect string for the single sign-on schema. Use the format <code>host:port:sid</code> .
-ss	The name of the single sign-on schema. This parameter must be <code>orasso</code> .
-sw	The password for the single sign-on schema. See Appendix B to learn how to obtain it.
-h	The host name for the Oracle Internet Directory server.
-p	The port number for the Oracle Internet Directory server.
-d	The bind DN for the Oracle Internet Directory server. The value of this parameter is <code>cn=orcladmin</code> . This is the directory super user.
-w	The password for the Oracle Internet Directory super user, <code>cn=orcladmin</code> .
-name	The realm nickname. This is the value that you enter into the company field on the login page.
-id	The realm ID. Choose an integer greater than 1. The value 1 is reserved for the default realm. The single sign-on server uses realm IDs internally, as an index.
-sp	The <code>sys</code> schema password. This password is chosen during the installation of OracleAS.

Note:

- When the script asks you about the duplicated subscriber entry, choose the option to use the existing entry.
 - If you are creating a one-level realm, include the parameters `-sd default_realm_id` and `-type db` in the script.
-
-

5. Update the sample login page with the multiple realm version of the page. You do this by editing `ORACLE_HOME/j2ee/OC4J_SECURITY/applications/sso/web/jsp/login.jsp`.

Note: In a distributed deployment, this file is located on the single sign-on Applications tier.

After making a backup copy of the file, search through it for the following string:

```
<%-- UNCOMMENT THE FOLLOWING BLOCK TO ENABLE MULTI-SUBSCRIBER SUPPORT --%>
```

Uncomment this section:

```

<!-- tr valign="middle">
  <td style="padding-top: 10px" align="<%= reverse? "left" : "right" %>">
    <label for="subscribername">
      <%= getString(rb, "login.form.label.subscribername") %>
    </label>
  </td>
  <td style="padding-top: 10px">
    <input type="text" name="subscribername" size="40" maxlength="255"
      class="textinput" value="<%= (subscribername != null) ?
      subscribername.trim() : " " %>">
    </td>
</tr --%>

```

6. Stop and then start the single sign-on Applications tier:

```

ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY

```

Granting Administrative Privileges for Multiple Realms

Oracle Internet Directory propagates the DIT structure of the default realm across realms when it creates these realms. Note, however, that the users, groups, and privileges that exist in the DIT of the default realm are not propagated. The super user (the `oidadmin` account) or realm administrator must assign, or reassign, privileges. For more information about assigning privileges, see ["Managing User Entries Using the Provisioning Console"](#) on page 4-7.

Managing the Oracle Internet Directory Service Registry

The Oracle Internet Directory 10g Service Registry is a new feature of Oracle Collaboration Suite 10g Release 1 (10.1.1). In order to allow the various Oracle Collaboration Suite components to easily locate interfaces (service URIs) of other components, a new directory of services has been created in the Oracle Internet Directory 10g. During the configuration of each Oracle Collaboration Suite component, URIs are recorded in the Service Registry.

Introduction to the Oracle Internet Directory Service Registry

During operation, components automatically check the Service Registry to discover the correct URI for each available service. For example, Oracle Mobile Collaboration checks the Service Registry to discover the URI for Oracle Mail's IMAP server, in order to display new e-mails to a user on a wireless device.

The Service Registry is particularly important to the operation of OracleAS Portal and Oracle Collaborative Portlets. These components make many connections to the various Oracle Collaboration Suite applications in order to populate the portlets with connection URLs and summarized data.

You may need to make changes to the URIs recorded in the Service Registry from time to time. Changes must be made manually when you perform any of the following procedures:

- Add a load-balancer and additional Applications tier nodes to your Oracle Collaboration Suite configuration
- Install or configure OracleAS Portal and Oracle Collaborative Portlets on separate Applications tiers

- Move an Applications tier to a new host computer, give it a new host name, or change ports used
- Change to Secure Socket Layers (SSL) access to Oracle Collaboration Suite applications

URIs Recorded in the Oracle Internet Directory Service Registry

The Oracle Internet Directory Service Registry stores a variety of information about each configured Oracle Collaboration Suite application. For the purposes of problem solving and handling changes made to Oracle Collaboration Suite applications, the most important information recorded is the set of URIs which are used to communicate between the various applications.

These URIs can be categorized into three broad groups:

- Browser URIs
- Web Service URIs
- Other miscellaneous URIs

Browser URIs are the URIs which are provided as links for users to select, in order to navigate to the various application Web resources.

Web Service URIs are used by the various applications themselves, to query each other for data to present in their own user interfaces. For example, OracleAS Portal makes extensive use of Web Service URIs to present information such as new Oracle Mail messages and upcoming Oracle Calendar events in the Portal page. Oracle Workspaces also makes extensive use of Web Service URIs to aggregate and present resources from different Oracle Collaboration Suite applications together in a single workspace view.

In a load balanced deployment, both Browser and Web Service URIs should be load balanced and must be modified in the Service Registry if you make host or port changes. Only the Browser URIs can be set to use **HTTPS** (SSL).

Various other URIs are also stored in the Oracle Internet Directory Service Registry, such as the RSS feed URL provided by Oracle Discussions.

Table 7–2, "URIs Recorded in the Oracle Internet Directory Service Registry" shows a comprehensive list of URIs recorded in the Oracle Internet Directory Service Registry. Note that the path of some objects is created based on your database <db> or hostname <host> values.

Table 7–2 URIs Recorded in the Oracle Internet Directory Service Registry

Application	Path	URI Label	URI Type
Calendar	cn=OCAD 24924	labeleduri;adminurl:	Browser
	cn=OCAL 78476	labeleduri;appuri:	
	cn=OCAL 78476	labeleduri;cshuri:	
	cn=OCAS 90991	labeleduri;syncserversecureurl:	Browser
	cn=OCAS 90991	labeleduri;syncserverurl:	Browser
	cn=OCAS 90991	labeleduri;webbaseurl:	Browser
	cn=OCAS 90991	labeleduri;webserviceurl:	Web Service
CollaborativeWorkspaces	cn=<db>	labeleduri;adminurl:	Browser
	cn=<db>	labeleduri;webbaseurl:	Browser

Table 7–2 (Cont.) URIs Recorded in the Oracle Internet Directory Service Registry

Application	Path	URI Label	URI Type
Email	cn=<db>	labeleduri;webui:	Browser
	cn=emailadmin	labeleduri;adminurl:	Browser
	cn=imap	labeleduri:	
	cn=smtp	labeleduri:	
	cn=Webmail	labeleduri;peopleurl:	Browser
	cn=Webmail	labeleduri;webbaseurl:	Browser
	cn=Webmail	orclraparameter;webbaseurl:	Browser
Content Services	cn=webservice	labeleduri;webservice:	Web Service
	cn=FILES	labeleduri;adminurl:	Browser
	cn=FILES	labeleduri;s2sauthenticationurl:	Web Service
	cn=FILES	labeleduri;webdavurl:	Browser / WebDAV
OCSCClient	cn=FILES	labeleduri;webservicesurl:	Web Service
	cn=IntegratedClient	labeleduri;baseurl:	Browser
	cn=IntegratedClient	labeleduri;popupliburl:	Browser
	cn=Search	labeleduri;webbaseurl:	Browser
Portal	cn=ReturnToPortalURL	labeleduri:	Browser
RTC	cn=RTC	labeleduri;adminurl:	Browser
	cn=RTC	labeleduri;enduserurl:	Browser
	cn=RTC	labeleduri;guesturl:	Browser
	cn=RTC	labeleduri;integrationservicehome:	Web Service
	cn=RTC	labeleduri:integrationserviceurl:	Web Service
ThreadedDiscussions	cn=Discussions:<db>:<host>	labeleduri;adminurl:	Browser
	cn=Discussions:<db>:<host>	labeleduri;rss:	RSS Feed
	cn=Discussions:<db>:<host>	labeleduri;webbaseurl:	Browser
	cn=Discussions:<db>:<host>	labeleduri;webui:	Browser
	cn=Discussions:<db>:<host>	orclassociasinstance:	Other
	cn=Discussions:<db>:<host>	orclraparameter:	Other
Wireless	cn=WIRELESS1	labeleduri;adminurl:	Browser
	cn=WIRELESS1	labeleduri;calendarnotificationlistenerurl:	
	cn=WIRELESS1	labeleduri;mobilesetupurl:	Browser
	cn=WIRELESS1	labeleduri;presencewebservicesurl:	Web Service

See Also: For instructions on locating and editing Oracle Internet Directory Service Registry URIs, see ["Using Oracle Directory Manager to Edit the Oracle Internet Directory Service Registry"](#) on page 7-10

Using Oracle Directory Manager to Edit the Oracle Internet Directory Service Registry

To edit the Oracle Internet Directory Service Registry using the Oracle Directory Manager:

1. Start the Oracle Directory Manager:

Unix:

```
ORACLE_HOME/bin/oidadmin
```

Windows:

```
Start > Programs > Oracle Application Server > OracleHome >  
Integrated Management Tools > Oracle Directory Manager
```

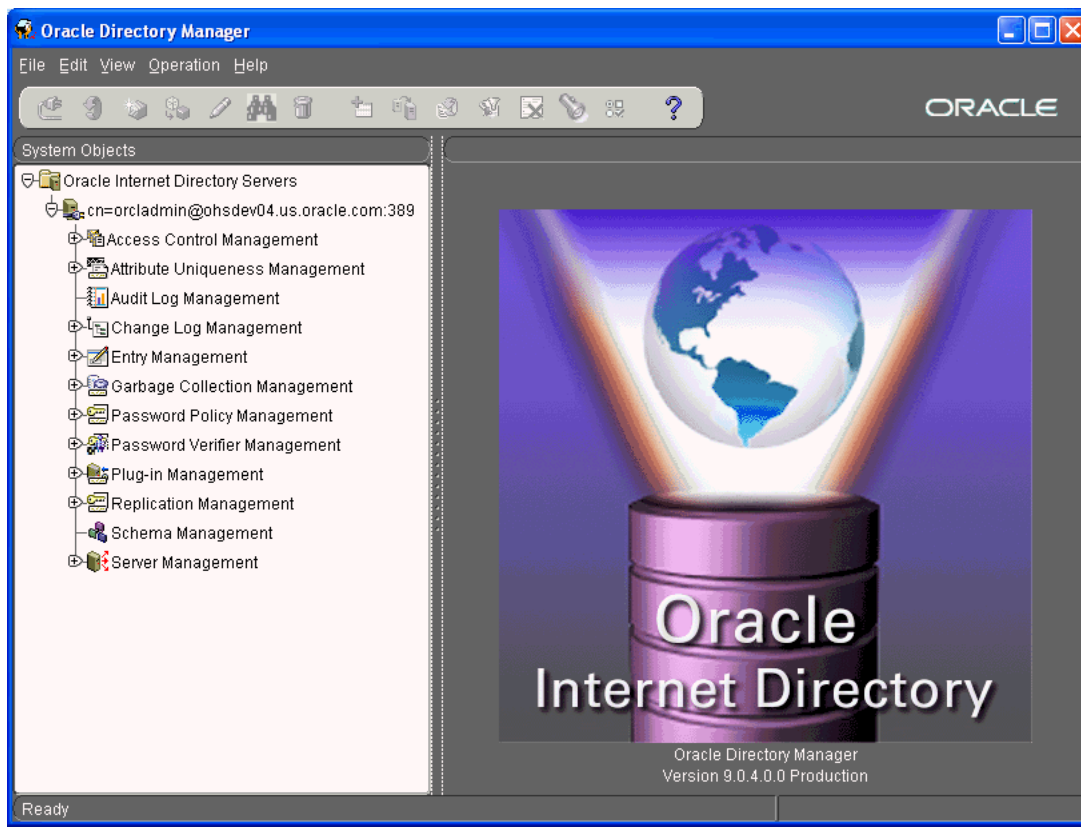
2. When you start Oracle Directory Manager, it will prompt you for connection information. Enter the following information to connect to your Oracle Internet Directory, typically hosted in the Oracle Collaboration Suite Database on your Oracle Collaboration Suite Infrastructure:

```
Host: <infrahost.yourdomain.com>  
Port: 389  
Username: cn=orcladmin  
Password: <password>
```

Port 389 is the default port used by Oracle Internet Directory. You may be using a different port. If so, enter the correct Oracle Internet Directory port.

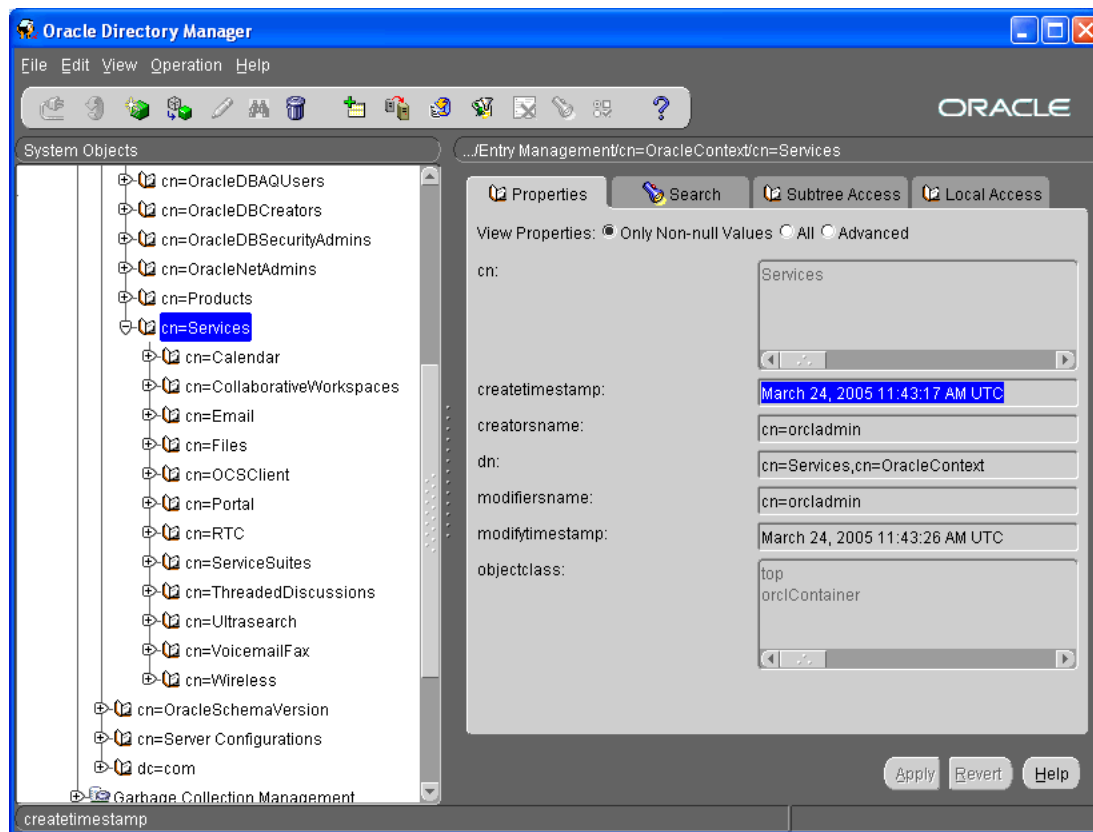
If you have configured your Oracle Internet Directory to be accessed using Secure Socket Layers (SSL), select the **SSL Enabled** checkbox. Otherwise, leave it blank.

3. Select **Login** to log in to the Oracle Internet Directory. When the connection is successful, the Oracle Internet Directory management screen is displayed. See [Figure 7-3, "Accessing Oracle Internet Directory with Oracle Directory Manager"](#) on page 7-11.

Figure 7–3 Accessing Oracle Internet Directory with Oracle Directory Manager

4. To access the Service Registry, drill down into the Oracle Internet Directory by selecting the following items in the System Objects pane:
 - a. Select Entry Management
 - b. Select cn=OracleContext
 - c. Select cn=Services

The System Objects pane displays a list of the Oracle Collaboration Suite applications which have entries in the Service Registry. The Properties tab displays the properties of the cn=Services object. See [Figure 7–4, "Displaying the Service Registry with Oracle Directory Manager"](#) on page 7-12.

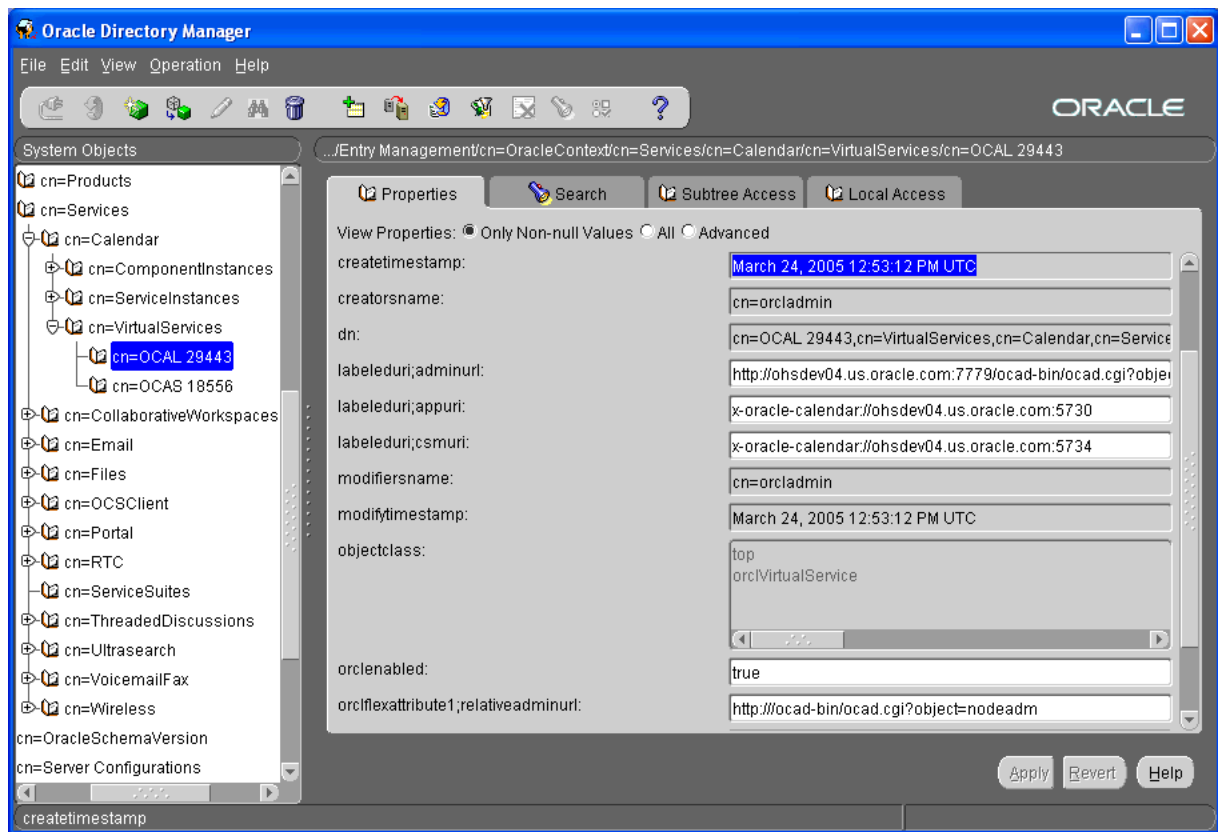
Figure 7–4 *Displaying the Service Registry with Oracle Directory Manager*

- To display URIs stored by each component in the Service Registry, select the component in the System Objects pane. Most components will contain a `cn=VirtualServices` object; this object contains one or more URIs used by other applications and OracleAS Portal to access that application. Applications store URIs in one or more child objects of the `cn=VirtualServices` object.

Note: The Oracle Universal Installer seeds the Oracle Internet Directory with objects for every Oracle Collaboration Suite application during installation, even if you do not configure and deploy every application. These unconfigured application entries will not contain child objects of their `cn=VirtualServices` objects. The child objects, and the URIs they store, are created in the Service Registry by each component's Configuration Assistant when it first runs.

See [Figure 7–5, "Oracle Calendar OCAL Virtual Services Object in the Service Registry"](#) on page 7-13 for an example of URIs stored in child objects of the `cn=VirtualServices` object. For illustrative purposes, the OCAL child object of Oracle Calendar is shown.

Figure 7-5 Oracle Calendar OCAL Virtual Services Object in the Service Registry



- Carefully edit application URIs stored in the Service Registry, according to the specific procedure you are following. For example, if you are creating a load-balanced cluster of Applications tiers for OCAS, edit the OCAS URIs to point to the new virtual host name of the load balancer.

When you have finished editing the properties of an object, select **Apply** to save the new values in Oracle Internet Directory. If you decide to reject the changes you have made, select **Revert** to reset the displayed attributes to those currently stored in the Oracle Internet Directory.

- Using `opmnctl` or Oracle Collaboration Suite Control, restart the Oracle Collaboration Suite Infrastructure and all Oracle Collaboration Suite Applications tiers, to clear caches that may still be storing the old URIs and to load the new URIs you have entered.

There is no need to restart the Oracle Collaboration Suite Database.

Managing Oracle Collaboration Suite Log Files

Each of the major components of Oracle Collaboration Suite records various important status and error messages in a variety of logs. As an administrator, one of your primary responsibilities is to monitor and maintain the log files. This chapter describes each of the log files used by Oracle Collaboration Suite, and how to view and manage them.

Oracle Collaboration Suite components generate log files containing messages that record all types of events, including startup and shutdown information, errors, warning messages, access information on HTTP requests, and additional information. This chapter describes how to view and manage log files to assist in monitoring system activity and in diagnosing system problems.

See Also: [Appendix B, "Default Locations of Component Log Files"](#)

This chapter contains the following topics:

- [Introduction to Oracle Collaboration Suite Logging](#)
- [Listing and Viewing Log Files with Oracle Collaboration Suite Control](#)
- [Searching Diagnostic Messages in a Log Repository](#)
- [Diagnosing Problems and Correlating Messages](#)
- [Using Oracle Collaboration Suite Log Loader](#)
- [Advanced Logging Topics](#)

Introduction to Oracle Collaboration Suite Logging

The Oracle Collaboration Suite Control lets you list and search log files across Oracle Application Server and Oracle Collaboration Suite components. You can view log files from the Oracle Collaboration Suite Control pages or download a log file to your local client and view the log files using another tool.

This section covers the following topics:

- [Understanding Log File Data and Naming](#)
- [Using a Log Repository](#)
- [Configuring Component Logging Options](#)

Understanding Log File Data and Naming

Several Oracle Collaboration Suite components use Oracle Diagnostic Logging (ODL). Using ODL, log file naming and the format of the contents of log files conforms to an Oracle standard and the diagnostic messages are written in XML. Some Oracle Collaboration Suite components do not use ODL, and write their diagnostic messages using a component specific text format. Regardless of the format of the messages that are stored in log files, ODL or text based, you can view log files using the Oracle Collaboration Suite Control, or you can download log files to your local client and view them using another tool (for example a text editor, or another file viewing utility).

This section covers the following topic:

- [ODL Message Formatting and ODL Log File Naming](#)

See Also: [Appendix B, "Default Locations of Component Log Files"](#) for a list of Oracle Collaboration Suite logs and their formats.

ODL Message Formatting and ODL Log File Naming

When Oracle Collaboration Suite components run and produce ODL messages, the messages are written to diagnostic log files using XML format. Each ODL message includes a `HEADER` element containing fields with information about the message, optionally a `CORRELATION_DATA` element containing information to assist in correlating messages across components, and a `PAYLOAD` element containing the message text, including optional arguments and associated values.

Using ODL, Oracle Collaboration Suite components write diagnostic log files to a logging directory and determine the names for logging directories using a component specific naming convention.

See Also:

- ["Understanding ODL Messages and ODL Log Files"](#) on page 8-15
- ["Correlating Messages Across Log Files and Components"](#) on page 8-10

Using a Log Repository

The Oracle Collaboration Suite Control supports viewing diagnostic messages from a Log Repository. A Log Repository can be file-based or stored in a database, and contains messages collected from multiple diagnostic log files across components. A Log Loader does not contain messages from access or trace log files because access logs and trace logs are verbose and do not contain diagnostic information.

The Oracle Collaboration Suite **Log Loader** component initializes and updates the data in a Log Repository. After the Log Loader starts, at regular intervals it stores information from diagnostic log files to the Log Repository.

Using a Log Repository consolidates Oracle Collaboration Suite log file data; this enables you to use the Oracle Collaboration Suite Control Console to easily search and view log file data generated by multiple components. Using a Log Repository can speed up the diagnostic process and reduce the resources required to support Oracle Collaboration Suite.

Note: By default, the Log Loader is not started. Use the Oracle Collaboration Suite Control Console or OPMN to start Log Loader.

See Also: ["Using Oracle Collaboration Suite Log Loader"](#) on page 8-11

Configuring Component Logging Options

Administrators configure logging options to manage and limit the logging information that Oracle Collaboration Suite components generate and save.

Note: The Oracle Collaboration Suite Control Console does not directly support configuring logging options. In many cases, to configure component logging options, you need to use the Oracle Collaboration Suite Control Console Advanced Server Properties page to edit the values in configuration files.

The logging configuration options include:

- **Specifying Log File Names and Pathnames:** Some Oracle Collaboration Suite components let you specify the directory for storing diagnostic log files. Specifying the diagnostic logging directory allows you to manage system and network resources.
- **Limiting Log File Size:** As Oracle Collaboration Suite components run and generate diagnostic messages, the size of the log files increases. Oracle Collaboration Suite components use one of several strategies to deal with log file size. Some components allow log files to keep increasing in size; in this case it is the administrator's responsibility to monitor and cleanup the log files. Other components, including OC4J applications, let you specify configuration options that limit how much log file data is collected and saved.
- **Using Log File Archiving:** Certain Oracle Collaboration Suite components let you specify configuration options to control the size of diagnostic logging directories. This lets you determine a maximum size for the directories containing a component's log files. When the maximum size is reached, older logging information is deleted before newer logging information is saved.
- **Setting Component Logging Levels:** Certain Oracle Collaboration Suite components, including Oracle HTTP Server, allow administrators to configure logging levels. By configuring logging levels, the number of messages saved to diagnostic log files can be reduced. For example, you can set the logging level so that the system only reports and saves critical messages.

See Also: Oracle Collaboration Suite component Administrator's Guides for information on setting logging configuration options.

Listing and Viewing Log Files with Oracle Collaboration Suite Control

Use the Oracle Collaboration Suite Control to list log files by selecting the **Logs** link on the Oracle Collaboration Suite Control Console. This brings up the View Logs page.

See Also: ["Using the printlogs Tool to View Log Messages"](#) on page 8-15 for information on a command-line tool for viewing log files

This section covers the following:

- [Listing Log Files for Components](#)
- [Listing Log Files from Oracle Collaboration Suite Components Pages](#)

- [Using Log Files Advanced Search](#)

Listing Log Files for Components

Selecting the **Logs** link on the Oracle Collaboration Suite Control Console shows the View Logs page. To list the log files, from the View Logs page, perform the following steps:

1. To view all components, select **Move All** to move all available components to **Selected Components**. To view some components, select them in the Available box and click **Move**.
2. Select **Search** to list the log files for the selected components.
3. After the search returns, the **Results** section shows log file information such as the name of the component associated with a log file and a link to the log file.

Figure 8–1 shows the Oracle Collaboration Suite Control Console View Logs page after a search.

Figure 8–1 Oracle Collaboration Suite Control Console View Logs Search Results

ORACLE Enterprise Manager 10g
Application Server Control for Collaboration Suite

Topology Preferences Help

Farm > Application Server: ocs14.mcarrer-sun.us.oracle.com >

View Logs

Page Refreshed Jun 25, 2005 6:22:16 PM

Log Files Search Log Repository

The Log Files tab lists the log files for this application server. View a log file by clicking on the Log File name in the search results table.

Simple Search

Available Components

- ADF Business Components
- ASCLONE
- Backup/Recovery
- Calendar Application System
- DCM
- Email Application
- Enterprise Manager
- Files
- HTTP_Server
- LogLoader

Selected Components

- OCSCIENT
- OPMN

Move Move All Remove Remove All

Search

Advanced Search

Results: 4 Log Entries Retrieved

Component Type	Component Name	Log Type	Log File	Modified	Size (bytes)
OCSCIENT	OCSCIENT	Trace	ocscient0.0.log	June 15, 2005 9:28:08 PM EDT	126603
OPMN	Process Manager	Error	ipm.log	June 20, 2005 11:18:02 AM EDT	18281
OPMN	Notification Manager	Error	ons.log	June 25, 2005 6:20:41 PM EDT	710518
OPMN		Server	redirected output/errors	June 20, 2005 11:15:12 AM EDT	918

Topology Preferences Help

Copyright © 1996, 2005, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control for Collaboration Suite

Listing Log Files from Oracle Collaboration Suite Components Pages

After you select a system component link on the Oracle Collaboration Suite home page, you can view the log files for the selected component by clicking **Logs** at the top

of the page. When you click **Logs**, the Oracle Collaboration Suite Control searches for the log files associated with the current component. You can then view the log files on the resulting View Logs page by selecting the Log File links shown in the **Results** section of the page.

For example, if you click **Logs** on the HTTP Server Home page, then Enterprise Manager searches for the log files associated with the Oracle HTTP Server and displays the View Logs page with a list of Oracle HTTP Server log files in the Results section of the page.

When you select the **Logs** link from a component page, the log file pages include a **Return to** link at the bottom of each page. The **Return to** link returns you to the component page from which you selected the **Logs** link.

Using Log Files Advanced Search

After you select the **Logs** link on an Oracle Collaboration Suite Control page, the View Logs page is shown. Clicking **Advanced Search** shows the View Logs Advanced Search page. The Advanced Search page lets you list log files for Oracle Collaboration Suite components and enables you to filter the search for log files by certain log file attributes.

Starting on the View Logs Advanced Search page you can list log files using a search filter by performing the following steps:

1. Select the desired components from the **Available Components** box by clicking **Move** or **Move All** to move components to the **Selected Components** box.
2. Select a field from the **Log File Attribute** list.
3. Click **Add Row** to add a row for the selected log file attribute.
4. Enter the desired search value in the **Value** field.
5. If you want to select additional fields with values, click **Add Another Row** and enter additional values.
6. Click **Search** to perform the search. When the search returns, the **Results** section shows log files with matching fields.

To obtain more information on filtering using log file attributes, click the information icon next to the **Log File Attribute** list.

Figure 8–2 shows the Advanced Search Filter By Log File Attributes selection box, with the **Log File Attribute** list and the **Add Another Row** button.

Figure 8–2 Log Files Advanced Search Filter By Log File Attributes

Filter By Log File Attributes

Attribute	Value	Delete
Component Type	HTTP Server	
Log File Attribute	OPMN Process Set	Add Another Row

TIP Log Attribute values containing spaces should be enclosed in single quotation marks.

Search

Searching Diagnostic Messages in a Log Repository

The Oracle Collaboration Suite Control lets you search through diagnostic messages in a Log Repository containing messages collected from several Oracle Collaboration Suite components. The advantage of using a Log Repository is that you can search, view, and correlate diagnostic messages in a uniform way across multiple Oracle Collaboration Suite components.

This section covers the following topics:

- [Getting Started with Log Repository](#)
- [Searching Log Repository with Simple Search](#)
- [Searching Log Repository with Advanced Search](#)
- [Viewing Repository Log Entry Details](#)
- [Using Regular Expressions With Log Repository Search](#)

Getting Started with Log Repository

To use a Log Repository for searching and viewing diagnostic messages, select the **Logs** link on an Oracle Collaboration Suite Control page and then select the **Search Log Repository** link. The Search Log Repository Simple Search and Advanced Search pages allow you to search the diagnostic messages stored in the Log Repository.

[Figure 8–3](#) shows the Oracle Collaboration Suite Control Search Log Repository page.

The Log Repository needs to contain diagnostic messages before you can search the Log Repository. The Log Loader component initializes and updates the diagnostic messages in the Log Repository.

Note: By default, the Oracle Collaboration Suite Log Loader is not started and does not contain any diagnostic messages.

See Also: ["Using Oracle Collaboration Suite Log Loader"](#) on page 8-11 for information on starting and using Log Loader

Searching Log Repository with Simple Search

To search the Log Repository for diagnostic messages, go to the View Logs > Search Log Repository page, and use the **Available Components** and **Selected Components** boxes to select components. The online help describes the available search and display options for the Search Log Repository page.

To search for diagnostic log entries in the Log Repository, do the following:

1. Select components from the **Available Components** box (optional). Select components and then click **Move** or **Move All** to move the selected components to the **Selected Components** box. This step is optional.
2. Use the default selections, or select the available search and result display options. The online help describes the available search and display options for the Search Log Repository page.
3. Click **Search** to search for messages in the Log Repository that match the constraints you specify. When the search returns, the Results section shows the matching diagnostic log messages from the Log Repository.

[Figure 8–3](#) shows the Search Log Repository page.

Note: The **Message Type** selection box includes the Unknown option. Some components do not include a message type when the component writes log file entries. These messages are loaded into the Log Repository with Unknown specified as the message type.

See Also: ["Viewing Repository Log Entry Details"](#) on page 8-8

Figure 8–3 Search Log Repository Page

ORACLE Enterprise Manager 10g
Application Server Control

Application Server: portal_m16.iasdocs1.us.oracle.com > View Logs

View Logs

Page Refreshed Sep 19, 2003 3:51:33 PM

Log Files **Search Log Repository**

The Search Log Repository tab allows you to query the Log Repository. The Log Repository contains diagnostic log entries that are periodically loaded by the Log Loader. **Log Loader**

Simple Search

Available Components

- BC4J
- Enterprise Manager
- HTTP_Server
- OC4J_Portal
- OC4J_Wireless
- OPMN
- Port Tunneling
- Web Cache
- Wireless
- home

Selected Components

- DCM
- LogLoader

Message Types

- ☒ Internal Error
- ☒ Warning
- ☒ Trace
- ☒ Error
- ☒ Notification
- ☒ Unknown

Message Text

☐ Regular Expression

Maximum Entries Retrieved

Entries Per Page

☒ Load logs before performing search

Date Range

☒ Most Recent Days

☐ Time Interval

Start Date End Date

(Example: 12/15/02) (Example: 12/17/02)

Start Time AM ☐ PM End Time AM ☐ PM

Search

Results: 16 Log Entries Retrieved

Select Log Entries and...

[Select All](#) | [Select None](#)

Select	Time	Component	Message Type	Module	Message Text
☐	September 18, 2003 10:12:31 AM PDT	DCM	Error	oracle/defaultLogger/ExceptionLogger	principals specified in application is not a valid path: /private/mid_deployments/portalTools/principals.xml
☐	September 18, 2003 10:12:32 AM PDT	DCM	Error	oracle/defaultLogger/ExceptionLogger	principals specified in application is not a valid path: /private/mid_deployments/webclipping/principals.xml

Searching Log Repository with Advanced Search

To search the Log Repository for diagnostic messages using advanced search, go to the View Logs > Search Log Repository page, and click **Advanced Search**. On the Search Log Repository Advanced Search page, use the **Filter By Log Entry Fields** box to select log message fields and values to search. When you click **Search**, Enterprise Manager

displays on the View Logs page a list of the log repository messages that match the log message field values you specified.

The View Logs pages shows the diagnostic log entries with matching field values which you enter after you click **Search**.

To display Log Repository entries matching the **Advanced Search** filter, perform the following steps:

1. Use the default selections, or specify search and result date range and message type options by making selections and entering constraints on the Search Log Repository Advanced Search page.
2. Select log entries with specified field values using the **Filter by Log Entry Fields** box. Select multiple fields by clicking **Add Another Row**. When you specify values for multiple fields, the search only returns results that match all of the specified constraints. The online help describes the available search and display options for the Search Log Repository page.
3. Click **Search** to search for messages in the Log Repository that match the selection constraints. When the search returns, the Results section shows the matching log entries.

Figure 8–4 shows the Advanced Search Log Repository **Filter By Log Entry Fields** box.

Figure 8–4 Search Log Repository Advanced Search Filter By Log Entry Fields

Field	Value	Regular Expression	Delete
Message Text	Create	☐	

Log Entry Field: Organization ID Add Another Row

See Also: ["Viewing Repository Log Entry Details"](#) on page 8-8

Viewing Repository Log Entry Details

Using either the link shown in the Time field of the Results area on the View Logs page, or by selecting entries in the **Select** field and then selecting **View Details**, you can view a log entry and its associated information, including the Message Type, Component, the Message Text, and optionally the Execution Context ID (ECID).

Figure 8–5 shows a log entry details page.

Figure 8–5 Log Repository Log Entry Details Page

ORACLE Enterprise Manager 10g
Application Server Control

Application Server: [portal_m16.iasdocs1.us.oracle.com](#) > [View Logs](#) > Log Entry Details

Log Entry Details

Page Refreshed **Sep 19, 2003 4:03:45 PM**

Log Entry: September 18, 2003 10:12:31 AM PDT

Component	DCM
Message Type	Error
Module ID	oracle/defaultLogger/ExceptionLogger
User ID	midtier3
Host Name	iasdocs1.us.oracle.com
Host Network Address	139.185.140.30
Process/Thread ID	null-Thread[Deamon Worker for TaskMaster of iAS instance at: /private/midtier3 JVM Id = 1c9b9ca.f7b20e22f7.8000,5,main]
Message Level	1
Execution Context ID	139.185.140.30:75398:1063905150256:0

(The Execution Context is a globally unique identifier associated with a thread of execution. It is used to correlate messages from one or more application server components. Click this link to display the log entries with this Execution Context.)

Message Text

principals specified in application is not a valid path: /private/midtier3/j2ee/OC4J_Portal/config/.application-deployments/portalTools/principals.xml

See Also: "Diagnosing Problems and Correlating Messages" on page 8-9 for information on Execution Context IDs

Using Regular Expressions With Log Repository Search

Regular expression matching is applied when the checkbox in the Regular Expression field is selected on the Log Repository Simple Search or Advanced Search page. On the Simple Search page, the Regular Expression checkbox is under the Message Text field. On the Advanced Search page, the Regular Expression checkbox is in the **Filter by Log Entry Fields** box. Using a regular expression in a search enables you to enter a pattern description that enables you to match strings for a Log Repository search.

The Log Repository search uses the Apache Jakarta regular expression engine which uses "*" for a string of characters, "?" for a single character, and supports boundary matches, including "^" for a match only at the beginning of an entry, and "\$" for a match only at the end of an entry, and special characters, including "\t" for Tab, "\n" for newline, "\r" for return, and "\f" for form feed.

See Also: <http://jakarta.apache.org/regexp> for more information on supported regular expressions

Diagnosing Problems and Correlating Messages

Generally administrators and others view log file data to diagnose, monitor, and search for component errors or problems that may cause component errors. The Oracle Collaboration Suite Control Console supports a unified architecture and provides cross component tools that can assist you in these tasks.

This section covers the following topics:

- [Correlating Messages Across Log Files and Components](#)
- [Diagnosing Component Problems](#)

Correlating Messages Across Log Files and Components

Certain Oracle Collaboration Suite components provide **message correlation** information for diagnostic messages. Message correlation information helps those viewing diagnostic messages determine relationships between messages across components. The Execution Context ID (ECID), is a globally unique identifier associated with a thread of execution. The ECID helps you to use log file entries to correlate messages from one application or across application server components. By searching related messages using the message correlation information, multiple messages can be examined and the component that first generates a problem can be identified (this technique is called **first-fault component isolation**). Message correlation data can help establish a clear path for a diagnostic message across components, within which errors and related behavior can be understood.

When you view an entry on the Log Entry Details page in the Oracle Collaboration Suite Control Console, if the Execution Context ID field is available, it displays the Execution Context ID as a link. Selecting the **Execution Context ID** link shows you all the diagnostic messages in the Log Repository with the same execution context ID.

You can use the ECID to track requests as they move through Oracle Application Server.

The ECID takes the following format:

request_id, sequence_number

The *request_id* is a unique integer that is associated with each request. The *sequence_number* represents the hop number of the request, as it passes through Oracle Collaboration Suite (or through the component). For example, OracleAS Web Cache assigns an initial sequence number of 0 to a request (when OracleAS Web Cache handles the request). After that, the sequence number is incremented as the request moves through Oracle Collaboration Suite components.

Table 8–1 lists the Oracle Collaboration Suite components that provide message correlation information (using an ECID).

Note: Some Oracle Collaboration Suite components do not support generating message correlation data. Other Oracle Collaboration Suite components support generating message correlation data, but by default do not enable this option.

Table 8–1 Oracle Collaboration Suite Components Supporting Message Correlation

Component	Message Correlation Configuration Reference
DCM	DCM supports message correlation.
OC4J	OC4J supports message correlation when ODL logging is enabled and when the property <code>oracle.dms.transtrace.ecidenabled</code> is set to the value <code>true</code> (by default this is <code>false</code>). This property is set on the OC4J command line. See Also: "Configuring Components to Produce ODL Messages and ECIDs" on page 8-19 <i>Oracle Application Server Containers for J2EE User's Guide</i> for details on enabling ODL logging in OC4J

Table 8–1 (Cont.) Oracle Collaboration Suite Components Supporting Message Correlation

Component	Message Correlation Configuration Reference
HTTP Server	Oracle HTTP Server supports message correlation. See Also: "Configuring Components to Produce ODL Messages and ECIDs" on page 8-19
Portal	Portal supports message correlation. Portal outputs the ECID with error messages in the Portal Repository Diagnostics log file. See Also: "Diagnosing OracleAS Portal Problems" <i>Oracle Application Server Portal Configuration Guide</i> .
Web Cache	Web Cache supports message correlation. See Also: "Oracle-ECID Request-Header Field" in Chapter 2 of <i>Oracle Application Server Web Cache Administrator's Guide</i>

Diagnosing Component Problems

When an Oracle Collaboration Suite component has a problem you can isolate and determine the cause of the problem by viewing the diagnostic messages. There are general techniques that can assist you in accomplishing this task. In general, the techniques include the following:

- Search for errors, or warnings, related to the problem
- Correlate the errors across components
- Correlate the errors across a time interval
- Perform component based analysis

Using a Log Repository can make searching for the root cause of a problem much easier. A Log Repository consolidates log file data and enables you to easily search, correlate, and view log file data that is generated by multiple Oracle Collaboration Suite components. A Log Repository correlates cross component information by time, and correlates events that occur in a cascading fashion. Once a problem is isolated to a particular component in the repository, then, if needed, the problem can be further analyzed by examining the component-specific diagnostic files.

See Also: ["Using Oracle Collaboration Suite Log Loader"](#) on page 8-11

Using Oracle Collaboration Suite Log Loader

The Oracle Collaboration Suite **Log Loader** component is a process that periodically updates a Log Repository. A Log Repository stores diagnostic messages read from multiple log files across Oracle Collaboration Suite components in a single Oracle home. After the Log Loader starts, at regular intervals it reads the contents of log files incrementally and writes the contents to the Log Repository.

This section covers the following topics:

- [Starting and Stopping Log Loader](#)
- [Enabling and Disabling Log Loader](#)
- [Updating the Log Configuration](#)
- [Setting Log Loader Properties](#)
- [Understanding Log Loader Diagnostic Messages](#)

Starting and Stopping Log Loader

You can use the controls on the Oracle Collaboration Suite Control Console Log Loader page to start and stop the Log Loader. Starting the Log Loader starts a process that periodically updates the Log Repository. Stopping the Log Loader stops the process that periodically updates the Log Repository.

Note: By default, when Oracle Collaboration Suite is installed, the Log Loader is stopped.

To start the log loader, perform the following steps:

1. Select the **Logs** link on any Oracle Collaboration Suite Control Console page.
2. From the View Logs page, select the **Search Log Repository** link.
3. Select **Log Loader** on the View Logs page.
4. On the Log Loader page, click **Start**.
5. On the confirmation page click either **Cancel**, **Start**, or **Start and Load Existing Logs**. Click **Cancel** to cancel, click **Start** to start the Log Loader, and click **Start and Load Existing Logs** to start and initialize the log repository with the existing log messages.

See Also: ["Searching Diagnostic Messages in a Log Repository"](#) on page 8-6

Enabling and Disabling Log Loader

On the Log Loader page, the **Enable** button enables the Log Loader. By default, when you first install Oracle Collaboration Suite, the Log Loader is enabled, but not started. When you disable the Log Loader, Enterprise Manager stops the Log Loader and the Log Loader component does not appear in the list of components on the View Logs page.

When you enable the Log Loader, the Log Loader component appears in the components list on the View Logs page, but it is not started.

Updating the Log Configuration

When the Log Loader starts, it loads configuration information about the component log files it will use as sources for the diagnostic messages that are stored in the Log Repository (this includes information on the location and format of the log files).

Most log configuration files are installed when Oracle Collaboration Suite components are configured. The log configuration files for HTTP Server, OPMN, OC4J and the Log Loader are generated when the Log Loader is initially started.

If configuration changes are made that effect the location of diagnostic log files for these components, use the **Update Log Configuration** button to regenerate the log configuration files for these components. This will ensure the Log Loader is loading the correct set of logs into the Log Repository.

See Also: ["Component Diagnostic Log File Registration"](#) on page 8-18

Setting Log Loader Properties

You can set Log Loader properties from the Log Loader page. To navigate to the Log Loader page:

1. Select the **Logs** link on any Oracle Collaboration Suite Control Console page.
2. From the View Logs page, select the **Search Log Repository** link.
3. Click **Log Loader** on the View Logs page.
4. Select the **Log Loader Properties** link in the Administration section. The Log Loader Properties page includes fields showing the current values for the Log Loader properties.

To change the Log Loader properties, perform the following steps:

1. Enter updated values in the appropriate fields on the Log Loader Properties page.
2. Click **Apply** to apply the new values.

Figure 8–6 shows the Oracle Collaboration Suite Control Console Log Loader Properties page.

The Oracle Collaboration Suite Control Console online help includes detailed information on the Log Loader Properties fields.

Figure 8–6 Log Loader Properties Page

ORACLE Enterprise Manager 10g Application Server Control for Collaboration Suite [Topology](#) [Preferences](#) [Help](#)

[Farm](#) > [Application Server: ocs14.mccarrer-sun.us.oracle.com](#) > [View Logs](#) > [Log Loader](#) >

Log Loader Properties

Page Refreshed Jun 25, 2005 6:31:53 PM

These properties can be used to control the behavior of the Log Loader and the size of the Log Repository it updates.

Location of Log Repository	diagnostics/repository	(This property identifies the directory where the Log Repository is located.)
Maximum size of Log Repository (MB)	50	(The total size of the Log Repository is controlled by this property.)
Size of each segment (MB)	5	(The Log Repository is a set of files called segments. Segments are reused to control the size the the repository.)
Interval between loads (Minutes)	5	(This property defines how often the Log Loader reads component log files and updates the Log Repository.)
Maximum load size (KBytes)	51200	(The Log Loader may skip the loading of some log entries if a log file has grown very large since it was last loaded. This property controls the maximum number of bytes that may be loaded from a file or set of ODL files during a run of the Loader.)
Log Loader Port	44001	(This property identifies the communication port used by the Log Loader.)

[Revert](#) [Apply](#)

[Topology](#) | [Preferences](#) | [Help](#)

Copyright © 1996, 2005, Oracle. All rights reserved.
[About Oracle Enterprise Manager 10g Application Server Control for Collaboration Suite](#)

Understanding Log Loader Diagnostic Messages

The Log Loader logs its diagnostic messages, including errors to its log file. Diagnostic messages might include errors encountered due to an incorrect configuration, or errors that occur while the Log Loader is reading data from a log file or is writing data to the log repository.

The common Log Loader problems include:

- Errors in the Log Loader configuration file (`$ORACLE_HOME/diagnostics/config/logloader.xml`). Errors in the configuration file usually prevent the Log Loader from running. Such errors need to be corrected before the Log Loader can work properly.
- Configuration errors that occur when a component's registration file contains errors (`$ORACLE_HOME/diagnostics/config/registration/*.xml`). Errors in the registration files do not prevent the Log Loader from running but may prevent the contents of certain log files from being loaded in the repository. Typically, there are two common types of registration file errors:
 - XML syntax errors that prevent the file from being parsed. If such errors are encountered, the Log Loader completely ignores the contents of the file.
 - A wrong path specified for a configuration file. If the Log Loader cannot find a log file at the specified path, it issues a Warning level diagnostic message. This does not always indicate an error. For example, it is possible that the component that generates that log was not active when the Log Loader started and the log file had not been created yet. The Log Loader continues to look for the log file and starts reading messages when the log file is created.
- Errors may occur while the Log Loader is reading messages from a log file. If the log file includes contents that cannot be read or parsed, then the Log Loader issues a log message indicating that it cannot read part of the contents of the file. In this case, the Log Loader attempts to recover from the error and continue to read the Log File.
- Errors may occur when writing messages to the repository (for example, a disk error). This type of error may indicate a problem that may require attention from the system administrator to correct the problem.
- The Log Loader produces an error message when it skips reading log files because a log file exceeds the currently specified maximum load size. The maximum load size can be specified on the Log Loader properties page.

In this case the Log Loader logs an error message in the following format:

```
Size of data to be read from log /logfile exceeds threshold of x bytes.  
Skipping y_skipped bytes and moving to end of log.
```

This message indicates the size of data to be read exceeds the specified maximum load size *x*, and that the Log Loader is skipping to the end of the log file. The error message provides information on the name of the log file */logfile*, and the number of bytes skipped *y_skipped*.

Advanced Logging Topics

This section covers the following topics:

- [Using the printlogs Tool to View Log Messages](#)
- [Understanding ODL Messages and ODL Log Files](#)

- [Understanding Log Loader Log File Format Conversion](#)
- [Component Diagnostic Log File Registration](#)
- [Configuring Components to Produce ODL Messages and ECIDs](#)
- [Creating and Managing a Diagnostic Message Database Repository](#)
- [Limitations and Configuration](#)

Using the printlogs Tool to View Log Messages

The `printlogs` tool is a command-line alternative to the Oracle Collaboration Suite Control Console for viewing log messages. `printlogs` supports a variety of options for gathering and filtering log messages, and prints the results to standard output in a single format. For example, you can use `printlogs` to:

- Read log messages from the Log Repository or individual log files
- Filter log messages according to timestamp or log field value
- Print log messages in ODL or text format
- Sort log messages by field
- Report the number of log messages of a specified type
- Run in a continuous loop, printing log reports and sleeping for a specified amount of time

See Also: *Oracle Application Server Administrator's Guide* Appendix F for more information

Understanding ODL Messages and ODL Log Files

This section covers the following topics:

- [ODL Message Contents](#)
- [ODL Log File Naming](#)

ODL Message Contents

Using ODL, diagnostic messages are written to log files using XML format and each message includes a `HEADER` element containing information about the message, optionally a `CORRELATION_DATA` element containing information to assist in correlating messages across components, and a `PAYLOAD` element containing the message text including optional arguments and associated values.

[Example 8-1](#) shows a sample ODL format message that includes the optional `CORRELATION_DATA` element.

Example 8-1 Sample ODL Message Content

```
<MESSAGE>
  <HEADER>
    <TSTZ_ORIGINATING>2002-04-01T18:38:48.058-08:00</TSTZ_ORIGINATING>
    <ORG_ID>oracle.com</ORG_ID>
    <COMPONENT_ID>OHS</COMPONENT_ID>
    <HOSTING_CLIENT_ID>0.0.255.255</HOSTING_CLIENT_ID>
    <MSG_TYPE TYPE="ERROR"></MSG_TYPE>
    <MSG_LEVEL>17</MSG_LEVEL>
    <HOST_ID>test-perf9</HOST_ID>
    <HOST_NWADDR>0.0.255.255</HOST_NWADDR>
```

```

    <MODULE_ID>apache_core</MODULE_ID>
    <PROCESS_ID>5713</PROCESS_ID>
  </HEADER>
  <CORRELATION_DATA>
    <EXEC_CONTEXT_ID>
      <UNIQUE_ID>1017715128:255..255.255.88:5713:0:1</UNIQUE_ID>
      <SEQ>1</SEQ>
    </EXEC_CONTEXT_ID>
  </CORRELATION_DATA>
  <PAYLOAD>
    <MSG_TEXT>File does not exist:
    /files/Apache/docs/images/java-apache-project.gif
    </MSG_TEXT>
  </PAYLOAD>
</MESSAGE>

```

Table 8–2 describes the contents of an ODL message header. For any given component that produces ODL format messages, the optional header fields may not be present in the generated diagnostic messages.

Table 8–2 ODL Format Message Header Fields

Header Field Name	Description	Required
COMPONENT_ID	Specifies the product or component ID for the component that originated the message.	Required
HOST_ID	Specifies the DNS host network ID.	Optional
HOST_NWADDR	Specifies the IP or other network address for the originating host.	Optional
HOSTING_CLIENT_ID	Specifies the ID of the client or security group that the message relates to.	Optional
MODULE_ID	Specifies the ID for the module that originated the message.	Optional
MSG_GROUP	Name of the group the message belongs to, for purposes of selecting similar messages.	Optional
MSG_ID	Specifies the message ID. The message ID uniquely identifies the message.	Optional
MSG_LEVEL	Specifies an integer value that qualifies the message type (MSG_TYPE). Lower level values are for higher severity errors. Valid Values: 1 - 32	Optional
MSG_TYPE	Specify the type of the message, which is one of: INTERNAL_ERROR, ERROR, WARNING, NOTIFICATION, TRACE, UNKNOWN. If MSG_TYPE is included, the TYPE attribute is required when MSG_TYPE is included in the message header.	Required
ORG_ID	Specifies the organization ID, for the originating component. This is usually the domain name for the organization.	Optional
PROCESS_ID	Specifies the process ID for the process, or execution unit associated with the message. Java components may use this field to specify the process ID and the thread ID, or only the thread ID.	Optional
TSTZ_NORMALIZED	Timestamp normalized for clock drift across hosts. This field is used when the diagnostic message is copied to a repository in a different hosts.	Optional
TSTZ_ORIGINATING	Timestamp with local time zone. This specifies the date and time when the message was generated.	Required
USER_ID	Specifies the User ID associated with the message.	Optional

ODL Log File Naming

Using ODL, Oracle Collaboration Suite components write diagnostic log files to a logging directory. Components determine the names for logging directories using a component specific naming convention.

An **ODL log** is a set of log files that includes: the current ODL log file, typically named `log.xml`, and zero or more **ODL Archives (segment files)** that contain older messages. As the log file grows, new information is added to the end of the log file, `log.xml`. Each ODL log can specify a maximum segment size. When the log file reaches the maximum segment size, it is renamed and a new log file, `log.xml` is created (specify the maximum ODL segment size using component-specific configuration options).

Note: Some Oracle Collaboration Suite components, including Oracle HTTP Server, do not support the ODL log file naming mechanism that this section describes. In Oracle HTTP Server, ODL diagnostic messages are written to a file, `log.xml`, that does not have a configurable size limit.

Segment files are created when the ODL log file `log.xml` reaches the maximum segment size. That is, the `log.xml` is renamed to `log $n$ .xml`, where n is an integer, and a new `log.xml` file is created when the component generates new diagnostic messages.

To limit the size of the ODL log, components use a configuration option specifying the maximum size of the logging directory. Whenever the sum of the sizes of all of the files in the directory reaches the maximum, the oldest archive is deleted to keep the total size under the specified limit.

Note: The most recent segment file is never deleted.

For example, when the maximum directory size is reached, with the starting segment file named `log9872`, the following files could be present in the log file directory:

File	Size
<code>log.xml</code>	10002
<code>log9872.xml</code>	15000
<code>log9873.xml</code>	15000
<code>log9874.xml</code>	15000
<code>log9875.xml</code>	15000
<code>log9876.xml</code>	15000

In this case, when `log.xml` fills up, `log9872.xml` is removed and `log.xml` is moved to the new file `log9877.xml`; new diagnostic messages then are written to a new `log.xml`.

Using ODL provides the following benefits:

- Limits the total amount of diagnostic information saved
- Older segment files are removed and newer segment files are saved in chronological fashion
- Components can remain active, and do not need to be shutdown, when diagnostic logging files are cleaned

Understanding Log Loader Log File Format Conversion

The Log Loader reads logs in several different formats and it converts the contents of non-ODL logs to ODL format. In most cases, the resulting ODL log record will contain only a timestamp and the message text from the original log entry. Values for other ODL message fields, such as `COMPONENT_ID` and `MODULE_ID` can be provided in the log registration file for each log, so that these values are set to all log records parsed from the log. The Log Loader attempts to determine the severity or level of each non-ODL log and generate an appropriate ODL message type. However, in many cases, if the severity or level cannot be determined, the resulting ODL log record will have the message type set to `UNKNOWN`.

The Log Loader can even read "unformatted" logs, that may not even contain timestamp values. This is the case for several logs in the `$ORACLE_HOME/opmn/logs` directory which contain redirected output from Oracle Collaboration Suite processes managed by Oracle Process Manager and Notification Server (including most Oracle Collaboration Suite applications). When log entries do not contain a timestamp, the Log Loader will set the timestamp to the value of the "last known timestamp" for that log. The value of the last known timestamp is determined according to the following rules:

1. The initial value of the last known timestamp is zero. Note that whenever adding a log record to the repository, a zero value timestamp will be converted to the current time.
2. If the Log Loader finds an Oracle Process Manager and Notification Server generated timestamp it will set the last known timestamp with its value.
3. When the Log Loader reaches the end of the log, it sets the last known timestamp with the current time. If the Log Loader is running regularly, such as once every five minutes, this will result in timestamps that are approximate to the actual time the message was written within a five minute range. If the Log Loader is not run frequently, the value of these timestamps could be inaccurate.

Note: The OC4J redirected logs found in the `$ORACLE_HOME/opmn/logs` directory are not treated as "unformatted" logs, since each line in the OC4J logs contains a timestamp. Most other logs in this directory are treated as unformatted logs, and will have timestamps assigned according to the preceding rules.

Component Diagnostic Log File Registration

The Oracle Collaboration Suite Control Console and the Log Loader read Oracle Collaboration Suite component diagnostic registration files to determine names, locations, and additional configuration information about diagnostic log files. The directory `$ORACLE_HOME/diagnostics/config/registration` contains the diagnostic log file registration files.

Oracle Collaboration Suite components may have multiple registration files in the configuration registration directory.

The format for the registration files includes a Oracle Collaboration Suite component ID, and extension, `.xml`. [Table 8–3](#) lists the Oracle Collaboration Suite Components and their associated Component IDs.

Note: Components are responsible for creating the component diagnostic registration files. Normally, Oracle Collaboration Suite administrators should not modify these files.

Table 8–3 *Component IDs For Diagnostic Log File Configuration*

Component Name	Component ID
ADF	ADFBC
DCM	DCM
Discoverer	DISCOVER
Enterprise Manager	EM
HTTP Server	OHS
Infrastructure Database	RDBMS
Internet Directory	OID
Listener for Infrastructure Database	LISTENER
Log Loader	LOGLOADER
OC4J	OC4J
OPMN	OPMN
Port Tunneling	IASPT
Portal	PORTAL
Single Sign-On	SSO
TopLink	TOPLINK
Ultra Search	ULTRSRCH
Universal Installer	OUI
Voicemail & Fax	VMAILFAX
Web Cache	WEBCACHE
Oracle Mobile Collaboration	WIRELESS

Configuring Components to Produce ODL Messages and ECIDs

[Table 8–4](#) lists the Oracle Collaboration Suite components that support ODL messages but that generate text messages by default. By making configuration changes, these components can be configured to produce ODL messages and for OC4J, an ECID.

This section covers the following topics:

- [Configuring Oracle HTTP Server to Produce ODL Messages](#)
- [Configuring OC4J to Produce ODL Messages](#)
- [Configuring OC4J to Produce ECIDs](#)

Table 8–4 Oracle Application Server Components with Configuration Options for Supporting ODL

Component	Default Format	ODL Support	Location ¹
HTTP Server	Text	Yes	<code>ORACLE_HOME/Apache/Apache/logs</code>
OC4J Instance	Text	Yes	<code>ORACLE_HOME/j2ee/instance_name/log</code> <code>ORACLE_HOME/j2ee/application-deployments/application_name/application.log</code>

¹ Locations are shown in UNIX format. Invert the slashes for Windows format.

Configuring Oracle HTTP Server to Produce ODL Messages

To configure the Oracle HTTP Server to produce ODL messages, perform the following steps:

1. Add a directory named `oracle` where the Oracle HTTP Server ODL messages will be stored. The directory should be located at the following location:

 (UNIX) `ORACLE_HOME/Apache/Apache/logs`
 (Windows) `ORACLE_HOME\Apache\Apache\logs`
2. Using the Oracle Collaboration Suite Control or the `dcmctl` command line utility, modify the `httpd.conf` file to set the value of the `OraLogMode` and `OraLogSeverity` directives. Using the Oracle Collaboration Suite Control Console, from the Administration section of the HTTP_Server page select the Advanced Server Properties link. Specify the `OraLogMode` and `OraLogSeverity` directives in `httpd.conf`.

For example:

```
OraLogMode oracle
OraLogSeverity NOTIFICATION
```

3. Using the Oracle Collaboration Suite Control Console, restart the HTTP Server.

See Also: *Oracle HTTP Server Administrator's Guide* for details on using the `OraLogMode` and `OraLogSeverity` directives

Configuring OC4J to Produce ODL Messages

The supplied configuration files for OC4J include commented out specifications for ODL logging. Enabling ODL logging in OC4J involves uncommenting the ODL configuration options and restarting the associated OC4J instance.

To change the ODL logging configuration for OC4J, use the Oracle Collaboration Suite Control Console to select the Administration link for the OC4J instance that you want to enable ODL logging. Then, select the Advanced Properties link to show the Advanced Server Properties page. On this page, edit the configuration files and uncomment the lines that contain the `<odl>` element.

See Also: Chapter 3, "Advanced Configuration Development, and Deployment" in *Oracle Application Server Containers for J2EE User's Guide*

Configuring OC4J to Produce ECIDs

OC4J supports generating an Execution Context ID (ECID) for its log file entries. You can use the ECID to track requests as they move through Oracle Collaboration Suite, or through OC4J. By default ECID generation is disabled in OC4J.

To enable ECID generation in OC4J, set the Java command-line option `-Doracle.dms.transtrace.ecidenabled=true`.

To modify Java command line options using the Oracle Collaboration Suite Control Console, do the following:

1. Select the **Administration** link on the OC4J Home Page of the tier instance of interest.
2. Select **Server Properties** in the Instance Properties area.
3. Scroll down to the Multiple VM Configuration section. This section defines the ports and the command line options for OC4J and for the JVM that runs OC4J processes.
4. Under the Command Line Options area, add the following at the end of the Java Options text field:
`-Doracle.dms.transtrace.ecidenabled=true`
5. Click **Apply**.

Note the following when setting the `oracle.dms.transtrace.ecidenabled` property:

- The default value for `oracle.dms.transtrace.ecidenabled` is `false`.
- The property applies for the entire OC4J instance and it cannot be set to different values for different applications running on OC4J.
- When ODL is enabled for OC4J and you specify `oracle.dms.transtrace.ecidenabled=false`, OC4J uses an ECID that is generated from within OC4J, rather than receiving the ECID from Oracle HTTP Server. When ODL is enabled for OC4J, all log messages should include an ECID.

See Also: "Advanced Configuration Development, and Deployment" in *Oracle Application Server Containers for J2EE User's Guide*

Creating and Managing a Diagnostic Message Database Repository

You can use SQL scripts to create and manage a database repository for diagnostic messages. By creating a database repository for diagnostic messages, you can search, view, and correlate diagnostic messages across multiple Oracle Collaboration Suite tiers.

Use the following SQL scripts to create and manage a repository for diagnostic messages. The scripts are located in the following directory:

- On Windows:
`ORACLE_HOME\diagnostics\admin`
- On UNIX:
`ORACLE_HOME/diagnostics/admin`

The database that hosts the Log Repository can be an Oracle9i database or an Oracle Database 10g database.

Choose an Existing Tablespace or Create a New Tablespace

You can either use an existing tablespace for the repository or you can create a new tablespace. If you decide to create a new tablespace, connect to an Oracle database as

an administrator and run the script `dmrep_tablespace.sql`. This script requires two arguments: the name of the tablespace to be created and the location of the tablespace datafile, for example:

```
SQL> connect sys as sysdba
...
SQL> @ORACLE_HOME/diagnostics/admin/dmrep_tablespace.sql dmrep ORACLE_
HOME/diagnostics/repository/dmrep.dbf
```

Choose an Existing User or Create a New User

You can use an existing user or you can create a new user. If you decide to create a new user, connect to the Oracle database, containing the tablespace for the repository, as an administrator and run the script `dmrep_user.sql`. This script requires three arguments: name of the user, user password, and the default user tablespace. Use the tablespace you designated for the repository for the default user tablespace, for example:

```
SQL> @ORACLE_HOME/diagnostics/admin/dmrep_user.sql dmrepusr dmreppw dmrep
```

Create the Diagnostic Message Repository Schema

To create the diagnostic message repository schema, run the script `dmrep_create.sql`. Connect to the tablespace as the designated user, for example:

```
SQL> connect dmrepusr
...
SQL> @ORACLE_HOME/diagnostics/admin/dmrep_create.sql
```

Change the LogLoader Configuration To Use the Diagnostic Message Repository

In order for the LogLoader to load diagnostic messages into the repository, you must update the repository element in the `logloader.xml` file. To edit the repository element, you must know the [Java Database Connectivity \(JDBC\)](#) URL for the database hosting the diagnostic message repository. Replace the contents of the repository element with the following:

```
<repository>
  <database_repository
    url="jdbc:oracle:thin:@DB host:DB port:DB instance"
    user="dmrepusr" />
</repository>
```

Replace the variables in the preceding example with the values for your installation. The repository password for your installation should be stored in a [wallet](#) in the LogLoader configuration directory. To store the password, use the following command:

```
ORACLE_HOME/diagnostics/bin/logloader -storePassword -user dmrepusr -pwd dmreppw
```

If your installation is part of an OracleAS Cluster, updating the LogLoader configuration in one instance of the cluster and then running the following command propagates the changes to the other instances in the cluster:

```
ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct logloader
```

Removing Old Messages From the Diagnostic Message Repository

The script, `dmrep_drop.sql`, deletes messages that are older than a specified number of days, hours, minutes, or seconds. The script takes two arguments:

- N, which is the number of units

- Unit, which must be one of the following: DAY, HOUR, MINUTE, or SECOND

The following is an example of the script with arguments:

```
SQL> @ORACLE_HOME/diagnostics/admin/dmrep_cleanup.sql 7 DAY
```

Deleting the Diagnostic Message Repository

The script, `dmrep_drop.sql`, enables you to delete the schema for the diagnostic message repository. The following is an example of deleting the `dmrep` schema:

```
SQL> connect dmrepusr
...
SQL> @ORACLE_HOME/diagnostics/admin/dmrep_drop.sql
```

To delete the user and tablespace, connect to the databases as administrator and run the SQL commands for dropping a user and dropping a tablespace. The following is an example of dropping a user and tablespace including contents and datafiles:

```
SQL> connect sys as sysdba
...
SQL> drop user dmrepusr;
SQL> drop tablespace dmrep including contents and datafiles;
```

Limitations and Configuration

The Logs link in the Oracle Collaboration Suite Control Console gives you an integrated view of many Oracle Collaboration Suite component log files. However, certain log files are only available at the component level. Oracle Collaboration Suite components use the directory `ORACLE_HOME/diagnostics/config/registration` to make their log files visible to the Oracle Collaboration Suite Control Console. Some Oracle Collaboration Suite component log files are not exposed through Oracle Collaboration Suite Control Console pages.

Managing Microsoft Active Directory Integration

This chapter explains how Oracle Identity Management can integrate with Microsoft Active Directory in a production environment.

Note: This chapter assumes familiarity with the chapter on Oracle Internet Directory concepts and architecture in the *Oracle Internet Directory Administrator's Guide*.

If you are configuring a demonstration of integration with Microsoft Active Directory, then see the Oracle By Example series for Oracle Identity Management Release 10g Release 1 (10.1.1), available on Oracle Technology Network at <http://www.oracle.com/technology/>

This chapter contains these topics:

- [Concepts and Architecture of Microsoft Active Directory Integration](#)
- [Deployment Options for Integrating with Microsoft Active Directory](#)
- [Configuration of Integration with Microsoft Active Directory](#)
- [Managing Integration with Microsoft Active Directory](#)

See Also:

- *Oracle Identity Management Integration Guide* for information about integrating with the Microsoft Windows domain database
- "Oracle Internet Directory Frequently Asked Questions" on the Oracle Technology Network at <http://www.oracle.com/technology>
- *Oracle Identity Management Guide to Delegated Administration* for instructions on how to use the Oracle Internet Directory Self-Service Console

Concepts and Architecture of Microsoft Active Directory Integration

Oracle provides centralized security administration for all Oracle components by integrating them with Oracle Identity Management. Similarly, Microsoft provides centralized security administration in Microsoft Windows by integrating all Microsoft applications with Microsoft Active Directory.

If your environment uses both Oracle Identity Management and Microsoft Active Directory, then, to synchronize data in one with data in the other, you need to integrate the two systems. You do this by using Active Directory Connector.

This section discusses the Oracle components and architecture involved in integrating Oracle Identity Management with Active Directory. It contains these topics:

- [Components for Integrating with Microsoft Active Directory](#)
- [How Oracle Directory Integration and Provisioning Maintains Synchronization](#)
- [Oracle Internet Directory Schema Elements for Integration with Microsoft Active Directory](#)
- [Directory Information Tree in an Integration with Microsoft Active Directory](#)

Components for Integrating with Microsoft Active Directory

This section describes the following components that are used to integrate with Microsoft Active Directory:

- [Oracle Internet Directory](#)
- [Oracle Directory Integration and Provisioning](#)
- [Oracle Application Server Single Sign-On](#)
- [Active Directory External Authentication Plug-in](#)
- [Windows Native Authentication](#)

See Also: *Oracle Identity Management Integration Guide* for a description of the tools used to integrate Oracle Internet Directory with Microsoft Active Directory

Oracle Internet Directory

Oracle Internet Directory is the repository in which Oracle components and third-party applications store and access user identities and credentials. It uses the Oracle directory server to authenticate users by comparing the credentials entered by users with the credentials stored in Oracle Internet Directory. When credentials are stored in a third-party directory and not in Oracle Internet Directory, users can still be authenticated. In this case, Oracle Internet Directory uses an external authentication plug-in that authenticates users against the third-party directory server.

See Also:

- The chapter on security in *Oracle Internet Directory Administrator's Guide* for a discussion of security in Oracle Internet Directory
- ["Active Directory External Authentication Plug-in"](#) on page 9-3 for a brief discussion of the external authentication plug-in

Oracle Directory Integration and Provisioning

Oracle Directory Integration and Provisioning is installed as part of the Oracle Application Server infrastructure. You can configure it to run on the same host as Oracle Internet Directory or on a different host.

Oracle Directory Integration and Provisioning enables:

- Synchronization between Oracle Internet Directory and other directories and user repositories

- Automatic provisioning services for Oracle components

Oracle Directory Integration and Provisioning includes connectors to synchronize Oracle Internet Directory with other LDAP directories or data stores. One of its connectors, Active Directory Connector, is designed to synchronize Oracle Internet Directory with Microsoft Active Directory.

Active Directory Connector enables you to:

- Configure either one-way or two-way synchronization with Microsoft Active Directory
- Designate a specific subset of attributes for synchronization. You do this by configuring the appropriate mapping rules, which you can then change at run time
- Synchronize with multiple Microsoft Active Directory domains. You can synchronize changes with an individual domain or an entire Active Directory environment by using the Microsoft Global Catalog.

See Also: *Oracle Identity Management Integration Guide* for instructions on synchronizing with a Microsoft Windows NT domain database and information about configuring attribute mapping rules

Oracle Application Server Single Sign-On

OracleAS Single Sign-On enables users to access Oracle Web-based components by logging in only once.

Oracle components delegate the login function to the OracleAS Single Sign-On server. When a user first logs in to an Oracle component, the component directs the login to the OracleAS Single Sign-On server. The OracleAS Single Sign-On server compares the credentials entered by the user to those stored in Oracle Internet Directory. After verifying the credentials, the OracleAS Single Sign-On server grants the user access to all components the user is authorized to use throughout the current session.

OracleAS Single Sign-On enables native authentication in a Microsoft Windows environment. Once logged in to the Windows environment, the user automatically has access to Oracle components. OracleAS Single Sign-On automatically logs in the user to the Oracle environment using the user's Kerberos credentials.

See Also:

- *Oracle Application Server Single Sign-On Administrator's Guide* for information about OracleAS Single Sign-On
- The sections "[Windows Native Authentication](#)" on page 9-4 and "[Configuring Windows Native Authentication](#)" on page 9-38 for discussions on using Windows native authentication and how to configure it when integrating with Microsoft Active Directory

Active Directory External Authentication Plug-in

This plug-in, which is part of the Oracle directory server, enables Microsoft Windows users to log in to the Oracle environment by using their Microsoft Windows credentials. When this plug-in is in place, it is invoked by the Oracle directory server. This plug-in verifies the user's credentials in Microsoft Active Directory. If the verification is successful, then the Oracle directory server notifies OracleAS Single Sign-On.

See Also: ["Configuring the Active Directory External Authentication Plug-in"](#) on page 9-36

Windows Native Authentication

Windows native authentication is an authentication scheme for users of Microsoft Internet Explorer on Microsoft Windows. When this feature is enabled in OracleAS Single Sign-On, users log in to OracleAS Single Sign-On partner applications automatically. To do this, they use Kerberos credentials obtained when the user logged in to a Microsoft Windows domain.

Using the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) protocol, Internet Explorer version 5.0 and later can automatically pass the user's Kerberos credentials to a requesting Kerberos-enabled Web server. The Web server can then decode the credentials and authenticate the user.

Although the SPNEGO protocol supports both Kerberos version 5 and NT Lan Manager (NTLM) authentication schemes, Oracle Application Server 10g Release 1 (10.1.1) supports only Kerberos V5 with SPNEGO.

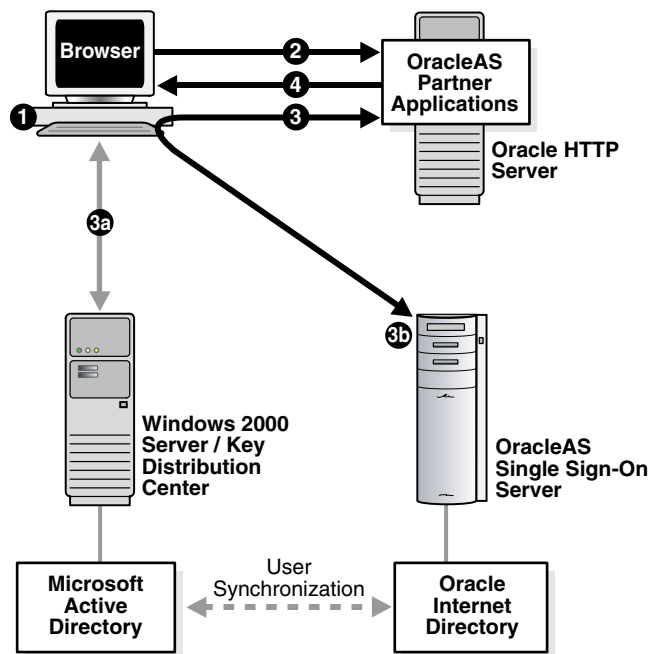
Note: Although this chapter refers only to Windows 2000, Windows native authentication is also supported on the Windows XP platform.

If the browser is not Internet Explorer 5.0, then Oracle Identity Management authenticates the user by using OracleAS Single Sign-On. Authentication to Active Directory is performed by using the Active Directory external authentication plug-in.

The following steps, shown in [Figure 9-1](#), describe what happens when a user tries to access a single-sign-on-protected application:

1. The user logs in to a Kerberos realm or domain, on a Microsoft Windows computer.
2. The user attempts to access a single-sign-on partner application by using Internet Explorer.
3. The application routes the user to the single sign-on server for authentication. As part of this routing, the following occurs:
 - a. The browser obtains a Kerberos session ticket from the Key Distribution Center (KDC).
 - b. The OracleAS Single Sign-On server verifies the Kerberos session ticket and, if the user is authorized, then the user is allowed to access the requested URL.
4. The application provides content to the user.

Figure 9–1 Flow for Windows Native Authentication



When the user logs out of the Windows session, this application and any single sign-on applications accessed are logged out at the same time.

See Also: ["Configuring Windows Native Authentication"](#) on page 9-38

How Oracle Directory Integration and Provisioning Maintains Synchronization

To keep Oracle Internet Directory and Microsoft Active Directory synchronized, Oracle Directory Integration and Provisioning brings in incremental changes made available by Microsoft Active Directory change tracking mechanisms. Oracle Directory Integration and Provisioning supports the following mechanisms:

- The DirSync approach, which uses an LDAP control that is supported by Microsoft Active Directory
- The USN-Changed approach, which uses an attribute of the entry

In each approach, the directory from which changes are derived is queried at scheduled intervals by Active Directory Connector.

Each approach has advantages and disadvantages. [Table 9–1](#) compares the two approaches.

Table 9–1 Comparing the DirSync Approach to the USN-Changed Approach

Considerations	DirSync Approach	USN-Changed Approach
Change key	Presents changes to the ObjectGUID, the unique identifier of the entry	Presents changes to the distinguished name (DN). The ObjectGUID is used to keep track of modifications of the DN.
Error handling	If synchronization stops as a result of an error condition, then, during the next cycle, all changes that are already applied are read and skipped.	Does not require synchronization to be atomic. If synchronization stops, then the next synchronization cycle starts from the entry where the synchronization was interrupted.
Information in the search results	Changes consist of only the changed attributes and the new values. This can be quicker than the USN-Changed approach.	All attributes of the changed entry are retrieved. The retrieved values are compared to the old values stored in Oracle Internet Directory and updated. This can be more time consuming than the DirSync approach.
Changes to multivalued attributes	Reflects incremental changes made to multivalued attributes as a complete replacement of the attribute value.	Reflects incremental changes made to multivalued attributes as a complete replacement of the attribute value.
How synchronization point is tracked	When queried for changes in the directory, presents incremental changes based on a cookie value that identifies the state of the directory.	The changes are queried in the directory based on the uSNChanged attribute, which is a long integer, that is, 8 bytes. You can modify the value to adjust where to start the synchronization.
Required user privileges	Requires the user to have the "Replicate Changes" privilege on the naming context of interest. This enables reading all objects and attributes in Microsoft Active Directory regardless of the access protections on them. See Also: ■ "Configuring the Connection Details for Microsoft Active Directory" on page 9-18 ■ The Microsoft Knowledge Base Article 303972 available at http://support.microsoft.com/ for instructions on how to assign privileges to Microsoft Active Directory users when using the DirSync approach. Apply to this context the instructions used for Active Directory management agent in this article.	Requires the Microsoft Active Directory user to have the privilege to read all required attributes to be synchronized to Oracle Internet Directory. See Also: Microsoft networking and directory documentation available in the Microsoft library at the following URL: http://msdn.microsoft.com/ for instructions about how to assign privileges to Microsoft Active Directory users when using the USN-Changed approach.
Support of multiple domains	Requires separate connections to different domain controllers to read changes made to the entries in different domains.	Can obtain changes made to the multiple domains by connecting to the Global Catalog server. See Also: "Considerations for Synchronizing with a Multiple-Domain Microsoft Active Directory Environment" on page 9-26

Table 9–1 (Cont.) Comparing the DirSync Approach to the USN-Changed Approach

Considerations	DirSync Approach	USN-Changed Approach
Synchronization from a replicated directory when switching to a different Microsoft Active Directory domain controller	Synchronization can continue. The synchronization key is the same when connecting to a replicated environment.	Requires: ■ Full synchronizing to a known point ■ Updating the uSNChanged value ■ Starting synchronization with the failover directory See Also: "Switching to a Different Microsoft Active Directory Domain Controller in the Same Domain" on page 9-50
Synchronization scope	Reads all changes in the directory, filters out changes to the required entries, and propagates to Oracle Internet Directory	Enables synchronization of changes in any specific subtree
Usability in an environment with multiple Microsoft Active Directory servers behind a load balancer	-	Either connect to a specific Microsoft Active Directory domain controller, or connect to a Global Catalog. Connect to Global Catalog if: ■ You are interested in import operations only. ■ The Global Catalog contains all entries and attributes to be synchronized. ■ Performance of the Global Catalog is acceptable.

Oracle Internet Directory Schema Elements for Integration with Microsoft Active Directory

To identify objects that are synchronized with those in Microsoft Active Directory, Oracle Internet Directory contains schema elements that correspond to Active Directory-specific attributes. These schema elements are described in Appendix B of *Oracle Identity Management Integration Guide*.

Directory Information Tree in an Integration with Microsoft Active Directory

This section contains the following topics:

- [About Realms in Oracle Internet Directory](#)
- [Planning the Deployment](#)
- [Example: Integration with a Single Microsoft Active Directory Domain Controller](#)
- [Example: Integration with Multiple Microsoft Active Directory Domain Controllers](#)

See Also: The chapter on directory concepts and architecture in *Oracle Internet Directory Administrator's Guide* for a discussion of directory information trees.

About Realms in Oracle Internet Directory

In Oracle Internet Directory, an identity management realm defines an enterprise scope over which certain identity management policies are defined and enforced by the deployment. It comprises:

- A well-scoped collection of enterprise identities, for example, all employees in the US domain.

- A collection of identity management policies associated with these identities. An example of an identity management policy would be to require that all user passwords have at least one alphanumeric character.
- A collection of groups, that is, aggregations of identities that simplify setting the identity management policies

Multiple Realms

You can define multiple identity management realms within the same Oracle Identity Management infrastructure. This enables you to isolate user populations and enforce a different identity management policy, for example, password policy, naming policy, self-modification policy, in each realm. This is useful in a hosted deployment of Oracle Collaboration Suite.

Each identity management realm is uniquely named to distinguish it from other realms. It also has a realm-specific administrator with complete administrative control over the realm.

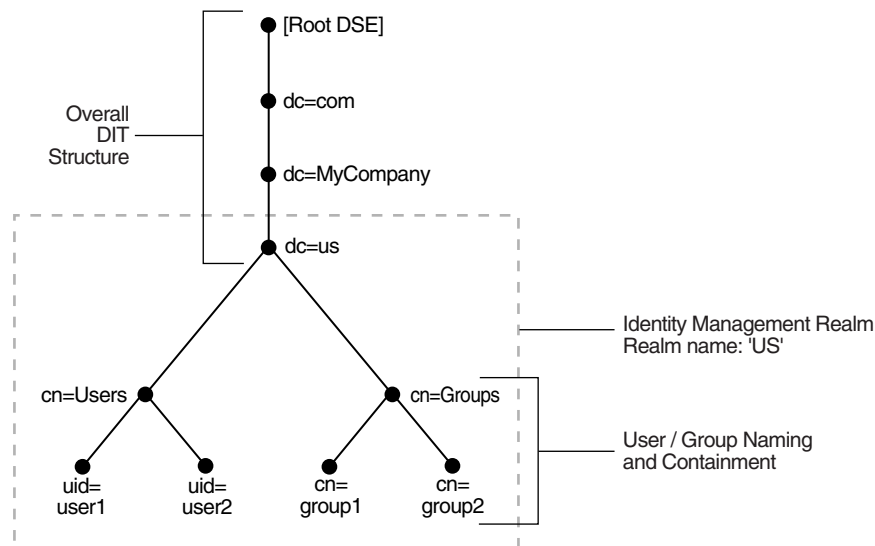
The Default Realm

For all Oracle components to function, an identity management realm is required. One particular realm, created during installation of Oracle Internet Directory, is called the default identity management realm. It is where Oracle components expect to find users, groups, and associated policies whenever the name of a realm is not specified. This default realm facilitates proper organization of information and enforces proper access controls in the directory.

There can be only one default identity management realm in the directory. If a deployment requires multiple identity management realms, then one of them must be chosen as the default.

Figure 9–2 illustrates the default identity management realm.

Figure 9–2 The Default Identity Management Realm



As Figure 9–2 shows, the default identity management realm is part of a global DIT. The node just below the root DSE is `dc=com`, followed by `dc=MyCompany`, then `dc=us`. These four nodes represent the overall DIT structure. The node `dc=us` is the

root of the default identity management realm. It has two subtrees for containing user and group information: `cn=Users` and `cn=Groups`. For illustration purposes, the `cn=Users` node contains two leaves: `uid=user1` and `uid=user2`. Similarly, the `cn=Groups` node contains `cn=group1` and `cn=group2`.

Access Control Policies in the Realm

You must configure appropriate ACLs in Oracle Internet Directory to enable Oracle Directory Integration and Provisioning to:

- Enable the import profile to add, modify and delete objects in the `users` and `groups` containers. By default, import profiles are part of the Realm Administrators group, which can perform all operations on any entry under the realm DN. If you have customized ACLs in the realm, then you need to ensure that the import profiles have the appropriate privileges to perform these operations on the subtree to be synchronized or on either the `user` container, the `group` container, or both depending on where the synchronization takes place.
- Enable Oracle components to manage the users and groups in the realm. By default, Oracle components can manage users and groups in the `users` and `groups` containers, respectively. If you have updated your `usersearchbase` and `groupsearchbase` in the realm, then set up appropriate ACLs on the `users` container and `groups` container.

See Also: The chapter on deployment of Oracle Identity Management realms in *Oracle Internet Directory Administrator's Guide* for a description of the default realm installed with Oracle Internet Directory

Planning the Deployment

When planning the directory information tree (DIT), the most important decisions to make before synchronization are:

- Which directory is to be the central one
- What objects to synchronize, for example:
 - The portion of the DIT that you want to synchronize. You can synchronize the entire DIT or just a portion of it.
 - For each entry, the specific contents that you want to synchronize. You can synchronize the entire content of the entry or just a portion of it.
- Where to synchronize. You have two options:
 - You can synchronize so that the relative position of each entry in the DIT is the same in the source and destination directories. This configuration, called one-to-one distinguished name mapping, is the most commonly used configuration. Because the source DN is the same as the destination DN, this configuration provides better performance than when the two DNs are different.
 - You can synchronize so that the relative position in the DIT of each entry in the destination directory is different from that in the source directory. In this configuration, the Oracle directory integration and provisioning server must change the DN values of all entries being mapped, including their references in group entries. This requires more intensive computation.

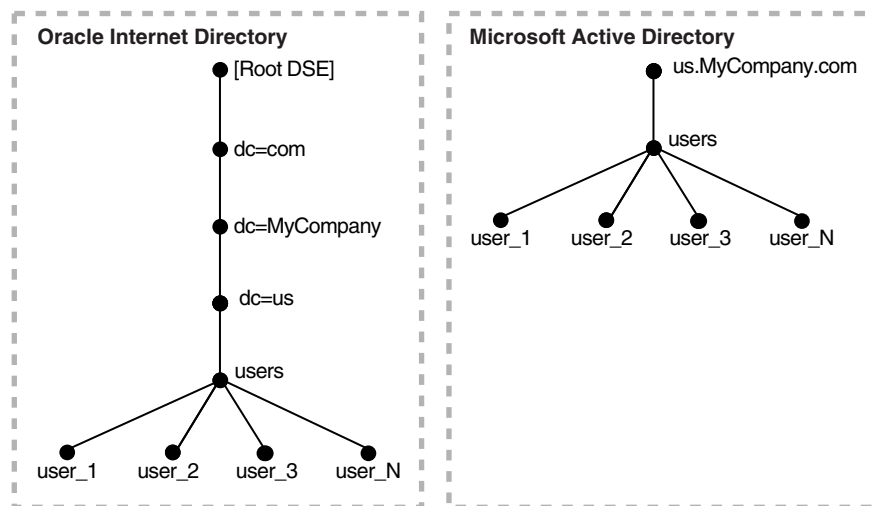
If you synchronize in this way, you need to use the `dnconvert` mapping rule as described in Chapter 6 of *Oracle Identity Management Integration Guide*.

See Also: Chapter 15 of *Oracle Identity Management Integration Guide* for more information about planning the directory information tree

Example: Integration with a Single Microsoft Active Directory Domain Controller

Figure 9–3 shows an example of one-to-one mapping between the two directories.

Figure 9–3 Default DIT Structures in Oracle Internet Directory and Active Directory When Both Directory Hosts Are Under the Domain *us.MyCompany.com*



In the one-to-one mapping illustrated in Figure 9–3:

- Both Active Directory and Oracle Internet Directory hosts have the same topology.
- Users are synchronized only from Active Directory to Oracle Internet Directory. All users to be synchronized are stored in one container in Active Directory, in this case `users.us.MyCompany.com`.
- The same DIT structure is maintained in both Active Directory and Oracle Internet Directory. All users appear in the same `users` subtree identified by the value `cn=users, dc=us, dc=MyCompany, dc=com`.

In the example shown in Figure 9–3, only the `users` subtree must be synchronized from Active Directory to Oracle Internet Directory using one-to-one domain mappings.

Note: In the example in Figure 9–3, the two directories have the same topology, but be aware that this is for illustration purposes only. The two directories do not need to be in the same domain. Oracle Internet Directory can be anywhere in the network, provided it can connect to Microsoft Active Directory.

In addition, although the synchronization in the example is one-way, from Microsoft Active Directory to Oracle Internet Directory, the synchronization can, alternatively, be bi-directional.

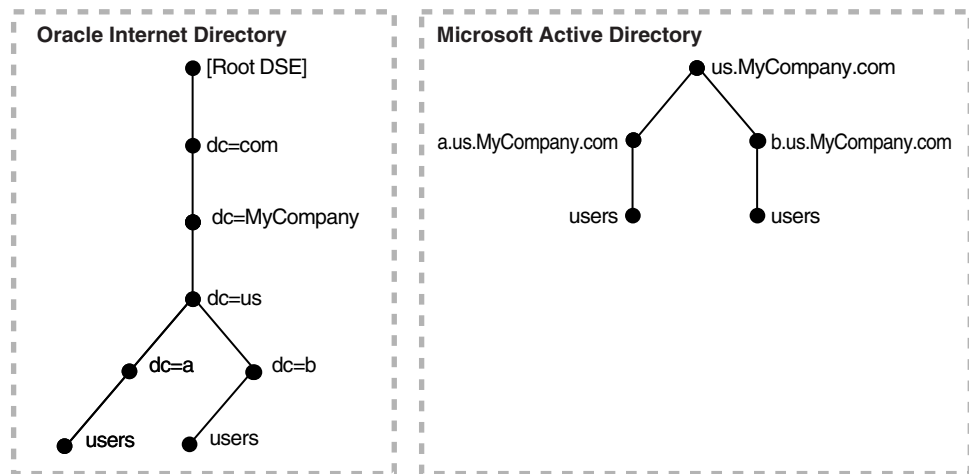
Example: Integration with Multiple Microsoft Active Directory Domain Controllers

A deployment of Microsoft Active Directory with multiple domains can have either a single DIT or a combination of two or more DITs. In Microsoft Active Directory, a group of DITs is called a forest.

One-to-One Mapping of Multiple Microsoft Active Directory Domains

Figure 9-4 shows how multiple domains in Microsoft Active Directory are mapped to a DIT in Oracle Internet Directory.

Figure 9-4 Example of a Mapping Between Oracle Internet Directory and Multiple Domains in Microsoft Active Directory



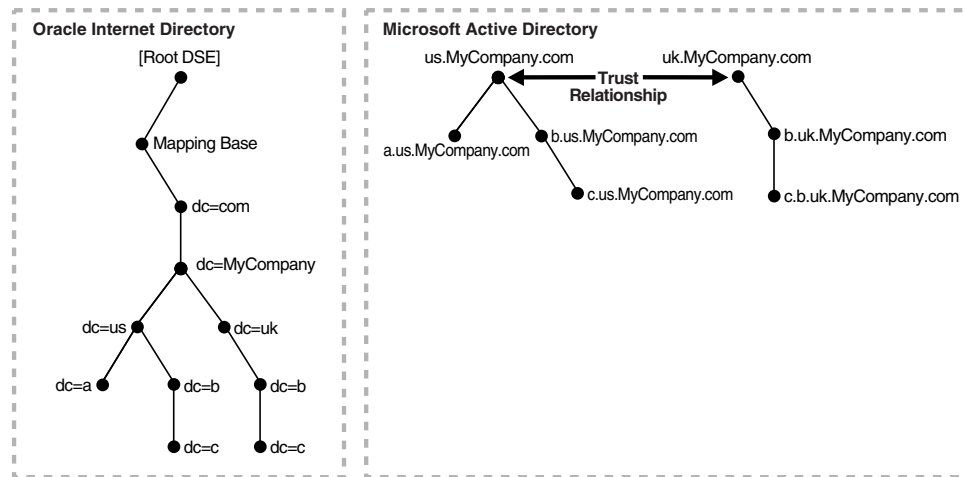
In Figure 9-4, the Microsoft Active Directory environment has a parent and two children. Each domain has a domain controller associated with it. The Active Directory domain controller supporting the node `us.mycompany.com` is the Global Catalog server.

The first child domain `a.us.MyCompany.com` maps to `dc=a, dc=us, dc=MyCompany, dc=com` in Oracle Internet Directory. The second child domain `b.us.MyCompany.com` maps to `dc=b, dc=us, dc=MyCompany, dc=com` in Oracle Internet Directory. The common domain component in Active Directory environment `us.MyCompany.com` maps to the default identity management realm in Oracle Internet Directory, in this case `dc=us, MyCompany, dc=com`.

Mapping of a Microsoft Active Directory Forest

Figure 9-5 shows how a forest in Microsoft Active Directory is reflected in Oracle Internet Directory.

Figure 9–5 Mapping Between Oracle Internet Directory and a Forest in Microsoft Active Directory



In this directory, two domain trees constitute a forest. These trees are in a trust relationship, that is, users in one domain are authenticated by the domain controller in the other domain. This forest in Microsoft Active Directory maps to an identically structured subtree in Oracle Internet Directory.

Foreign Security Principals

A Microsoft Active Directory user or computer account represents a physical entity such as a computer or person. User accounts and computer accounts, as well as groups, are called security principals. Security principals are directory objects that are automatically assigned security identifiers. Objects with security identifiers can log on to the network and access domain resources. A user or computer account is used to:

- Authenticate the identity of the user or computer
- Authorize or deny access to domain resources
- Administer other security principals
- Audit actions performed using the user or computer account

For example, the user and computer accounts that are members of the Enterprise Administrators group are automatically granted permission to log on at all of the domain controllers in the forest.

User and computer accounts are added, disabled, reset, and deleted by using Microsoft Active Directory Users and Computers.

In a trust relationship in Active Directory, users in one domain are authenticated by a domain controller in another domain. The trust relationship can be transitive or nontransitive.

- In a transitive trust relationship, the trust relationship extended to one domain is automatically extended to all other domains that trust that domain. For example, suppose you have three domains: A, B, and C in which both B and C are in a direct trust relationship with A. In this scenario, both B and C also trust each other. This is because, although they are not in a direct trust relationship with each other, they are in a direct trust relationship with A.

- In a nontransitive trust relationship, the trust is bound by the two domains in the trust relationship; it does not flow to any other domains in the forest.

When a trust is established between a Windows 2000 domain in a particular forest and a Windows 2000 domain outside of that forest, security principals from the external domain can be granted access to resources in the forest. A security principal from an external domain is called a *foreign security principal* and is represented in Active Directory as a "foreign security principal" object. These foreign security principals can become members of domain local groups, which can have members from domains outside of the forest.

Foreign security principals are used when there is a nontransitive trust between two domains in a Microsoft Active Directory environment.

In a nontransitive trust relationship in a Microsoft Active Directory environment, when one domain recognizes a foreign security principal from the other domain, it represents that entity similar to a DN entry. In that entry, the RDN component is set to the SID of the original entry in the trusted domain. In the case of groups, the DNs of the foreign security principals are represented as member values, not as the DNs of the original entries in the trusted domain. This can create a problem when foreign security principals are synchronized with Oracle Internet Directory.

Deployment Options for Integrating with Microsoft Active Directory

There are two common ways of integrating with a Microsoft Windows environment:

- Using Oracle Internet Directory as the central directory for user and group data for the Microsoft Windows 2000 and Windows NT environments
- Using Microsoft Active Directory as the central enterprise directory for user and group data for Oracle components

This section discusses the requirements of each deployment. It contains the following topics:

- [Deployments with Oracle Internet Directory as the Central Directory](#)
- [Deployments with Microsoft Active Directory as the Central Directory](#)

Deployments with Oracle Internet Directory as the Central Directory

[Table 9–2](#) describes the typical requirements in this deployment.

Table 9–2 Typical Requirements with Oracle Internet Directory as the Central Directory

Requirement	Description
Initial startup	The Directory Integration and Provisioning Assistant populates Microsoft Active Directory with users and groups stored in Oracle Internet Directory. If there are multiple Microsoft Active Directory domains, then the Directory Integration and Provisioning Assistant must be run as many times as there are Microsoft Active Directory domains. Each time you do this, you choose the specific data set required by the target Microsoft Active Directory domain.
Synchronization	User and group information is managed in Oracle Internet Directory. Changes to that information are synchronized with Microsoft Active Directory by the Oracle directory integration and provisioning server when an import profile has been configured. Synchronization from Microsoft Active Directory into Oracle Internet Directory can be achieved by configuring an import profile.
Passwords and password verifiers	Passwords are managed in Oracle Internet Directory by using Oracle tools such as the Oracle Internet Directory Self-Service Console. Password changes are synchronized with Microsoft Active Directory by the Oracle directory integration and provisioning server. However, before this server can synchronize the password changes, the password synchronization must be configured in the mapping rules. Because the password is securely managed, the communication for synchronizing passwords to Microsoft Active Directory must be over SSL. Run the Oracle directory integration and provisioning server in the server-only authentication mode with the proper certificate from Microsoft Active Directory. Be sure that Active Directory is also enabled for SSL. If the Oracle environment requires a password verifier, then the password verifier is automatically generated when a new user entry is created or when a password is modified.
Oracle Application Server Single Sign-On	Users log in to the Oracle environment by using the OracleAS Single Sign-On server. When called upon by the OracleAS Single Sign-On server to authenticate a user, the Oracle directory server uses credentials available locally. No external authentication is involved. Users must log in only once to access various components in the Oracle environment.

New users or groups in Oracle Internet Directory can be automatically provisioned into the Microsoft Windows environment by the Oracle directory integration and provisioning server. This automatic provisioning requires that:

- The Oracle directory server is running with the change log enabled
- The change log is not purged

If these two conditions are not met, then you must load the entries in Oracle Internet Directory to an LDIF file and upload the data to Microsoft Active Directory.

If multiple Microsoft Active Directory domains are involved, then the Oracle directory integration and provisioning server provisions users and groups in the respective Microsoft Active Directory domains. Before provisioning can take place, you must configure a one-way synchronization from Oracle Internet Directory to the Microsoft Active Directory domain.

See Also: The chapter on garbage collection in *Oracle Internet Directory Administrator's Guide* for information about purging the change log

Deployments with Microsoft Active Directory as the Central Directory

Table 9–3 describes the typical requirements in this deployment.

Table 9–3 Typical Requirements with Microsoft Active Directory as the Central Directory

Requirement	Description
Initial startup	The Directory Integration and Provisioning Assistant populates Oracle Internet Directory with users and groups stored in Microsoft Active Directory. If there are multiple Microsoft Active Directory servers, then you must bootstrap the data from each Microsoft Active Directory domain. If you use the Global Catalog for one-way synchronization from Microsoft Active Directory to Oracle Internet Directory, then you need to bootstrap only once from the Global Catalog server. You can choose to manage user information, including password credentials, in Microsoft Active Directory only. In such deployments, to enable single sign-on in the Oracle environment, the Oracle directory integration and provisioning server can synchronize only those user entry attributes required by Oracle components. Passwords are not migrated from Microsoft Active Directory to Oracle Internet Directory.
Synchronization	The central directory for user and group information is Microsoft Active Directory. Changes to user and group information in Active Directory are synchronized with Oracle Internet Directory by the Oracle directory integration and provisioning server when an import profile has been configured. Synchronization from Oracle Internet Directory to Microsoft Active Directory is achieved by configuring an export profile.
Passwords and password verifiers	Passwords are managed in typically Active Directory by using Microsoft Windows tools. The Oracle directory integration and provisioning server does not synchronize password changes into Oracle Internet Directory.
Oracle Application Server Single Sign-On	Users log in to the Oracle environment only once by using the OracleAS Single Sign-On server. Users with credentials only in Microsoft Active Directory are authenticated by the Oracle directory server invoking the external authentication plug-in. Users with credentials in Oracle Internet Directory are authenticated locally by the Oracle directory server.
Windows native authentication	Same as in Oracle Internet Directory-centered deployment. However, for a user to use Windows native authentication, a user must exist in Active Directory. If Windows native authentication is enabled, then, for local Oracle Internet Directory users to invoke the single sign-on server, you must populate the attributes <code>orclsamaccountname</code> and <code>krbprincipalname</code> for each user entry.
Active Directory external authentication plug-in	When user credentials are managed in Microsoft Active Directory, this plug-in is required. To authenticate a user, the OracleAS Single Sign-On server calls upon the Oracle directory server. The plug-in then performs the authentication of the user against the user credentials stored in Active Directory.

New users or groups created in Microsoft Active Directory are automatically synchronized into Oracle Internet Directory by the Oracle directory integration and provisioning server. Before the provisioning can take place, a one-way synchronization between Microsoft Active Directory and Oracle Internet Directory must be established.

If multiple Microsoft Active Directory domains are involved, then the Oracle directory integration and provisioning server synchronizes users and groups from the respective Microsoft Active Directory domains into Oracle Internet Directory. Before the provisioning can take place, a one-way synchronization between Oracle Internet Directory and a domain controller on each Microsoft Active Directory domain must be established.

Passwords are not migrated from Microsoft Active Directory to Oracle Internet Directory.

Configuration of Integration with Microsoft Active Directory

This section contains these topics:

- [Configuring the Realm](#)
- [Configuring Synchronization Profiles](#)
- [Customizing Access Control Lists](#)
- [Configuring the Active Directory Connector for Synchronization in SSL Mode](#)
- [Considerations for Synchronizing with a Multiple-Domain Microsoft Active Directory Environment](#)
- [Configuring the Active Directory Connector Profiles](#)
- [Configuring the Active Directory External Authentication Plug-in](#)
- [Configuring Windows Native Authentication](#)
- [Configuring Synchronization of Oracle Internet Directory Foreign Security Principal References with Microsoft Active Directory](#)

Configuring the Realm

To configure the realm, perform the following steps:

1. Choose the realm DN structure as described in Chapter 15 of *Oracle Identity Management Integration Guide*, and, more specifically, in the section "[Planning the Deployment](#)".
2. Select the attribute for the login name of the user. This attribute contains the name of the attribute used for logging in. By default, it is `uid`. If you are integrating with Microsoft Active Directory, and the `userprincipalname` attribute is used for logging in, then you would map `userprincipalname` to the `uid` attribute in Oracle Internet Directory. For more information, see Chapter 15 of *Oracle Identity Management Integration Guide*.
3. Set up the `usersearchbase` and `groupsearchbase` values in Oracle Internet Directory. These values indicate to the various Oracle components where to look for users and groups in Oracle Internet Directory. They are set to default values during installation. However, in deployments requiring integration with Active Directory, you may need to reset these values so that they correspond to the DIT structures in the two directories. Be sure to set them correctly. Otherwise, even if the synchronization seems to function properly, components still may be unable to access users and groups in Oracle Internet Directory.

To illustrate how you might configure the user search base and group search base: In the example in [Figure 9–3](#), the value of `usersearchbase` should be set to `cn=users,dc=us,dc=MyCompany,dc=com` or one of its parents. Similarly, assuming there is a subtree named `groups` in the DIT, the multivalued `groupsearchbase` attribute should be set to both of the following:

- `cn=groups,dc=us,dc=MyCompany,dc=com` or one of its parents
- `cn=users,dc=us,dc=MyCompany,dc=com`

To configure the user search base and group search base, use the Oracle Internet Directory Self-Service Console.

4. Set up the `usercreatebase` and `groupcreatebase` values in Oracle Internet Directory. These values indicate to the various Oracle components where users and groups can be created. They are set to default values during installation.

To illustrate how to configure the user create base and group create base: In the example in [Figure 9-3](#), the value of `usercreatebase` should be set to `cn=users,dc=us,dc=MyCompany,dc=com` or one of its parents. Similarly, the `groupcreatebase` should be set to `cn=groups,dc=us,dc=MyCompany,dc=com` or one of its parents.

To configure the user create base and group create base, use the Oracle Internet Directory Self-Service Console.

See Also: The section on modifying configuration settings for an identity management realm in *Oracle Identity Management Guide to Delegated Administration*

Configuring Synchronization Profiles

This section describes various customizations that a deployment may require. It contains these topics:

- [About the Sample Synchronization Profiles](#)
- [Creating Synchronization Profiles](#)
- [Configuring the Connection Details for Microsoft Active Directory](#)
- [Customizing Mapping Rules](#)
- [Customizing the LDAP Schema](#)
- [Customizing the Search Filter to Get Information from Microsoft Active Directory](#)
- [Synchronizing Deletions from Microsoft Active Directory](#)
- [Synchronizing Passwords](#)

Note: Be sure your ORACLE home environment variable is set to the correct value; otherwise, the commands specified in various scenarios do not function properly.

About the Sample Synchronization Profiles

During installation, three sample Active Directory Connector synchronization profiles are provided. You can customize these samples to meet your deployment needs. The sample synchronization profiles are:

- `ActiveImport`—The profile for importing changes from Microsoft Active Directory to Oracle Internet Directory by using the DirSync approach
- `ActiveChgImp`—The profile for importing changes from Microsoft Active Directory to Oracle Internet Directory by using the USN-Changed approach
- `ActiveExport`—The profile for exporting changes from Oracle Internet Directory to Microsoft Active Directory

Whether you use `ActiveImport` or `ActiveChgImp` depends on the method you chose for tracking changes, either DirSync or USN-Changed.

If these sample profiles meet your needs, then copy them and use the exact copies for running Active Directory Connector. If they do not meet your needs, then copy them and customize the copies.

To copy the sample profiles, use the `createprofilelike (cpl)` command of the Directory Integration and Provisioning Assistant, then enable the profile by following the instructions in Chapter 7 of *Oracle Identity Management Integration Guide*. When you

restart the Oracle directory integration and provisioning server, it uses the duplicate profile for synchronization, automatically refreshing its cache with any changed information.

Mapping Rules Mapping rules, an important part of the synchronization profile, determine the directory information to be synchronized and how it is to be transformed when synchronized. You can change mapping rules at run time to meet your requirements.

Each sample Active Directory synchronization profile includes default mapping rules. These rules contain a minimal set of default user and group attributes configured for out-of-the-box synchronization.

Note: When a synchronization is underway, it relies on the mapping rules configured prior to any changes in the directory. To ensure consistent mapping, you may need to remove an already synchronized entry or perform a full synchronization.

See Also:

- Chapter 9 of *Oracle Identity Management Integration Guide* for instructions on how to modify the sample profiles to meet your needs
- Chapter 6 of *Oracle Identity Management Integration Guide* for instructions on how to create mapping rules
- ["Customizing Mapping Rules"](#) on page 9-19 for instructions on how to modify the mapping rules to meet your needs

Creating Synchronization Profiles

To create new profiles, copy the sample profiles provided during installation and modify the copies.

To create and configure new profiles, use the Directory Integration and Provisioning Assistant. The Assistant can be invoked as a command-line tool or a graphical interface tool.

- To invoke the Assistant as a command-line tool, enter `dipassistant`.
- To invoke the Assistant as a graphical interface tool, enter the following command:

```
$ORACLE_HOME/bin/dipassistant -gui
```

This displays the Oracle Directory Integration and Provisioning Server Administration tool, which provides a subset of the functionality provided through the command-line version of the tool.

See Also:

- Chapter 3 of *Oracle Identity Management Integration Guide* for a detailed description of each tool
- Appendix A of *Oracle Identity Management Integration Guide*

Configuring the Connection Details for Microsoft Active Directory

You can configure the Active Directory Connector by using either the Oracle Directory Integration and Provisioning Server Administration tool or the express configuration

option of the Directory Integration and Provisioning Assistant. Using either of these, you can specify the connection details as input to the script. This is the recommended method for configuring these details.

You can also create the profiles based on the template properties file provided during installation. If you are doing this, then you must specify the connection details in the `odip.profile.condirurl`, `odip.profile.condiraccount`, and `odip.profile.condirpassword` properties of the profile.

In addition to specifying the connection details, you must also ensure that the user account in Active Directory has the privileges to replicate directory changes for every domain of the forest monitored for changes. You can do this by one of the following methods:

- Grant to this account Domain Administrative permissions
- Make this account a member of the Domain Administrator's group
- Grant to this account Replicating Directory Changes permissions for every domain of the forest that is monitored for changes

To grant this permission to a non-administrative user, follow the instructions in the "More Information" section of the Microsoft Help and Support article "How to Grant the 'Replicating Directory Changes' Permission for the Microsoft Metadirectory Services ADMA Service Account" available at <http://support.microsoft.com/>.

Customizing Mapping Rules

Mapping rules govern the way data is transformed when a source directory and a destination directory are synchronized. Customize the default mapping rules found in the sample profiles when you need to do the following:

- Change distinguished name mappings. The distinguished name mappings establish how the Microsoft Active Directory DIT maps to the Oracle Internet Directory DIT.
- Change the attributes that need to be synchronized.
- Change the transformations (mapping rules) that occur during the synchronization.

You can perform any mapping if the resulting data in the destination directory conforms to the schema in that directory.

Note: For password synchronizations, there are additional mapping considerations. See the section "[Synchronizing Passwords](#)" on page 9-23.

See Also: Chapter 6 of *Oracle Identity Management Integration Guide* for a full discussion of mapping rules

Distinguished Name Mapping You can change how the DIT in Active Directory maps to the one in Oracle Internet Directory.

Example 9-1 Example of Distinguished Name Mapping

Distinguished Name Rules
`%USERBASE INSOURCE%:%USERBASE ATDEST%:`

USERBASE refers to the container from which Microsoft Active Directory users and groups must be mapped. Usually, this is the `users` container under the root of the Microsoft Active Directory domain.

Example 9-2 Example of One-to-One Distinguished Name Mapping

For one-to-one mapping to occur, the DN in Microsoft Active Directory must match that in Oracle Internet Directory.

In this example, the DN in Microsoft Active Directory matches the DN in Oracle Internet Directory. More specifically:

- The Microsoft Active Directory host is in the domain `us.mycompany.com`, and, accordingly, the root of the Microsoft Active Directory domain is `us.mycompany.com`. A user container under the domain would have a DN value `cn=users,dc=us,dc=mycompany,dc=com`.
- Oracle Internet Directory has a default realm value of `dc=us,dc=mycompany,dc=com`. This default realm automatically contains a `users` container with a DN value `cn=users,dc=us,dc=mycompany,dc=com`.

Because the DN in Microsoft Active Directory matches the DN in Oracle Internet Directory, one-to-one distinguished name mapping between the directories can occur.

If you plan to synchronize only the `cn=users` container under `dc=us,dc=mycompany,dc=com`, then the domain mapping rule is:

```
Distinguished Name Rules
cn=users,dc=us,dc=mycompany,dc=com:cn=users,dc=us,dc=mycompany,dc=com
```

This rule synchronizes every entry under `cn=users,dc=us,dc=mycompany,dc=com`. However, the type of object synchronized under this container is determined by the attribute-level mapping rules that follow the DN Mapping rules.

If you plan to synchronize the entry `cn=groups,dc=us,dc=mycompany,dc=com` under `cn=users,dc=us,dc=mycompany,dc=com` then the domain mapping rule is as follows:

```
cn=groups,dc=us,dc=mycompany,dc=com: cn=users,dc=us,dc=mycompany,dc=com
```

Attribute-Level Mapping Attribute-level mapping specifies:

- The attributes in source directory that are to be synchronized
- The corresponding attributes in the target directory with which they are to be synchronized
- Any transformation of attribute values that is to occur as the data is synchronized from one directory to the other

The following attribute-level mapping is mandatory for all objects:

```
ObjectGUID: : :orclObjectGUID:
ObjectSID: : :orclObjectSID:
```

Example 9-3 Attribute-Level Mapping for the User Object

```
SAMAccountName:1: :user:orclADSAMAccountName: :orclADUser
userPrincipalName: : :user:orclADUserPrincipalName:
:orclADUser:userPrincipalName
```


Example 9–4 Attribute-Level Mapping for the Group Object

```
SAMAccountName:1: :user:orclADSAMAccountName: :orclADGroup
```

In this example, `SAMAccountName` and `userPrincipalName` from Microsoft Active Directory are mapped to `orclADSAMAccountName` and `orclADUserPrincipalName` in Oracle Internet Directory.

Adding another attribute to be synchronized requires adding another rule, as previously indicated earlier. Similarly, if an attribute no longer needs to be synchronized, then the corresponding rule needs to be removed or put in a comment.

See Also:

- Chapter 6 of *Oracle Identity Management Integration Guide* for examples of how attribute values are transformed when synchronized from one directory to another
- The file `$ORACLE_HOME/ldap/odi/conf/activeimp.map.master` for an example of import mapping rules.

How to Customize the Mapping Rules To customize the mapping rules:

1. Make a duplicate of the sample mapping rules file based on your deployment scenario. For example, whether you are using the DirSync approach or the USN-Changed approach, or whether or not you are doing one-to-one mapping.
2. Edit the sample mapping rules file to make the previously discussed modifications. The sample mapping rules files are stored in the directory `$ORACLE_HOME/ldap/odi/conf` with the extension of `map.master` for the various profiles. You can find instructions for editing mapping rules in Chapter 6 of *Oracle Identity Management Integration Guide*.
3. After the changes are made, enter the following command:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name
-host oid_host -port oid_port -dn DN -passwd password
odip.profile.mapfile=path_name
```

For example:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -profile my_profile
-host my_host -port 3060 -dn cn=orcladmin -passwd welcome1
odip.profile.mapfile=my_profile.map
```

See Also: Appendix A of *Oracle Identity Management Integration Guide*

Customizing the LDAP Schema

Customizing the LDAP schema is required if:

- A directory deployment contains schema extensions such as custom object classes and attributes
- The custom attributes must be synchronized from one directory server to the other

To customize the LDAP schema, you must:

- Identify the schema extensions on the source directory

- Create those extensions on the target directory before starting the data migration and the synchronization.

Note: In addition to creating schema extensions, you must also add the attribute to be synchronized with the corresponding object classes to the mapping rules.

See Also:

- The chapter on administering the schema in *Oracle Internet Directory Administrator's Guide* for instructions on customizing the schema in Oracle Internet Directory
- Microsoft documentation available at <http://msdn.microsoft.com/> for instructions on customizing the schema in Microsoft Active Directory

Customizing the Search Filter to Get Information from Microsoft Active Directory

By default, Active Directory Connector retrieves changes to all objects in the container configured for synchronization. If you are interested in retrieving only a certain type of change, for example only changes to users and groups, then you should configure an LDAP search filter. This filter screens out changes that are not required when Active Directory Connector queries Active Directory. The filter is stored in the `searchfilter` attribute in the synchronization profile.

In the sample profiles `activeChgImp` and `activeImport`, only groups and users are retrieved from Microsoft Active Directory. Computers are not retrieved. The value of the `searchfilter` attribute is set as:

```
searchfilter=(|(objectclass=group) (&(objectclass=user) (!(objectclass=computer)))).
```

You can use either Oracle Directory Integration and Provisioning Server Administration tool or Directory Integration and Provisioning Assistant to update the `searchfilter` attribute.

To customize the search filter by using the Directory Integration and Provisioning Assistant:

1. Enter the following command to customize the Connected Directory Matching Filter (`orclODIPConDirMatchingFilter`) attribute:
2. Enter the following command to customize the Oracle Internet Directory Matching Filter (`orclODIPOIDMatchingFilter`) attribute:

```
$ORACLE_HOME/bin/dipassistant
```

```
$ORACLE_HOME/bin/dipassistant
```

To customize the search filter by using the Oracle Directory Integration and Provisioning Server Administration tool:

1. Launch the Oracle Directory Integration and Provisioning Server Administration tool by entering:

```
$ORACLE_HOME/bin/dipassistant -gui
```

2. In the navigator pane, expand *directory_integration_and_provisioning_server*, then expand **Integration Profile Configuration**.

3. Select the configuration set, and, in the right pane, select the profile you want to customize. The Integration Profile window appears.
4. In the Integration Profile window, select the Mapping tab. The fields in this tab page are described in Appendix C of *Oracle Identity Management Integration Guide*.
5. In the Mapping tab page, in the Connected Directory Matching Filter (`orclODIPConDirMatchingFilter`) and the OID Matching Filter (`orclODIPOIDMatchingFilter`) fields, enter the appropriate values for the `searchfilter` attribute. Instructions for specifying the `searchfilter` attribute are provided in Chapter 6 of *Oracle Identity Management Integration Guide*.
6. Choose OK.

Note: All attributes specified in the `searchfilter` attribute should be configured as indexed attributes in Microsoft Active Directory.

See Also: The appendix on the LDAP filter definition in *Oracle Internet Directory Administrator's Guide* for instructions on configuring an LDAP search filter

Synchronizing Deletions from Microsoft Active Directory

Active Directory deletions can be synchronized with Oracle Internet Directory by querying for them in Active Directory. The way to do this depends on whether you are using the DirSync approach or the USN-Changed approach.

For the DirSync approach, the Active Directory user account that the Oracle directory integration and provisioning server uses to access Active Directory must have Domain Administrative permissions, belong to the Domain Administrators group, or be explicitly granted Replicating Directory Changes permissions. For information on how to grant Replicating Directory Changes permissions, see Article ID 303972 at <http://support.microsoft.com>.

For the USN-Changed approach, the Active Directory user account that the Oracle directory integration and provisioning server uses to access Active Directory must have "List Content" and "Read Properties" permission to the `cn=Deleted Objects` container of a given domain. In order to set these permissions, you must use the `dscls.exe` command that is available with recent versions of Active Directory Application Mode (ADAM). You can download the most recent version of ADAM at <http://www.microsoft.com/downloads/>.

Synchronizing Passwords

You can synchronize Oracle Internet Directory passwords with Active Directory. You can also make passwords stored in Microsoft Active Directory available in Oracle Internet Directory. Password synchronization is possible only when the directories run in SSL mode 2, that is, server-only authentication, as described in Appendix A of *Oracle Identity Management Integration Guide*.

Synchronizing Passwords from Oracle Internet Directory to Microsoft Active Directory Before Active Directory Connector can synchronize passwords in this direction, perform the following steps:

1. Add a mapping rule that enables password synchronization. For example:

```
Userpassword: : :inetorgperson:unicodepwd: :user
```

2. Enable the password policy and reversible password encryption in the Oracle directory server. To do this, assign a value of 1 to the `orclPwPolicyEnable` and `orclPwEncryptionEnable` attributes in the entry `cn=PwPolicyEntry,cn=common,cn=products,cn=oraclecontext,DN_of_realm`. You can do this by using either Oracle Directory Manager or `ldapmodify`.

See Also:

- ["Configuring the Active Directory Connector for Synchronization in SSL Mode"](#) on page 9-26
- Chapter 6 of *Oracle Identity Management Integration Guide* for instructions on adding mapping rules
- The chapter on directory storage of password verifiers in *Oracle Internet Directory Administrator's Guide* for information about enabling reversible encryption

Synchronizing from Microsoft Active Directory to Oracle Internet Directory Because passwords in Microsoft Active Directory cannot be accessed by LDAP clients, you cannot synchronize Oracle Internet Directory passwords with Microsoft Active Directory in Oracle Application Server. However, if a deployment requires passwords to be available in Oracle Internet Directory, then Oracle recommends the following two methods:

- Build a custom plug-in for Active Directory that captures a password change and synchronizes it with Oracle Internet Directory. For more information:
 - See the chapter about the Oracle Internet Directory plug-in framework in *Oracle Internet Directory Administrator's Guide*
 - Visit the Microsoft Developer Network (MSDN) at <http://msdn.microsoft.com/>
- Manage Active Directory passwords from the Oracle environment. With this method, passwords are available in both Oracle Internet Directory and Microsoft Active Directory. The Active Directory Connector can synchronize the two directories.

Note: To synchronize passwords, you must enable SSL mode as discussed in ["Configuring the Active Directory Connector for Synchronization in SSL Mode"](#) on page 9-26.

Customizing Access Control Lists

This section discusses how to customize ACLs for import profiles, export profiles, and for other Oracle components. It contains these topics:

- [Customizing ACLs for Import Profiles](#)
- [Customizing ACLs for Export Profiles](#)
- [ACLs for Other Oracle Components](#)

Customizing ACLs for Import Profiles

The import profile is the identity used by the Oracle directory integration and provisioning server to access Oracle Internet Directory. ACLs must enable the import profile to add, modify, and delete objects in either the users and groups containers or

the subtree where entries are accessed. By default, import profiles are part of the Realm Administrators group (`cn=RealmAdministrators, cn=groups, cn=OracleContext, realm_DN`) in the default realm. This group grants privileges to perform all operations on any entry under the DN of the default realm.

You should not need to customize the ACLs for import synchronization with the default realm that is installed with Oracle Internet Directory Release 10g Release 1 (10.1.1). If you are upgrading from an earlier version of Oracle Internet Directory, or if the synchronization is with a nondefault Oracle Internet Directory realm, then be sure that the necessary privileges in the proper subtree or containers are granted to the import profiles handling the synchronization.

For an ACL template in LDIF format, see the file `$ORACLE_HOME/ldap/schema/oid/oidRealmAdminACL.sbs`. If you have not changed the ACLs on the default realm, then this template file can be applied directly after instantiating the substitution variables, replacing `%s_SubscriberDN%` with the default realm DN in Oracle Internet Directory and replacing `%s_OracleContextDN%` with `cn=OracleContext, default_realm_DN` respectively. For example, if `realmacl.ldif` is the instantiated file, then you can upload it by using the following `ldapmodify` command:

```
$ORACLE_HOME/bin/ldapmodify -h <OID host> -p <OID port>
-D "DN of privileged OID user" -w "password of privileged OID user"
-v -f realmacl.ldif
```

See Also: The chapter on access controls in *Oracle Internet Directory Administrator's Guide*

Customizing ACLs for Export Profiles

To enable the Oracle directory integration and provisioning server to access Active Directory, you must create an identity in Active Directory. This identity is configured in each export profile.

ACLs for Other Oracle Components

Default ACLs enable you to create, modify, and delete users and groups, but only in the users and groups containers under the default realm. To synchronize objects in other containers, you must customize the ACLs.

There are sample ACL files that you can use to customize ACLs for Oracle Components. These sample files are installed in the directory `$ORACLE_HOME/ldap/schema/oid/`. They are:

- `oidUserAdminACL.sbs`: Grants necessary rights to the subtree for Oracle components to manage and access users
- `oidGroupAdminACL.sbs`: Grants necessary rights to the subtree for Oracle components to manage and access groups.
- `oidUserAndGroupAdminACL.sbs`: Grants the privileges for Oracle components to manage and access users and groups in the subtree.

You can customize your ACL policy to grant privileges on a container-by-container basis with the required rights.

See Also: The chapter on access control in *Oracle Internet Directory Administrator's Guide* for instructions on customizing ACLs

Configuring the Active Directory Connector for Synchronization in SSL Mode

Active Directory Connector uses SSL to secure the synchronization process. Whether or not you synchronize in the SSL mode depends on your deployment requirements. For example, synchronizing public data does not require SSL, but synchronizing sensitive information such as passwords does. To synchronize password changes between Oracle Internet Directory and Microsoft Active Directory, you must use SSL mode with server-only authentication, that is, SSL Mode 2.

Securing the channel requires:

- Enabling SSL between Oracle Internet Directory and the Oracle directory integration and provisioning server
- Enabling SSL between the Oracle directory integration and provisioning server and Microsoft Active Directory

Although you can enable SSL either between Oracle Internet Directory and the Oracle directory integration and provisioning server or between that server and Microsoft Active Directory, Oracle recommends that you completely secure the channel before you synchronize sensitive information. In certain cases, such as password synchronization, synchronization can occur only over SSL.

Configuring SSL requires the following:

- Running the Oracle directory server in SSL mode as described in the chapter on Secure Sockets Layer (SSL) in *Oracle Internet Directory Administrator's Guide*
- Running the Oracle directory integration and provisioning server in the SSL mode as described in Chapter 2 of *Oracle Identity Management Integration Guide*. The SSL mode should be the same as the one in which Oracle Internet Directory server was started. When starting the Oracle directory integration and provisioning server, specify the `sslauth` parameter to 1 for no authentication or 2 for server-only authentication.
- Running the Microsoft Active Directory server in SSL mode. Communication with Microsoft Active Directory over SSL requires SSL Mode 2, that is, server-only authentication. This requires that both Oracle Internet Directory and the Oracle directory integration and provisioning server be run in SSL mode 2.
- Configuration of the Microsoft Active Directory connector to use SSL. This includes creating a wallet, which will contain the certificates for both Oracle Internet Directory and Microsoft Active Directory. For more information, see Chapter 4 of *Oracle Identity Management Integration Guide*.

Note: The Oracle Directory and Integration Provisioning Server does not support SSL in the client/server authentication mode.

Considerations for Synchronizing with a Multiple-Domain Microsoft Active Directory Environment

This section describes how to import from Microsoft Active Directory to Oracle Internet Directory and export from Oracle Internet Directory to Microsoft Active Directory.

Configuration Required for Importing from Microsoft Active Directory to Oracle Internet Directory

Normally, importing requires configuring one import profile for each Microsoft Active Directory domain regardless of whether you are using the DirSynch approach or the

USN-Changed approach. However, if you are using the USN-Changed approach, you can use the Global Catalog to import from an entire Microsoft Active Directory forest. Although this requires configuring only one import profile, consider the following:

- Because Global Catalog is read-only, you can use it only for importing data into Oracle Internet Directory.
- Global Catalog does not contain all the attributes, although the available attributes can be configured in Microsoft Active Directory.
- Because Global Catalog is a global synchronization point, the process can become congested as a result of additional access to the import file.

See Also: The Microsoft Knowledge Base Article 256938 available from Microsoft Help and Support at <http://support.microsoft.com/> for information about Global Catalog attributes in the Microsoft Active Directory schema

Configuration Required for Exporting from Oracle Internet Directory to Microsoft Active Directory

To integrate with multiple-domain Microsoft Active Directory environments, the Oracle directory integration and provisioning server obtains configuration information from each Active Directory domain. You must configure as many export profiles as there are Microsoft Active Directory domains.

Configuring the Active Directory Connector Profiles

The Oracle directory integration and provisioning server includes an express configuration option that you can run with either the Directory Integration and Provisioning Assistant or the Oracle Directory Integration and Provisioning Server Administration tool. Express configuration creates two synchronization profiles, one for import and one for export, using predefined assumptions. After you enable the profiles, you can immediately begin synchronizing users and groups between `cn=users, default_naming_context` in Microsoft Active Directory and `cn=users, default_realm` in Oracle Internet Directory.

The Active Directory connector import and export synchronization profiles created with express configuration are only intended as a starting point for you to use when deploying your integration of Oracle Internet Directory and Microsoft Active Directory. Because the default synchronization profiles are created using predefined assumptions, you must further customize them for your environment.

Note: While customizing the synchronization profiles for your environment, you may need to add test users and groups to facilitate your deployment effort. Be sure to remove any test users and groups when you are finished customizing and testing your synchronization profiles.

WARNING: In order to successfully customize your import and export synchronization profiles, do not enable SSL until you have finished with all other configuration tasks.

In order to successfully complete configuration of the profiles for your environment, be sure to perform the procedures listed in this section in the following order:

1. [Preparing for Synchronization](#)
2. [Creating Synchronization Profiles with Express Configuration](#)
3. [Customizing Attribute Mapping](#)
4. [Final Configuration Requirements](#)
5. [Configuring Synchronization Profiles for SSL](#)
6. [Additional Considerations](#)

Preparing for Synchronization

To prepare for synchronization between Oracle Internet Directory and Microsoft Active Directory:

1. Plan your deployment by reading the following:
 - Chapter 15 of *Oracle Identity Management Integration Guide*
 - ["Concepts and Architecture of Microsoft Active Directory Integration"](#) on page 9-1
2. Use Oracle Collaboration Suite Control to verify that Oracle Internet Directory is running.
3. Create a user account in Microsoft Active Directory with sufficient privileges to perform both import and export operations. Oracle Directory Integration and Provisioning will use this account to log in to Microsoft Active Directory.
 - **For Import Operations from Microsoft Active Directory:** Grant the user account read access privileges to the subtree root. The user account must be able to read all objects under the source container (subtree root) in Active Directory that are to be synchronized with the Oracle directory integration and provisioning server. To verify whether an Active Directory user account has the necessary privileges to all Active Directory objects to be synchronized with Oracle Internet Directory, use the command-line `ldapsearch` utility to perform a subtree search, as follows:

```
$ORACLE_HOME/bin/ldapsearch -h <AD host> -p <AD port> -b "DN of subtree"  
-s sub -D "DN of privileged AD user" -w "password for privileged AD user"  
"objectclass=*
```

The return results from the `ldapsearch` utility should include all objects of interest, including all attributes and values that will be synchronized.

To synchronize deletions of users in Active Directory with Oracle Internet Directory, you must grant the user account the necessary privileges by following the instructions in ["Synchronizing Deletions from Microsoft Active Directory"](#) on page 9-23.

- **For Export Operations to Microsoft Active Directory:** Grant the user account the following privileges to the subtree root that is the parent of all the containers to which the Oracle directory integration and provisioning server will export users:
 - Write
 - Create all child objects
 - Delete all child objects

See Also: Your Microsoft Active Directory documentation for information how to grant privileges to user accounts

Creating Synchronization Profiles with Express Configuration

This section describes how to create and customize synchronization profiles with express configuration. It contains these topics:

- [Understanding Express Configuration](#)
- [Running Express Configuration](#)
- [Additional Synchronization Considerations](#)

Understanding Express Configuration To simplify the configuration, the express configuration option assumes the following:

- Only creation and modifications of organizational units, users, and groups are synchronized.
Entries for Users and groups in Active Directory are located in the container `cn=users, default_naming_context`.
- Entries for users of the default realm in Oracle Internet Directory are located in the container `cn=users, default_realm_DN`.
- Entries for groups of the default realm in Oracle Internet Directory are located in the container `cn=groups, default_realm_DN`.
- The method used for tracking changes in Active Directory is the USN-Changed approach.
- The default Active Directory Connector profiles, namely, `ActiveImport`, `ActiveExport`, and `ActiveChgImp`, are present in the Oracle directory server.
- The Directory Integration and Provisioning master mapping rules files created during installation are present in `$ORACLE_HOME/ldap/odi/conf`. The file names are `activechg.map.master` and `activeexp.map.master`.
- The logon credential is that of a Directory Integration and Provisioning administrator with sufficient privileges to configure a profile, a realm, and access controls on the Users container in the Oracle directory server. Members of the Directory Integration and Provisioning Administrators group (`cn=dipadmingrp, cn=odi, cn=oracle internet directory`) have the necessary privileges.
- Connections to Active Directory or Oracle Internet Directory are NOT over SSL.

Perform the following steps to run express configuration and verify that users and groups are synchronizing between `cn=users, default_naming_context` in Microsoft Active Directory and `cn=users, default_realm` in Oracle Internet Directory:

1. Run express configuration by following the procedures described in "[Running Express Configuration](#)" on page 9-30.
2. Enable the import and export synchronization profiles by using either the Oracle Directory Integration and Provisioning Server Administration tool or the Directory Integration and Provisioning Assistant with the `modifyprofile` option. For example, the following Directory Integration and Provisioning Assistant command enables an import profile named `myprofile`:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -host myhost -port 3060  
-passwd my_password -file import.profile -dn bind_DN  
-passwd Password_of_bind_DN -profile myprofile odip.profile.status=ENABLE
```

3. Start the Oracle directory integration and provisioning server by following the instructions described in Chapter 4 of *Oracle Identity Management Integration Guide*.
4. Wait until the scheduling interval has elapsed and verify that synchronization has started by entering the following command:

```
$ORACLE_HOME/bin/ldapsearch -h <OID host> -p <OID port>  
-D "DN of privileged OID user" -w "password of privileged OID user"  
-b "orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog  
subscriber,cn=oracle internet directory" -s base "objectclass=*"  
orclodipsynchronizationstatus orclodioplastsuccessfulexecutiontime
```

Note: The default scheduling interval is 60 seconds (1 minute). You can use the Directory Integration and Provisioning Assistant or the Oracle Directory Integration and Provisioning Server Administration tool to change the default scheduling interval. For more information, see Chapter 3 of *Oracle Identity Management Integration Guide*.

When synchronization is successfully started:

- The value of the Synchronization Status attribute is Synchronization Successful.
- The value of the Last Successful Execution Time attribute is the specific date and time of that execution. Note that this must be close to the current date and time.

An example of a result indicating successful synchronization is:

```
Synchronization successful November 04, 2003 15:56:03
```

Note:

- The date and time must be close to current date and time.
 - When running the ldapsearch command, you need the dipadmin password, which, as established at installation, is the same as orcladmin password.
-

5. After verifying that synchronization has started, examine the entries in Oracle Internet Directory and Microsoft Active Directory to confirm that users and groups are synchronizing between `cn=users,default_naming_context` in Microsoft Active Directory and `cn=users,default_realm` in Oracle Internet Directory.

Running Express Configuration You can run express configuration using either the Oracle Directory Integration and Provisioning Server Administration or the Directory Integration and Provisioning Assistant, as described in the following sections:

- [Running Express Configuration with the Oracle Directory Integration and Provisioning Server Administration Tool](#)
- [Running Express Configuration with the Directory Integration and Provisioning Assistant](#)

Running Express Configuration with the Oracle Directory Integration and Provisioning Server Administration Tool

To perform an express configuration of the Active Directory Connector:

1. Launch the Oracle Directory Integration and Provisioning Server Administration tool by entering:

```
$ORACLE_HOME/bin/dipassistant -gui
```

2. In the Oracle Directory Integration and Provisioning Server Administration tool, expand *directory_server*, then Integration Profile Configuration, and select Active Directory Connector Configuration. The corresponding tab pages appear in the right pane.
3. In the Active Directory Connector Express Synchronization tab page, enter the appropriate values.
4. Click **Apply**.

Running Express Configuration with the Directory Integration and Provisioning Assistant

To perform an express configuration of the Active Directory Connector:

1. Launch the Directory Integration and Provisioning Express Configuration Tool:

```
$ORACLE_HOME/bin/dipassistant expressconfig
[-h oracle_internet_directory_host
-p oracle_internet_directory_port -configset configuration_set_entry]
```

The arguments in the preceding example are listed in [Table 9-4](#).

Table 9-4 Arguments for the Directory Integration and Provisioning Express Configuration Tool

Argument	Description
<i>oracle_internet_directory_host</i>	Host of the Oracle directory server. The default is the local host.
<i>oracle_internet_directory_port</i>	Non-SSL port for Oracle Internet Directory. The default is 389.
<i>configuration_set_entry</i>	Configuration set for Oracle Directory Integration and Provisioning. The default is 1.

2. When prompted, enter the following information:

- Oracle Internet Directory credentials. You must specify the super user, that is, `cn=orcladmin`, or any user that is a member of the Directory Integration and Provisioning Administrators group (`cn=dipadmingrp`, `cn=odi`, `cn=oracle_internet_directory`).
- Active Directory connection details and credentials of a privileged user. To synchronize deletions, you must have the necessary administrative privileges in Microsoft Active Directory, for example `administrator@MyCompany.com`, if the host on which Microsoft Active Directory is installed is `hostname@us.oracle.com`.
- Name to identify the synchronization profiles to be created. For example, if you specify the name `abc`, then the tool creates two profiles: `abcImport` and `abcExport`.

- (Optional) Appropriate ACLs on the `cn=users` container. You can choose to enable users and groups to be managed by Oracle components under the `cn=users` container. If you customize ACLs in this way, then the original ACLs are saved in `$ORACLE_HOME/ldap/odi/archive/profile_name_prefix_useracl.ldif`.

Additional Synchronization Considerations This section describes additional issues that you may need to consider when configuring your synchronization profiles. It contains these topics:

- [Handling Synchronization Errors](#)
- [Synchronizing Deletions in Active Directory](#)
- [Using DirSync Change Tracking for Import Operations](#)

Handling Synchronization Errors

While examining synchronization results, you may notice that the Oracle directory integration and provisioning server is attempting to repeatedly process the same change. This indicates that an error is occurring during synchronization of that change. By default, the Oracle directory integration and provisioning server will.

Synchronizing Deletions in Active Directory

In order to synchronize deletions in Active Directory with Oracle Internet Directory, you must grant the necessary privilege to the Active Directory user account that the Oracle directory integration and provisioning server uses to perform synchronizations with Active Directory. "[Synchronizing Deletions from Microsoft Active Directory](#)" on page 9-23.

Using DirSync Change Tracking for Import Operations

The import synchronization profile created with express configuration uses the USN-Changed approach for tracking changes. To modify the import synchronization profile so it uses the DirSync change tracking approach:

Note: You may want to backup your current import synchronization profile before performing the following procedures. You can create a backup copy of a profile by using the Directory Integration and Provisioning Assistant's `createprofilelike` command.

1. You can use the `activeimp.cfg.master` file, located in your `$ORACLE_HOME/ldap/odi/conf` directory, to change the import synchronization profile from the USN-Changed approach to DirSync. Use the following command to update the profile:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name  
odip.profile.configfile=$ORACLE_HOME/ldap/odi/conf/activeimp.cfg.master
```

2. Update the last change number by running the following command:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name -updcln
```

In order to update the last change number, the value assigned to the `odip.profile.condirurl` property in the import synchronization profile must be for a non-SSL connection. If you have already configured the import synchronization profile for SSL, then before attempting to update the last change

number, you must temporarily change the value assigned to the `odip.profile.condirurl` property so it points to a non-SSL port.

See Also: ["Configuring the Connection Details for Microsoft Active Directory"](#) on page 9-18

Customizing Attribute Mapping

Once you have established a working synchronization between Oracle Internet Directory and Microsoft Active Directory, you can customize the attribute mapping rules for your synchronization profiles to meet the needs of your deployment. To customize the attribute mapping rules for your synchronization profiles:

1. When you use express configuration to create import and export synchronization profiles, mapping files are created for each profile in the `$ORACLE_HOME/ldap/conf` directory. The mapping files are named `profile_nameImport.map` and `profile_nameExport.map`. For example, if you enter "abc" when express configuration prompts you for the name of your profile, your import mapping files will be named `abcImport.map` and `abcExport.map`. Modify the mapping rules in your mapping files as needed by following the instructions described in ["Customizing Mapping Rules"](#) on page 9-19.
2. Wait until the scheduling interval has elapsed, and then check the synchronized users and groups to ensure that the attribute mapping rules meet your requirements.
3. Repeat Step 1 and Step 2 until the synchronized users and groups contain the attributes you need.

Tip: You may find it helpful to add test users and groups to Oracle Internet Directory or Microsoft Active Directory when customizing attribute mapping rules.

Final Configuration Requirements

This section describes the final configuration requirements for the import and export synchronization profiles created with express configuration. It contains these topics:

- [Customizing DN Mapping Rules](#)
- [Synchronizing Multiple Domains](#)
- [Performing Initial Bootstrapping](#)
- [Granting Privileges to Non-Default Realms](#)

Customizing DN Mapping Rules Once you have finished customizing the attribute mapping rules for your synchronization between Oracle Internet Directory and Microsoft Active Directory, you should customize the DN mapping rules for your synchronization profiles to meet the needs of your deployment.

WARNING: If you do not correctly map DN rules, then configuring multiple Microsoft Active Directory domains against a single instance of Oracle Internet Directory can result in name collision. This is because the container `cn=users, default_naming_context` in each of the multiple domains in Microsoft Active Directory is synchronized to the same container, `cn=users, default_realm`, in Oracle Internet Directory.

To customize the DN mapping rules for your synchronization profiles:

1. Modify the DN mapping rules in your mapping files as needed by following the instructions described in ["Customizing Mapping Rules"](#) on page 9-19.
2. Wait until the scheduling interval has elapsed, and then check the synchronized users and groups to ensure that the DN mapping rules meet your requirements.
3. Repeat Step 1 through Step 2 until the DN mapping rules meet the needs of your deployment.

Tip: You may find it helpful to add test users and groups to Oracle Internet Directory or Microsoft Active Directory when customizing DN mapping rules.

Synchronizing Multiple Domains When synchronizing with multiple Active Directory domains, you need separate import and export synchronization profiles for each domain in most cases. However, the profiles for each domain should be very similar. The only exception involves using Global Catalog with import synchronization profiles. In this case, you only need to create a single import synchronization profile for the entire Active Directory forest. For more information, see ["Configuration Required for Importing from Microsoft Active Directory to Oracle Internet Directory"](#) on page 9-26.

Note: Be sure to perform attribute and DN mapping before attempting to synchronize with multiple domains.

The best approach to creating separate import and export synchronization profiles for multiple domains is as follows:

1. Customize the import and export synchronization profiles for a single domain, using the procedures described earlier in this section.
2. Once you have finished customizing the import and export synchronization profiles for the first domain, use the Directory Integration and Provisioning Assistant's `createprofilelike` command to duplicate profiles, as follows.

`$ORACLE_HOME/bin/dipassistant`
3. Use the Directory Integration and Provisioning Assistant's `modifyprofile` command to customize the profiles for each additional Active Directory domain, as follows:

`$ORACLE_HOME/bin/dipassistant`
4. If necessary, update the connection details for each domain by following the instructions listed in ["Configuring the Connection Details for Microsoft Active Directory"](#) on page 9-18.
5. Update the last change number in the import and export synchronization profiles for each domain by running the following command:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name -updcln
```

In order to update the last change number, the value assigned to the `odip.profile.condirurl` property in the import synchronization profile must be for a non-SSL connection. If you have already configured the import synchronization profile for SSL, then before attempting to update the last change

number, you must temporarily change the value assigned to the `odip.profile.condirurl` property so it points to a non-SSL port.

6. Repeat Steps 2 through 5 for each Active Directory domain to which you need to synchronize.

Performing Initial Bootstrapping Once you have finished configuring your import and export synchronization profiles, including customizing attribute mappings, DN mappings, and configuring for multiple Active Directory realms, you can migrate data from an Active Directory domain to Oracle Internet Directory by using the `bootstrap` option of the Directory Integration and Provisioning Assistant. This is described in ["Bootstrapping Data Between Directories"](#) on page 9-48.

Granting Privileges to Non-Default Realms If you need to synchronize Microsoft Active Directory with an Oracle Internet Directory subtree that is not in the default realm, then be sure to grant the necessary privileges to the import and export synchronization profiles. The import synchronization profile must have privileges to create, modify, and delete entries while the export synchronization profile must have read privileges to Oracle Internet Directory, including `cn=changelog`.

Configuring Synchronization Profiles for SSL

Your last step in customizing the import and export synchronization profiles should be to enable SSL. By default, SSL is not enabled for the import and export synchronization profiles created with express configuration. This section describes how to enable SSL for Active Directory synchronizations.

Note: Be sure that you can successfully synchronize users in non-SSL mode before attempting to configure your synchronization profiles for SSL.

1. Follow the instructions in ["Configuring the Active Directory Connector for Synchronization in SSL Mode"](#) on page 9-26.
2. Once SSL is enabled for Active Directory and Oracle Internet Directory, you can modify the Active Directory connection information, including the host name and profile, using the Directory Integration and Provisioning Assistant's `modifyprofile` command, as follows:

```
$ORACLE_HOME/bin/dipassistant modifyprofile <-h hostName> <-p port>  
-profile profilename odip.profile.condirurl= ad_host_name:636:1
```

3. Restart the Oracle directory integration and provisioning server by following the instructions in Chapter 4 of *Oracle Identity Management Integration Guide*.
4. Add a test user and verify that it synchronizes successfully. If the test user does not synchronize successfully, then troubleshoot your SSL configuration.

Additional Considerations

Read the following topics for additional configuration requirements:

- ["Configuring the Realm"](#) on page 9-16
- ["Configuring the Active Directory External Authentication Plug-in"](#) on page 9-36
- ["Configuring Windows Native Authentication"](#) on page 9-38
- ["ACLs for Other Oracle Components"](#) on page 9-25

Configuring the Active Directory External Authentication Plug-in

This section explains how to delete, disable, and re-enable the Active Directory external authentication plug-in. It contains these topics:

- [Installing Active Directory External Authentication Plug-ins](#)
- [Enabling the Active Directory External Authentication Plug-ins](#)
- [Testing the Active Directory External Authentication Plug-ins](#)

Installing Active Directory External Authentication Plug-ins

To install the plug-in:

1. Execute the script `oidspadi.sh` by entering:

```
cd $ORACLE_HOME/ldap/admin
sh oidspadi.sh
```

Note: To run shell script tools on the Windows operating system, you need one of the following UNIX emulation utilities:

- Cygwin 1.3.2.2-1 or later. Visit <http://sources.redhat.com/>
 - MKS Toolkit 6.1. Visit <http://www.datafocus.com/>
-

If you are using the Windows operating system, then execute `oidspadi.sh` after you have installed the UNIX emulation utility by entering:

```
sh oidspadi.sh
```

2. Enter the Microsoft Active Directory host name. This is the Microsoft Active Directory with which you are going to synchronize. This value is required.
3. Specify whether to use an SSL connection to Microsoft Active Directory. If you choose to use SSL, then you need to enter the following:
 - The Microsoft Active Directory SSL connection port number
 - The location of the Oracle wallet. This wallet needs to have the valid certificate from the Microsoft Active Directory that you are trying to connect to.
 - The Oracle wallet password.

When specifying the wallet location on the Microsoft Windows operating system, add an additional backslashes (\). For example, if the wallet location is `D:\storage\wallet`, then enter `D:\\storage\\wallet`.

4. Enter the connect string for the database designated for Oracle Internet Directory.
5. Enter the Oracle directory server password for Oracle Internet Directory
6. Enter the directory server host name. This value is required.
7. Enter directory server port number. The default port is 389.
8. Enter the password of the Oracle administrator (`orcladmin`). This value is required.
9. (Optional) Enter the distinguished name of the container to which the plug-in needs to be applied. Every entry in this container will be authenticated against Active Directory. Note that this need not necessarily be the User Search Base supplied by using the Oracle Internet Directory Self-Service Console. All the users

under this search base are authenticated externally to the Active Directory. If more than one container is specified, then separate the DNs with semi-colons (;).

10. Enter the Plug-in Request Group DN. For security reasons, the plug-in can be invoked only by users belonging to this group. For example, suppose that the Oracle Application Server Single Sign-On administrators are in the group `cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext`. If you enter this DN as the value for the Plug-in Request Group DN, then only requests from Oracle Application Server Single Sign-On administrators can trigger the external authentication plug-in. You can enter multiple DN values. Use a semicolon (;) to separate them. This value is not required, but, for security purposes, it should be specified.
11. (Optional) Enter the value of the entry that is to be excluded from authentication to Microsoft Active Directory. This value is the exception to Step 9. You need to enter the value in the standard ldapsearch filter format. For example, if you specify the value `(&(objectclass=inetorgperson)(cn=orcladmin))`, then any entry under the user container specified in Step 9 that has the `cn=orcladmin` and `objectclass=inetorgperson` attribute values will not be authenticated to Microsoft Active Directory.
12. (Optional) Specify the backup Microsoft Active Directory domain controller details.

Enabling the Active Directory External Authentication Plug-ins

By default, the Active Directory external authentication plug-ins are enabled. However, you may need to enable them at some point.

To enable Active Directory external authentication plug-ins:

1. Create an LDIF file with the following entries:

```
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
```

```
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
```

2. Load the LDIF file with the `ldapmodify` command as follows:

```
ldapmodify -h host -p port -D cn=orcladmin -w password -f fileName
```

See Also: The section about registering and managing plug-ins in *Oracle Internet Directory Administrator's Guide*

Testing the Active Directory External Authentication Plug-ins

To test the Active Directory external authentication plug-ins:

1. Use your browser to visit `http://host of OracleAS Single Sign-On:port number of OracleAS Single Sign-On/pls/orasso`.
2. Log in by using a pre-defined user in Microsoft Active Directory: `user identifier@domain`.

Configuring Windows Native Authentication

This section describes the system requirements and tasks for configuring Windows native authentication. It contains these topics:

- [System Requirements](#)
- [Configuration Tasks](#)
- [Fallback Authentication](#)
- [Login Scenarios](#)

See Also: ["Windows Native Authentication"](#) on page 9-4

System Requirements

Windows native authentication is intended for intranet Web applications. Your intranet deployment must include the following:

- Windows 2000 server with Microsoft Active Directory
- Kerberos service account established for OracleAS Single Sign-On server
- Oracle Collaboration Suite 10g Release 1 (10.1.1) Infrastructure installed

Note: Although the sample configurations in this section are for UNIX, Oracle Collaboration Suite can also be installed on Microsoft Windows.

- OracleAS Single Sign-On configured to use a Kerberos realm
- Synchronization of Active Directory with Oracle Internet Directory
- Oracle Internet Directory configured to use the Windows external authentication plug-in

Configuration Tasks

To set up Windows native authentication, configure Oracle Internet Directory, the OracleAS Single Sign-On server, and the user's browser by performing the following tasks in the order listed.

Task 1: Verify That Microsoft Active Directory Is Set Up and Working

To ensure that Microsoft Active Directory is properly configured and running, consult the Windows 2000 server documentation.

Task 2: Install Oracle Internet Directory and OracleAS Single Sign-On

Install Oracle Internet Directory and OracleAS Single Sign-On. To determine which deployment configuration suits your installation, see the chapter about advanced configurations in *Oracle Application Server Single Sign-On Administrator's Guide*. For installation instructions, see the installation documentation for your operating system.

Task 3: Synchronize Oracle Internet Directory with Microsoft Active Directory

User entries in Oracle Internet Directory must be synchronized with user entries in Microsoft Active Directory.

Task 4: Configure Oracle Internet Directory to Use the Active Directory External Authentication Plug-in

See [Configuring the Active Directory External Authentication Plug-in](#) on page 9-36.

Task 5: Verify That Synchronization and the Active Directory External Authentication Plug-in Are Working

Log in to the OracleAS Single Sign-On server to verify that you have synchronized user entries between the two directories and that the Active Directory external authentication plug-in is working.

1. Go to the login page:

```
http://host:port/pls/orasso
```

2. Enter your user name in the following format:

```
user_name@active_directory_domain
```

3. Enter your password.

Task 6: Configure the OracleAS Single Sign-On Server

To configure the single sign-on server, complete the tasks described in the following topics.

- [Set Up a Kerberos Service Account for the OracleAS Single Sign-On Server](#)
- [Run the OracleAS Single Sign-On Configuration Assistant](#)

Set Up a Kerberos Service Account for the OracleAS Single Sign-On Server Create a service account for the OracleAS Single Sign-On server in Active Directory, then create a keytab file for the server, and map the service principal (the server) to the account name. The keytab file stores the server's secret key. This file enables the server to authenticate to the KDC. The service principal is the entity, in this case, the single sign-on server, to which the KDC grants session tickets.

1. Synchronize system clocks. The OracleAS Single Sign-On tier and the Windows 2000 server must match. If you omit this step, then authentication fails because there is a difference in the system time. Be sure the time, the date, and the time zones are synchronized.
2. Check the port number of the Kerberos server on the OracleAS Single Sign-On computer. The port where the Kerberos server listens is selected from `/etc/services` by default. On Microsoft Windows systems, the services file is found at `system_drive:\WINNT\system32\drivers\etc`. The service name is Kerberos. Typically the port is set to 88/udp and 88/tcp on the Windows 2000 server. When added correctly to the services file, the entries for these port numbers are:

```
kerberos5      88/udp      kdc          # Kerberos key server
kerberos5      88/tcp      kdc          # Kerberos key server
```

3. In the hosts file, located in the same directory as the services file, check the entry for the OracleAS Single Sign-On tier. The fully qualified host name of the OracleAS Single Sign-On computer must appear after the IP address and before the short name. The following is an example of a correct entry:

```
130.111.111.111 sso.MyCompany.com sso loghost
```

4. Log in to the Active Directory Management tool on the Windows 2000 server; then choose Users, then New, then user.

Enter the name of the OracleAS Single Sign-On host, omitting the domain name. For example, if the host name is `sso.MyCompany.com`, then enter `sso`. This is the account name in Microsoft Active Directory.

Note the password that you assigned to the account. You will need it later. Do *not* select **User must change password at next logon**.

5. Create a keytab file for the OracleAS Single Sign-On server, and map the account name to the service principal name. You perform both tasks by running the following command on the Windows 2000 server:

```
C:> Ktpass -princ HTTP/sso.MyCompany.com@MyCompany.COM -pass password -mapuser sso -out sso.keytab
```

The `-princ` argument is the service principal. Specify the value for this argument by using the format `HTTP/single_sign-on_host_name@KERBEROS_REALM_NAME`. Note that HTTP and the Kerberos realm must be uppercase.

Note that `single_sign-on_host_name` can be either the OracleAS Single Sign-On host itself or the name of a load balancer where multiple OracleAS Single Sign-On tiers are deployed. `MyCompany.COM` is a fictitious Kerberos realm in Microsoft Active Directory. The user container is located within this realm. The `-pass` argument is the account password that you obtained in Step 4. The `-mapuser` argument is the account name of the OracleAS Single Sign-On tier. You created this account in Step 4. The `-out` argument is the output file that stores the service key.

Be sure to replace the example values given with values suitable for your installation. These values appear in boldface in the example.

Note:

- If the `Ktpass` is not found on your computer, then download the Windows resource kit to obtain the utility.
 - The default encryption type for Microsoft Kerberos tickets is RC4-HMAC. Microsoft also supports DES-CBC and DES-CBC-MD5, two DES variants used in MIT-compliant implementations. `Ktpass` converts the key type of the KDC account from RC4_HMAC to DES when you run the tool as explained in Step 5.
-
-

6. Copy or FTP the keytab file, `sso.keytab`, created in step 5, to the OracleAS Single Sign-On middle tier, placing it in `$ORACLE_HOME/j2ee/OC4J_SECURITY/config`. If you use FTP, be sure to transfer the file in binary mode.

Be sure to give the Web server unique identifier (UID) on the OracleAS Single Sign-On tier read permission for the file.

Run the OracleAS Single Sign-On Configuration Assistant Running the `ossoca.jar` tool at this point does the following:

- It configures the single sign-on server to use the Sun JAAS login module.
- It configures the server as a secured application.

To run the `ossoca.jar` tool on the OracleAS Single Sign-On tier:

1. Back up the following configuration files:
 - `/sso/conf/policy.properties`

- /j2ee/OC4J_SECURITY/config/jazn.xml
- /opmn/conf/opmn.xml
- /j2ee/OC4J_SECURITY/config/jazn-data.xml
- /j2ee/OC4J_SECURITY/applications/sso/web/WEB-INF/web.xml
- /j2ee/OC4J_SECURITY/applications-deployments/sso/orion-application.xml

2. Run the ossoca.jar tool:

■ UNIX:

```
/sso/bin/ssoca
-mode sso
-oh $ORACLE_HOME
-ad_realm AD_REALM
-kdc_host_port kerberos_server_host:port
-verbose
```

■ Windows:

```
%ORACLE_HOME%\jdk\bin\java -jar %ORACLE_HOME%\sso\lib\ossoca.jar wna
-mode sso
-oh %ORACLE_HOME%
-ad_realm AD_REALM
-kdc_host_port kerberos_server_host:port
-verbose
```

AD_REALM is the Kerberos realm in Microsoft Active Directory. This is the user container. Note from the syntax that this value must be entered in uppercase. The default port number for the KDC is usually 88. To confirm this, see step 2 in the section ["Set Up a Kerberos Service Account for the OracleAS Single Sign-On Server"](#) on page 9-39.

3. Step 2 shuts down the OracleAS Single Sign-On server. Restart it:

```
/opmn/bin/opmnctl startall
```

Task 7: Configure the End User Browser

Configure Internet Explorer to use Windows native authentication. How you do this depends on which version you have.

- [Internet Explorer 5.0 and Later](#)
- [Internet Explorer 6.0 Only](#)

Internet Explorer 5.0 and Later

To configure Internet Explorer and later, perform the following steps:

1. From the menu bar, select **Tools**, and then **Internet Options**.
2. In the Internet Options dialog box, select the **Security** tab.
3. On the Security tab page, select **Local Intranet**, then select **Sites**.
4. In the Local intranet dialog box, select **Include all sites that bypass the proxy server**; then click **Advanced**.
5. In the advanced version of the Local intranet dialog box, enter the URL of the OracleAS Single Sign-On tier. For example:

```
http://sso.mydomain.com
```

6. Click **OK** to exit the Local intranet dialog boxes.
7. In the Internet Options dialog box, select the **Security** tab; then choose **Local intranet**; then choose **Custom Level**.
8. In the Security Settings dialog box, scroll down to the User Authentication section and then select **Automatic logon only in Intranet zone**.
9. Click **OK** to exit the Security Settings dialog box.
10. From the menu bar, select **Tools** and then **Internet Options**.
11. In the Internet Options dialog box, select the **Connections** tab.
12. On the Connections tab page, choose **LAN Settings**.
13. Confirm that the correct address and port number for the proxy server are entered, then click **Advanced**.
14. In the Proxy Settings dialog box, in the **Exceptions** section, enter the domain name for the OracleAS Single Sign-On server (`MyCompany.com` in the example).
15. Click **OK** to exit the Proxy Settings dialog box.

Internet Explorer 6.0 Only

If you are using Internet Explorer 6.0, perform steps 1 through 12 in "[Internet Explorer 5.0 and Later](#)" and then perform the following steps:

1. From the menu bar, select **Tools** and then **Internet Options**.
2. In the Internet Options dialog box, select the **Advanced** tab.
3. On the Advanced tab page, scroll down to the Security section.
4. Select **Enable Integrated Windows Authentication (requires restart)**.

Task 8: Reconfigure Local Accounts

After configuring Windows native authentication, you must reconfigure accounts for the Oracle Internet Directory administrator (`orcladmin`) and other local Windows users whose accounts are in Oracle Internet Directory. If you omit this task, then these users will not be able to log in.

Use the Oracle Directory Manager for Oracle Internet Directory to perform these steps:

1. Add the `orclADUser` class to the local user entry in Oracle Internet Directory.
2. Add the login ID of the local user to the `orclSAMAccountName` attribute in the user's entry. For example, the login ID of the `orcladmin` account is `orcladmin`.
3. Add the local user to the `exceptionEntry` property of the external authentication plug-in.

Fallback Authentication

Only browsers that are Internet Explorer 5.0 or later support SPNEGO-Kerberos authentication. OracleAS Single Sign-On provides fallback authentication support for unsupported browsers such as Netscape Communicator. Depending upon the type of browser and how it is configured, the user is presented with the OracleAS Single Sign-On login form or the HTTP basic authentication dialog box. In either case, the user must provide a user name and password. The user name consists of the Kerberos realm name and the user ID. The default way to enter the user name is shown in the following example.

`domain_name\user_id`

The following example, based on the example provided in ["Set Up a Kerberos Service Account for the OracleAS Single Sign-On Server"](#) on page 9-39, illustrates how to enter the user name:

`MyCompany.COM\jdoe`

Note that the user name and password are case sensitive. Additionally, password policies for Microsoft Active Directory do not apply. You can configure a different synchronization profile by using the Oracle directory integration and provisioning server. If you do, the login format just provided does not apply.

Fallback authentication is performed against Microsoft Active Directory, using an external authentication plug-in for Oracle Internet Directory.

Note:

- HTTP basic authentication does not support logout. To clear credentials from the browser cache, users must close all open browser windows. Alternatively, they can log out of the Windows computer.
 - In cases where basic authentication is invoked, users must set their language preference manually in Internet Explorer. From the menu bar, select **Tools, Internet Options, Languages**, and then enter the desired language.
-
-

Login Scenarios

Users may encounter a number of different login behaviors within Internet Explorer depending upon which version they are using. [Table 9–5](#) shows under what circumstances automatic sign-on and fallback authentication are invoked.

Table 9–5 Single Sign-On Login Options in Internet Explorer

Browser Version	Desktop Platform	Desktop Authentication Type	Integrated Authentication in Internet Explorer Browser	OracleAS Single Sign-On Login Type
5.0.1 or later	Windows 2000/XP	Kerberos V5	On	Automatic sign-on
5.0.1 or later but earlier than 6.0	Windows 2000/XP	Kerberos V5	Off	Single sign-on
6.0 or later	Windows 2000/XP	Kerberos V5 or NTLM	Off	HTTP basic authentication
5.0.1 or later but earlier than 6.0	Windows NT/2000/XP	NTLM	On or off	Single sign-on
6.0 or later	NT/2000/XP	NTLM	On	Single sign-on
5.0.1 or later	Windows 95, ME, Windows NT 4.0	Not applicable	Not applicable	Single sign-on
Earlier than 5.0.1	N/A	Not applicable	Not applicable	Single sign-on
All other browsers	All other platforms	Not applicable	Not applicable	Single sign-on

Configuring Synchronization of Oracle Internet Directory Foreign Security Principal References with Microsoft Active Directory

This section explains how to synchronize Oracle Internet Directory foreign security principal references with Active Directory.

Although Microsoft Active Directory stores information for group members in a trusted domain as foreign security principal references, Oracle Internet Directory stores the DNs of these members as they appear in Oracle Internet Directory. This results in a mismatch between an entry and its value as a member of a group. The relationship between a user and a group cannot be directly established in Oracle Internet Directory.

To establish the relationship between users and groups, the member DNs that refer to the foreign security principals must be replaced by the DNs of the entries during the synchronization of such groups. This is called resolving foreign key references.

Note: Synchronization of foreign security principal references is supported only on Windows 2003.

Example 9–5 How Foreign Key References Are Resolved

This example illustrates how foreign key references are resolved.

Assume that there are three domains: A, B and C.

Domain A has a one-way non-transitive trust to Domain B. It can have foreign security principal references for users and groups from Domain B.
Domain A has a one-way non-transitive trust to Domain C. It can have foreign security principal references for users and groups from Domain C.
Domain B has a one-way non-transitive trust to Domain C. It can have foreign security principal references for users and groups from Domain C.

In this example, the one-way non-transitive trusts are from Domain A to Domain B, from Domain A to Domain C, and from Domain B to Domain C.

Tasks to Resolve Foreign Key References

This section explains the steps for resolving foreign key references.

Task 1: Update Agent Configuration Information For each profile that can have foreign security principal references, perform the following steps. The sample configuration files referred further are available in `$ORACLE_HOME/ldap/odi/samples` directory.

1. Copy the `activeimp.cfg.fsp` file. The following is an example of the `activeimp.cfg.fsp` file:

```
[INTERFACEDetails]
  Package: gsi
  Reader: ActiveReader
[TRUSTEDPROFILES]
  prof1 : <Name of the profile1>
  prof2 : <Name of the profile2>
[FSPMAXSIZE]
  val=10000
```


The preceding example assumes you are using the DirSync change tracking approach. If you are using the USN-Changed approach for tracking changes, assign a value of `ActiveChgReader` to the `Reader` parameter.

2. In the `activeimp.cfg.fsp` file, under the `[TRUSTEDPROFILES]` tag, specify the profile names of the other domains that have foreign security principal references in this domain.

Referring to [Example 9-5](#), agent configuration information for Domain A contains the following:

```
[INTERFACEDetails]
  Package: gsi
  Reader: ActiveReader
[TRUSTEDPROFILES]
  prof1: profile_name_for_domain_B
  prof2: profile_name_for_domain_C
```

Agent configuration information for domain B contains the following:

```
[INTERFACEDetails]
  Package: gsi
  Reader: ActiveReader
[TRUSTEDPROFILES]
  prof1: profile_name_for_domain_C
```

Agent configuration information for domain C has no changes because domain C has no foreign key references.

3. Under the `[FSPMAXSIZE]` tag, specify the foreign security principal cache size. This can be the average number of foreign security principals you can have. A sample value of 1000 is specified in the `activeimp.cfg.fsp` file.
4. Load the new agent configuration information file by using the Directory Integration and Provisioning Assistant, as follows:

```
$ORACLE_HOME/bin/dipassistant modifyprofile
-profile profile_name_for_domain_A_or_B
-host host_name
-port port_name
-dn bind_DN
-passwd password_of_bind_DN
odip.profile.configfile=activeimp.cfg.fsp
```

5. Repeat this task for every profile of interest.

Task 2: Modify the Input Data Before Bootstrapping to Resolve the Foreign Security Principal References To do this, perform the following steps:

1. Get the LDIF dump from the Active Directory with appropriate filtering so that the resultant LDIF file contains only the required objects, for example users and groups.

Note: The command to dump entries from Microsoft Active Directory to Oracle Internet Directory is `ldifde`. This command can be run only from a Microsoft Windows environment.

2. Resolve the foreign security principal references by entering the following command:

```
$ORACLE_HOME/ldap/odi/admin/fsptodn
host=oid_host
port=oid_port
dn= OID_privileged_DN (that is, superuser or dipadmin user)
pwd=OID_password
profile=profile_name_for_domain_A_or_B
infile=input_filename_of_the_LDIF_dump_from_Active_Directory
outfile=output_filename
[sslauth=0|1]
```

By default, `host` is set to `local_host`, `port` is set to 389, and `sslauth` is set to 0.

Note: You can verify the successful execution of the command by verifying that the output file contains no references to `cn=foreignsecurityprincipals` in the member attribute. This command performs no attribute-level mapping other than resolving foreign security principal references.

3. Use the `-bootstrap` option of the Directory Integration and Provisioning Assistant to bootstrap the data from Microsoft Active Directory to Oracle Internet Directory.

See Also: ["Bootstrapping Data Between Directories"](#) on page 9-48

Task 3: Update the Mapping Rules to Resolve the Foreign Security Principals During Synchronization After bootstrapping, modifications to groups must be reflected in Oracle Internet Directory with the correct group membership values. The `fsptodn` mapping rule enables you to do this when you synchronize. Modify this mapping rule in every profile that needs foreign security principal resolution. Referring to [Example 9-5](#), the mapping rules must be modified for Domains A and B.

If you do not have DN mapping, then change your mapping rule for the `member` attribute to the following:

```
member: :group:uniquemember: :groupofUniqueNames: fsptodn(member)
```

If you have DN mapping, then change the mapping rules as follows:

1. Add the DN mapping rules corresponding to each of the trusted domains. This is used to resolve the correct domain mapping. Referring to [Example 9-5](#), the `domainrules` in the mapping file for Domain A should have content similar to the following:

```
DOMAINRULES
<Src Domain A >:<Dst domain A1 in OID>
<Src Domain B >:< Dst domain B1 in OID>
<Src Domain C>:<Dst domain C1 in OID>
```

2. Change your mapping rule for the `member` attribute to:

```
member::group:uniquemember::groupofUniqueNames:dnconvert(fsptodn(member))
```

Upload the mapping file for the different profiles using Directory Integration and Provisioning Assistant.

Managing Integration with Microsoft Active Directory

This section describes what to do immediately after configuration and ongoing administration tasks. It contains these topics:

- [Tasks After Configuring with Microsoft Active Directory](#)
- [Typical Management of Integration with Microsoft Active Directory](#)

Tasks After Configuring with Microsoft Active Directory

Once configuration is complete, do the following:

1. Migrate data from one directory to the other as needed. This is described in ["Bootstrapping Data Between Directories"](#) on page 9-48.
2. Enable the integration profile. You can do this by using either the Oracle Directory Integration and Provisioning Server Administration tool or the command-line version of the Directory Integration and Provisioning Assistant.

To enable the integration profile by using the Oracle Directory Integration and Provisioning Server Administration tool, perform the following:

- a. Launch the Oracle Directory Integration and Provisioning Server Administration by entering the following:


```
$ORACLE_HOME/bin/dipassistant -gui
```
- b. In the navigator pane, expand *directory_integration_and_provisioning_server*, then expand **Integration Profile Configuration**.
- c. In the navigator pane, select the configuration set. A list of the available profiles appears in the right pane.
- d. In the right pane, select the profile, then choose **Edit**. The General tab page window appears.
- e. In the General tab page, in the Profile Status field, select **ENABLE**.
- f. Click **OK**.

To enable the synchronization profile by using the command-line version of the Directory Integration and Provisioning Assistant, enter the following command:

```
$ORACLE_HOME/bin/dipassistant modifyprofile  
[-h host name] [-p port_number] [-D bind_DN] [-w password]  
-profile profile_name_in_OID odip.profile.status=ENABLE  
[-configset configset_number]
```

3. Start the Oracle directory integration and provisioning server using the configuration set that corresponds to that of the profile. Instructions for starting the server are available in Appendix A of *Oracle Identity Management Integration Guide*.

Typical Management of Integration with Microsoft Active Directory

Management tasks typically include:

- Managing synchronization profiles and mapping rules:
 - Creating new profiles. You create new profiles if you need to synchronize with an additional domain controller in a multiple domain Active Directory environment.

You can create new profiles by using existing profiles as templates. To do this, use the `createlike` command of the Directory Integration and Provisioning Assistant.

- Changing configurations (attributes) in the profile
- Disabling profiles to allow maintenance and then re-enabling them. Disabling profiles stops synchronization related to that profile.
- Managing mapping rules:
 - Creating new rules when additional attributes need to be synchronized
 - Changing existing rules when the way attributes are synchronized needs to change
 - Deleting or commenting out rules not required when a particular attribute is not required to be synchronized
- Managing access control
- Starting and stopping the Oracle directory server and the Oracle directory integration and provisioning server

This section contains these topics:

- [Bootstrapping Data Between Directories](#)
- [Managing the Active Directory External Authentication Plug-in](#)
- [Switching to a Different Microsoft Active Directory Domain Controller in the Same Domain](#)

See Also:

- ["Configuring Synchronization Profiles"](#) on page 9-17 for instructions on managing profiles, mapping rules, and access control
- *Oracle Identity Management Integration Guide* for instructions on starting and stopping servers

Bootstrapping Data Between Directories

Bootstrapping is sometimes called data migration. To bootstrap data, do the following once the Active Directory Connector and plug-in configurations are complete:

1. Identify the data you want to migrate. You can choose to migrate all data in the directory or only a subset of data.
2. Make sure the synchronization is not enabled yet.
3. Bootstrap from one directory to another by using the Directory Integration and Provisioning Assistant with the `-bootstrap` option. Bootstrapping is described in Chapter 8 of *Oracle Identity Management Integration Guide*.

Once bootstrapping is accomplished, the profile status attributes are appropriately updated in the synchronization profile by the Directory Integration and Provisioning Assistant.

4. If you used LDIF file-based bootstrapping, then initialize the `lastchangekey` value with the Directory Integration and Provisioning Assistant as follows:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -updln
```

This `lastchangekey` attribute should be set to the value of the last change number in the source directory before you started the bootstrap.

In order to update the last change number, the value assigned to the `odip.profile.condirurl` property in the import synchronization profile must be for a non-SSL connection. If you have already configured the import synchronization profile for SSL, then before attempting to update the last change number, you must temporarily change the value assigned to the `odip.profile.condirurl` property so it points to a non-SSL port.

5. If two-way synchronization is required, then enable the export profile and make sure the change logging option is enabled for the Oracle directory server. Change logging is controlled by the `-l` option while starting Oracle Internet Directory. By default, it is set to `TRUE`, meaning that change logging is enabled. If it is set to `FALSE`, then use the OID Control Utility to shut down the Oracle directory server, and then to start the server again with the change log enabled.

Managing the Active Directory External Authentication Plug-in

This section explains how to delete, disable, and re-enable the Active Directory external authentication plug-in.

Deleting the Active Directory External Authentication Plug-in To delete the Active Directory external authentication plug-in, enter the following commands:

```
ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhencompare,cn=plugin,cn=subconfigsubentry"
```

```
ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhenbind,cn=plugin,cn=subconfigsubentry"
```

Disabling the Active Directory External Authentication Plug-in To disable the Microsoft Active Directory external authentication plug-in:

1. Create an LDIF file with the following entries:

```
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
```

```
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
```

2. Load the LDIF file with the `ldapmodify` command, as follows:

```
ldapmodify -h host -p port -D cn=orcladmin -w password -f fileName
```

Re-Enabling the Active Directory External Authentication Plug-in To re-enable the Active Directory external authentication plug-in, use these two commands:

1. Create an LDIF file with the following entries:

```
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
```

```
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
```

```
replace: orclpluginenable  
orclpluginenable: 1
```

2. Load the LDIF file with the `ldapmodify` command, as follows:

```
ldapmodify -h host -p port -D cn=orcladmin -w password -f fileName
```

See Also:

- ["Configuring the Active Directory External Authentication Plug-in" on page 9-36](#)
- ["Enabling the Active Directory External Authentication Plug-ins" on page 9-37](#)

Switching to a Different Microsoft Active Directory Domain Controller in the Same Domain

This section explains how to change the Microsoft Active Directory domain controller to which changes are exported. There are two methods, one for the USN-Changed approach and the other for the DirSync approach.

How to Change the Active Directory Domain Controller by Using the USN-Changed Approach

If you are using the USN-Changed approach, then perform the following steps:

1. Stop the current running profile. Modify the Microsoft Active Directory host connection information, that is, host, port, user, password, to point to the new host. Usually, the host name is the only item that you need to update.
2. Obtain the current value of the `highestCommittedUSN` by searching the new domain controller's root DSE for the current `uSNChanged` value (attribute value of the `highestCommittedUSN` attribute of the root DSE):

```
ldapsearch -h host -p port -b "" -s base -D user  
DN -w password "objectclass=*" highestCommittedUSN
```

3. Use Oracle Directory Integration and Provisioning to run a full synchronization from Microsoft Active Directory.
 - a. Run `ldifde`, the command to dump entries from Microsoft Active Directory to Oracle Internet Directory, using the intended `ldapsearch` scope and search filter. Normally, the search filter should be the same as that specified in the running profile. For example, the following search filter is set in the sample properties file: Note that `ldifde` can be run only from a Microsoft Windows environment.

```
searchfilter=(&(|(objectclass=user)(objectclass=organizationalunit))(!(objectclass=group)))
```

Essentially, run `ldifde` with a search scope and search filter that retrieve all Oracle Internet Directory objects (entries) that were configured to be synchronized with Microsoft Active Directory by the running profile.

- b. Run Oracle Directory Integration and Provisioning to upload the LDIF file generated in Step a using the same profile.
4. After the full synchronization is completed, update the `lastchangenumber` attribute with the `highestCommittedUSN` value obtained in Step 2.
 5. Resume the normal synchronization, that is, incremental synchronization from Microsoft Active Directory using `uSNChanged` attribute.

How to Change the Active Directory Domain Controller by Using the DirSync Approach

If you are using the DirSync approach, then perform the following steps:

1. Stop the current profile that is running.
2. Use the Directory Integration and Provisioning Assistant `createlike` option to create a new profile exactly the same as the profile already being used. In the newly created profile, modify the Microsoft Active Directory host connection information, that is, host, port, user, password, to point to the new host. Usually, the host name is the only item you need to update.
3. Resume normal synchronization with the modified profile. Note that all the domain controllers must be in the same Active Directory domain.

Monitoring and Tuning Oracle Collaboration Suite Performance

This chapter describes how to monitor daily performance and fine-tune the configuration parameters using Grid Control, Oracle Collaboration Suite Control, component administrator GUIs, and command-line tools.

This chapter includes the following sections:

- [Performance Tuning Oracle Collaboration Suite](#)
- [Monitoring and Tuning the Oracle Collaboration Suite Database](#)

Performance Tuning Oracle Collaboration Suite

This section discusses performance tuning information for the Oracle Collaboration Suite components. Topics include:

- [Tuning Oracle Calendar](#)
- [Tuning Oracle Mail](#)
- [Tuning Oracle Content Services](#)
- [Tuning Oracle Ultra Search](#)
- [Tuning Oracle Real-Time Collaboration](#)
- [Tuning Oracle Voicemail & Fax](#)
- [Tuning Oracle Mobile Collaboration](#)
- [Tuning Oracle Workspaces](#)

Tuning Oracle Calendar

See Appendix A, "Disk Space and Memory" in the *Oracle Calendar Administrator's Guide* for disk space and memory requirements.

See Appendix B, "Adjusting Calendar Kernel Parameters" in the *Oracle Calendar Administrator's Guide* for performance tuning information for Oracle Calendar.

Tuning Oracle Discussions

There are mainly three sets of configuration parameters that can be used to tune Oracle Discussions: OID connection parameters, database connection parameters, and Discussions in memory caches.

Oracle Internet Directory Connection Parameters

Oracle Discussions shares the same Oracle Internet Directory connection pool used by Oracle WebMail. The Oracle Internet Directory connection pool can be configured by editing the properties located in the file `oc4.properties` for the `OC4J_OCSCClient` container. The file path is `ORACLE_HOME/j2ee/OC4J_OCSCClient/config/oc4j.properties`. The following properties are available:

- `oracle.ocs.ldappool.initialsize`
- `oracle.ocs.ldappool.minsize`
- `oracle.ocs.ldappool.maxsize`
- `oracle.ocs.ldappool.shrinkinterval`
- `oracle.ocs.ldappool.timeoutinterval`
- `oracle.ocs.ldappool.incrementsize`
- `oracle.ocs.ldappool.reconnecttime`

Please refer to "[Oracle WebMail Parameter Recommendations](#)" on page 10-10 for details on how to configure the Oracle Internet Directory connection pool.

Database Connection Parameters

Oracle Discussions shares the same database connection pool used by Oracle WebMail. The database connection pool can be configured by editing the properties located in the file `oc4.properties` for the `OC4J_OCSCClient` container. The file path is `ORACLE_HOME/j2ee/OC4J_OCSCClient/config/oc4j.properties`. The following properties are available:

- `oracle.mail.sdk.esmail.connpool_min_limit`
- `oracle.mail.sdk.esmail.connpool_max_limit`
- `oracle.mail.sdk.esmail.connpool_increment`
- `oracle.mail.sdk.esmail.cache_inactivity_timeout`
- `oracle.mail.sdk.esmail.thread_wakeup_interval`

Please refer to "[Oracle WebMail Parameter Recommendations](#)" on page 10-10 for details on how to configure the database connection pool.

Oracle Discussions Caches

Oracle Discussions caches frequently accessed topics and messages in memory. Oracle Discussions caches can be monitored and configured using Oracle Collaboration Suite Control.

The Oracle Discussions component home page in Oracle Collaboration Suite Control displays the current cache settings and the current cache usage.

To configure cache sizes and behavior:

1. From the Oracle Collaboration Suite home page for the Applications tier hosting Oracle Discussions, select the **J2EE Applications** tab.
2. Select the **Discussions** link in the list of J2EE applications. The Application: discussions page loads.
3. Select the **Server** link in the Web Modules list. The Web Module: server page loads.

4. Select **Environment** from the **Properties** list in the **Administration** section of the page. The Environment page loads. From this page, you can configure cache sizes and behavior.

For optimal performance, Oracle suggests using the maximum cache size for category, forum, topic, and system, so the cache is never full. Cache sizes and behavior can be configured through the following parameters:

- **oracle.discussions.cache.containers.info.ttl**: In an environment where Oracle Discussions is deployed in more than one OC4J instance, Oracle Discussions will periodically check the message store database for updates by other instances. This time to live parameter will determine how frequently (in milliseconds), for a given forum, Oracle Discussions will check the database for updates by other instances. The recommended values are:
 - For a single Oracle Discussions instance deployment, use -1 to disable checking, because no periodic check for updates is required.
 - For a multi- Oracle Discussions instance deployment, use 60000 (milliseconds), so Discussions will check of other instances for updates once every minute.
- **oracle.discussions.cache.containers.max_size**: Maximum size in bytes for the cache's region dedicated to category information, such as display name and description.
- **oracle.discussions.cache.boards.max_size**: Maximum size in bytes for the cache's region dedicated to forum information such as last post, number of topics and messages.
- **oracle.discussions.cache.threads.max_size**: Maximum size in bytes for the cache's region dedicated to topic information such as topic subject, author, number of replies.
- **oracle.discussions.cache.messages.max_size**: Maximum size in bytes for the cache's region dedicated to message information such as subject, author, and message text body. This cache can grow quite large.
- **oracle.discussions.cache.system.max_size**: Maximum size in bytes for the cache's region dedicated to some system information, including popular topics and last posts.
- **oracle.discussions.cache.user_profile.max_size**: Maximum size in bytes for the cache's region dedicated to some user profile information such as user's known-as name, first and last name, and location.
- **oracle.discussions.cache.user_profile.ttl**: Time to Live in milliseconds for the cached user profile information. When the time expires, Oracle Discussions will reload user's profile information from Oracle Internet Directory. A typical value (in milliseconds) is 3600000 (1 hour).
- **oracle.discussions.cache.system.popular_threads.cache_loader.ttl**: Frequency in milliseconds used to reload the list of popular topics from the database. This parameter is related to the refresh rate of the ES_POPULAR_THREADS table, in the ES_MAIL schema. The default refresh rate is 10 minutes.

Oracle Discussions Logs

Oracle Discussions uses the discussions J2EE application for its logging. The log files are located under `ORACLE_HOME/j2ee/OC4J_OCSCClient/application-deployments/discussions/<oc4j_`

island>/application.log. The logs are also accessible through Oracle Collaboration Suite Control as part of the logs of the OC4J_OCSCliant instance.

To configure logging level:

1. From the Oracle Collaboration Suite home page for the Applications tier hosting Oracle Discussions, select the **J2EE Applications** tab.
2. Select the **Discussions** link in the list of J2EE applications. The Application: discussions page loads.
3. Select the **Server** link in the **Web Modules** list. The Web Module: server page loads.
4. Select **Environment** from the **Properties** list in the **Administration** section of the page. The Environment page loads. From this page, you can configure logging level.

Set the level by editing **oracle.discussions.log.level**. Valid values for the logging level are: fatal, error, assert, warn, info, debug.

Tuning Oracle Mail

This section provides an overview of Oracle Mail architecture, details of the major tunable components, and guidelines for scaling the system. It also includes a section describing typical symptoms of performance problems, how to identify the limiting component, and solutions for solving the problems.

See the *Oracle Mail Administrator's Guide* for information about monitoring Oracle Mail processes.

This section contains the following topics:

- [Overview of the Oracle Mail Architecture](#)
- [Understanding the Breakdown of Costs](#)
- [Recommended Database Connection Settings](#)
- [Recommended LDAP Connection Settings](#)
- [Oracle Mail Parameter Recommendations](#)
- [Monitoring CPU Usage for Oracle WebMail](#)
- [Monitoring JavaMail API Response Time for Oracle WebMail](#)
- [Determining the Optimum Database Pool Size for Oracle WebMail](#)
- [Oracle WebMail Parameter Recommendations](#)

Overview of the Oracle Mail Architecture

This section provides a brief overview of the Oracle Mail architecture and processes. This information is intended to help you understand the tuning recommendations included in this section.

Oracle Mail Processes

[Table 10–1](#) describes the Oracle Mail processes.

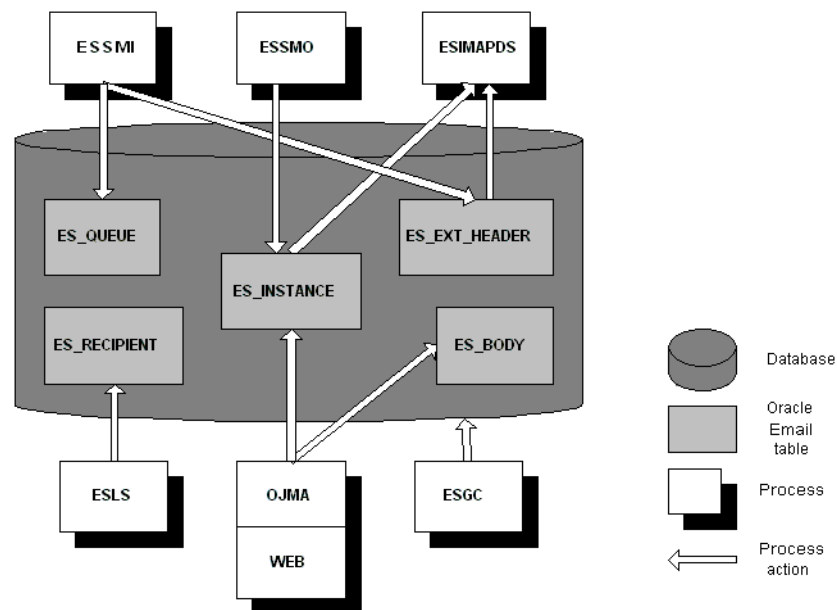
Table 10–1 Oracle Mail Processes

Process	Description
ESSMI	The inbound SMTP process

Table 10–1 (Cont.) Oracle Mail Processes

Process	Description
ESSMO	The outbound SMTP process
ESIMAPDS	The IMAP process
ESLS	The list server process
OJMA	An underlying technical base used by Web clients and other applications to access the message store. This is not a server.
ESGC	The housekeeping process that cleans up all transient tables within the Oracle Mail schema.

Figure 10–1 is an overview of the Oracle Mail processes and their interactions with the database.

Figure 10–1 Oracle Mail Processes

In Figure 10–1, the ESSMI process is acting in submit-only mode, allowing the outbound SMTP process ESSMO to perform message delivery. The Oracle directory server (part of Oracle Internet Directory), is not represented. The consumers of the Oracle Internet Directory server for user authentication purposes are the list server, the SMTP delivery module (ESSMO), and IMAP processes.

Mail Flow

The following steps describe an overview of the flow for a message entering the system:

1. An incoming message is inserted by ESSMI into the queue tables, ES_QUEUE and ES_RECIPIENT, and into the tables handling the content and metadata, ES_INSTANCE, ES_EXT_HEADER, ES_SHELL, and ES_BODY.
2. The ESSMO process performs an LDAP lookup to determine whether the message recipient(s) are local or not.

1. If the recipient(s) are local, ESSMO inserts a record into the pointer table, ES_INSTANCE, and updates the recipients' usage in the ES_USER and ES_FOLDER tables.
2. If the recipient(s) are not local, ESSMO forwards the mail message.

The following steps describe the flow for a user reading a message:

1. Using a Web, POP3, or **IMAP client**, a user requests a specific message to read.
2. The server collects the message body from the ES_BODY table and then finds the metadata (number of attachments, sender, and so on) of the body from the ES_SHELL, ES_HEADER, and ES_EXT_HEADER tables.
3. The server constructs the message in the format the protocol expects and sends it over the network for the user to view.

Understanding the Breakdown of Costs

The costs of an Oracle Mail system can be broken into three tiers: very costly, moderately costly, and inexpensive. These cost values are relative to other operations on the system. The following descriptions are provided to help you understand how changes in user behavior or application design can impact the hardware tiers.

What is Very Costly

For the database: Opening a folder. The list of all the user's messages must be retrieved from the database. The cost increases linearly with the size of the folder. This cost is not as high when the table is reorganized as an index-oriented table.

For the Applications tiers: IMAP fetch new headers operation. Fetching a new list of headers from the client requires the ESIMAPDS process to parse each message shell, which is an expensive CPU operation. This operation occurs when a user opens their inbox and downloads all unseen headers. This operation for a first-time user will be for all messages in their folder. For subsequent open folder calls, only new messages are downloaded.

What is Moderately Costly

For the database:

- Delivering a mail message. New records must be inserted into at least seven tables with the appropriate indexes maintained. Several of the queue tables are updated multiple times as the message moves through various states.
- Reading a mail message. The large object (LOB) in ES_BODY must be fetched and the other meta-tables queried to construct the message.
- The housekeeping process. The ESGC process marks and then sweeps the entire mail store for de-referenced bodies as well as clean up the queue and instance tables. This is not inexpensive, but the limiting factor can often be physical input/output constraints, as the objects that the housekeeping process is interested in are unlikely to be in the buffer cache.
- Performing a `get new mail` or `noop:` call. This causes the server to check for new instances for a particular folder identifier.

What is Inexpensive

For the database:

- Changing flags of mail messages. This occurs during operations such as marking a mail message read or marking it deleted.

- Reading a mail message already in the buffer cache. The message is already in the buffer, so no additional retrieval is needed.
- Delivering a message to multiple recipients. A large amount of the necessary mail database work has already been performed for delivering the message to a single recipient. Delivery to any additional recipients, especially in the case of a distribution list, is very inexpensive because only new `ES_INSTANCE` records are created.

For the Applications tiers:

- SMTP accepting a mail message. Given the efficiency of the Net8 Listener and Oracle Mail SMTP code, little processing power is necessary from the `ESSMT` component to insert a mail message.
- SMTP performing message delivery. The cost here is the Applications tier process, not the database. For example, a single E250 with two 300Mhz processors was able to easily handle delivery of 75,000 messages an hour.

Recommended Database Connection Settings

Database connection limits have a large effect on system performance. Setting the limit too low can lead to unnecessary client failures. Setting it too high can lead to wasted memory on the Applications tier and less efficient consumption of the physical memory on the back end database due to the size of the shadow processes.

Use the `oesmon` utility to obtain metric data about the database connections. Use the following command to determine the database connection usage per IMAP instance. For example:

```
oesmon get rgmum4:um_system:imap.DUMP.DBconnections.dump
```

The database connection pool algorithm starts at the top of the pool for each request and moves down the list until an available connection is located. Because of this, the database connection usage is pyramidal in shape: The first connection handles a large percentage of the load, the next connection handles a smaller percentage, and so on. The slope of this shape indicates the rate at which the database is servicing requests: A steep slope indicates a quick response, while a flat slope indicates a slow response. When evaluating this data, look for the connection at which the execution count becomes zero. This indicates that the pool at this point is large enough to accommodate the demands made on it. Resize the maximum database connection pool to this value or greater.

Recommended LDAP Connection Settings

The best way to determine the usage statistics for the LDAP connection pool is to set the minimum pool setting to a small number, increment the count by one, and then use the following command to determine how many LDAP connections were created:

```
netstat -a | grep ldap | grep ESTABLISHED | wc -l
```

Note that for some operating systems, you must specify the LDAP port instead of `ldap` in the command. The default LDAP port is 389.

Oracle Mail Parameter Recommendations

[Table 10–2](#) describes the parameters that affect the performance of Oracle Mail. These parameters can be accessed and edited through Oracle Enterprise Manager 10g. They are located on the server pages listed under Unified Messaging.

Note: You should use the recommended values to start with. However, the actual values could vary for one deployment to another, depending on the number of users, and mail traffic/load of the deployment. You should start with the default values, monitor your system's performance for a few days, and then adjust the values according to your specific deployment.

Table 10–2 *Parameter Recommendations for Oracle Mail*

Parameter	Description	Recommended Value
LDAP Maximum Connection Pool	Determines the maximum number of LDAP connections.	20
LDAP Minimum Connection Pool	Determines the minimum number of LDAP connections. Specify the number of connections required to handle 60% of the peak load.	5
LDAP Connection Pool Increment	The size increment by which to increase the pool of LDAP connections. If a large number of requests arrive at the same time, the pool may not be able to grow quickly enough and some connections will be refused.	1
LDAP Connection Retry Interval	The time to sleep (in microseconds) between attempts to make an LDAP connection. If the value is too large, response time can suffer because the process will sleep for too long a time interval even if an LDAP connection is available.	100000
LDAP Number of Retry Before Erroring	Number of time to try making an LDAP connection before ending the query. If the pool is full, the process will sleep for the value specified for the LDAP Connection Retry Interval parameter.	10
Get New Mail Interval	The time to sleep (in seconds) before entering administrative statistics into the database. If the value is too low, the frequent writes to the database will slow system performance.	600 (7200 for housekeeping processes)
Protocol Server Maximum Threads	The maximum number of threads available for client connection handling.	50
Protocol Server Minimum Threads	The minimum number of threads available for client connection handling.	10
Protocol Server Increment Thread	The number of threads to add to the client connection pool.	1

Table 10–2 (Cont.) Parameter Recommendations for Oracle Mail

Parameter	Description	Recommended Value
Maximum Number of Clients	The maximum number of concurrent connections. If the value is too large, IMAP will attempt to handle connections that the listener is rejecting. If the value is too small, an unnecessary number of IMAP processes will need to be configured.	1000
Timeout Interval	The length of time (in seconds) until the server disconnects idle sockets	1800
Submit Only	The delivery behavior of the SMTP inbound server. Setting this value to FALSE can cause long insert times on the inbound Oracle Mail server.	TRUE

Recommended Database Process Parameter Settings

[Table 10–3](#) describes the database process parameters that you can change in order to affect the performance of Oracle Mail.

Note: You should use the recommended values to start with. However, the actual values could vary for one deployment to another, depending on the number of users, and mail traffic/load of the deployment. You should start with the default values, monitor your system's performance for a few days, and then adjust the values according to your specific deployment.

Table 10–3 Database Process Parameter Recommendations for Oracle Mail

Parameter	Minimum Value	Maximum Value	Increment
ESIMAPDS	10	50	2
ESSMI	10	50	2
ESSMO	10	50	2

Monitoring CPU Usage for Oracle WebMail

Use the `sar` or `vmstat` operating system utilities to determine CPU load by averaging the values over ten minute periods. No more than 90% of the CPU resources should be used. Depending on the platform, a Java Virtual Machine might not be able to schedule threads on other processors. Because of this, when running one Java Virtual Machine on a two CPU computer you might only see 50% CPU utilization. However, that Java Virtual Machine might be using 100% of one of the CPUs.

Monitoring JavaMail API Response Time for Oracle WebMail

Set the parameter `oracle.mail.sdk.esmail.timing` to true to display timing data. Use this information to determine whether database or LDAP connection times

are slow. If database connection response times are slow, as shown by the timing data and by IMAP client observation, database performance must be tuned.

If LDAP connection times are slow, use the Oracle Internet Directory Statistics Collection tool (`oidstats.sh`) to generate data required by the Oracle Optimizer to choose an optimal plan to execute the queries corresponding to the LDAP operations. If LDAP connection times are still slow, monitor the CPU usage of the machine and check the network round-trip times.

Determining the Optimum Database Pool Size for Oracle WebMail

Set the Oracle WebMail parameter `oracle.mail.sdk.esmail.dbpool_timing` to `true` in order to generate a line marked `Active` in the Oracle WebMail log files. If you set the parameter to `true` for a single day and then search for the `Active` lines in the log files, you can determine the number of daily active database connections. By correlating this information with the timestamp, you can determine the peak number of database connections used. Use this information to determine whether the database connection pool is set correctly.

Oracle WebMail Parameter Recommendations

Table 10–4 describes the Oracle WebMail process parameters that you can change in order to affect the performance of your system. These values are located in the file `oc4j.properties` for the OC4J_UM container.

Note: You should use the recommended values to start with. However, the actual values could vary for one deployment to another, depending on the number of users, and mail traffic/load of the deployment. You should start with the default values, monitor your system's performance for a few days, and then adjust the values according to your specific deployment.

Table 10–4 Parameter Recommendations for Oracle WebMail

Parameter	Description	Recommended Value
<code>client.mail.defaultsort</code>	If <code>TRUE</code> , the Oracle WebMail client automatically sorts by the default sort field and order, when user first logs in.	<code>FALSE</code>
<code>client.esdsconnpoolparam.incrementsize</code>	Number of connections to add to the ESDS client connection pool	5
<code>client.esdsconnpoolparam.initialsize</code>	Initial number of connections in the ESDS client connection pool	30
<code>client.esdsconnpoolparam.maxsize</code>	Maximum number of connections in the ESDS client connection pool	60
<code>client.esdsconnpoolparam.minsize</code>	Minimum number of connections in the ESDS client connection pool	30
<code>client.esdsconnpoolparam.shrinkingtimeoutinterval</code>	Time delay before ESDS client connection pool can be shrunk	1800

Table 10–4 (Cont.) Parameter Recommendations for Oracle WebMail

Parameter	Description	Recommended Value
<code>client.esdsconnpoolparam.timeoutinterval</code>	Maximum number of seconds the ESDS client waits for a free connection in the pool. If no connections are released back to the pool within that time, the directory server code throws an exception.	30
<code>jdbc.connection.debug</code>	Enables or disables debugging JDBC connections	FALSE
<code>mail.debug</code>	Enables or disables debugging OJMA API for Oracle Mail. If enabled, this adversely effects performance.	FALSE
<code>oracle.mail.ldap.reconnecttime</code>	The amount of time in seconds the server waits to reconnect to the Oracle directory server if it is unavailable.	4
<code>oracle.mail.sdk.esmail.timing</code>	Prints timing data. This is used to determine slow LDAP and database access times.	FALSE Set to TRUE only when debugging performance issues. See Section , "Monitoring JavaMail API Response Time for Oracle WebMail" on page 9 for more information.
<code>oracle.mail.sdk.esmail.ldap_debug</code>	Enables or disables debugging OJMA API for LDAP.	FALSE
<code>oracle.mail.sdk.esmail.dbpool_timing</code>	Prints the active and total count of database connections. This is used to determine if the database pool is sized correctly.	FALSE Set to TRUE when sizing the database connection pool. See "Determining the Optimum Database Pool Size for Oracle WebMail" on page 10 for more information.
<code>oracle.mail.sdk.esmail.cache_inactivity_timeout</code>	Number of seconds to wait for a connection before the ESDS client connection pool times out	600
<code>oracle.mail.sdk.esmail.connpool_max_limit</code>	Maximum number of connections in the Oracle mail sdk esmail connection pool	20

Table 10–4 (Cont.) Parameter Recommendations for Oracle WebMail

Parameter	Description	Recommended Value
<code>oracle.mail.sdk.esmail.connpool_min_limit</code>	Determines the initial or minimum number of connections created in the connection pool. Oracle recommends keeping this limit as low as possible to avoid holding on to unused database connections.	5
<code>oracle.mail.sdk.esmail.cache_scheme</code>	Determines the cache scheme of the database connection pool. A value of 3 sets the parameter to <code>FIXED-NO-WAIT</code> , which returns null if a connection is not available in the pool.	3

Tuning Oracle Content Services

Oracle Content Services Administrator's Guide contains performance tuning information for Oracle Content Services. See the following chapters:

- Chapter 7, "Monitoring Domain, Node, and Service Performance"
- Chapter 10, "Oracle Content Services Maintenance and Tuning"
- Appendix A, "Troubleshooting Oracle Content Services"

Tuning Oracle Ultra Search

See Appendix A, "Tuning the Web Crawling Process" and Appendix B, "Tuning Query Performance" in the *Oracle Ultra Search Administrator's Guide* for performance tuning information.

Tuning Oracle Application Server Portal

See Chapter 9, "Tuning Performance in OracleAS Portal" in *Oracle Application Server Portal Configuration Guide* for performance tuning information.

Tuning Oracle Real-Time Collaboration

You can monitor Oracle Real-Time Collaboration processes using the `rtctl` utility, and by evaluating the Current Conferences reports in the **Reports** tab of the Oracle Real-Time Collaboration Web Client pages. You can also review Quality of Service reports from the same tab, to evaluate system efficiency and responsiveness. See Chapter 6, "Historical and Statistical Reports for Oracle Real-Time Collaboration" in *Oracle Real-Time Collaboration Administrator's Guide* for details about evaluating system performance.

Increasing Conference Server and Listening Processes

If you determine that your system is not responding adequately, you may choose to increase the number of processes listening for client requests for Web conferencing and instant messaging services. You can also increase the number of conferencing server processes. The Multiplexer is the process that listens for Web conferencing client requests to the Oracle Web Conferencing Server, and the Client Connection Manager is the process that listens for instant messaging client requests to the Oracle Presence

Server. By default, one multiplexer, one connection manager, one presence server and four conference server processes are started when Oracle Real-Time Collaboration is installed and configured on an Applications tier.

Note: You cannot increase the number of Oracle Presence Server processes. There can be only one presence server process running at a time for an entire Oracle Real-Time Collaboration system. If the server process goes down, a special high availability process for the presence server will attempt to restart it automatically. If the presence server instance is down, a waiting high availability process for another server process on another Oracle Real-Time Collaboration instance starts that presence server. See "Automatic Process Monitoring" in Chapter 5 of *Oracle Real-Time Collaboration Administrator's Guide* for details.

You use the `rtcctl` utility to set the number of processes as follows.

```
$ORACLE_HOME/imeeting/bin/rtcctl
rtcctl> setProperty -ct confsvr -pname SrvNumProcs -pvalue 8
rtcctl> setProperty -ct mx -pname SrvNumProcs -pvalue 2
rtcctl> setProperty -ct connmgr -pname SrvNumProcs -pvalue 2
rtcctl> exit
```

The example sets eight conference server processes (`confsvr`), two multiplexer (`mx`) processes, and two connection manager (`connmgr`) processes.

See "Increasing Component Processes and Connections" in Chapter 3 of *Oracle Real-Time Collaboration Administrator's Guide* for more details about these properties.

Increasing Messaging Connections

In addition to increasing the available number of Client Connection Manager properties as described in the previous section, you can also increase the maximum number of connections each connection manager process can handle. Use the `rtcctl` utility to set the number of connections as follows:

```
$ORACLE_HOME/imeeting/bin/rtcctl
rtcctl> setProperty -system true -pname IMMaxConnections -pvalue 2000
```

The example sets the maximum number of concurrent connections to 2,000. See "Increasing Component Processes and Connections" in Chapter 3 of *Oracle Real-Time Collaboration Administrator's Guide* for more details about these properties.

If you change this property, you should also make sure that the maximum number of open file descriptors allowed on your system matches the number you enter here. See ["Increasing the Number of Open File Descriptors Used for Client Connections"](#) on page 10-13 for details.

Increasing the Number of Open File Descriptors Used for Client Connections

The number of connections the Oracle Real-Time Collaboration Multiplexer and Client Connection Manager processes can handle on a UNIX, Linux, or Solaris system is limited by the number of open file descriptors allowed on the system. You can set this limit using the `ulimit` command (`sh`, `ksh`, `bash`), the `limit` command (`csh`, `tcsh`), or by changing entries in a configuration file for your operating system, such as `/etc/security/limits.conf` or `/etc/sysctl.conf`.

If the number of file descriptors is limited to 1024, a single multiplexer or connection manager process can handle about 1,000 users. If users are consistently unable to connect to multiplexer or client connection manager processes, you may need to increase the number of open file descriptors allowed.

1. To reset the limit, you must also stop and restart Oracle Real-Time Collaboration processes. Inform your users that you will be stopping Web conferencing and messaging processes before following the next steps.
2. Stop the Oracle Real-Time Collaboration OC4J_imeeting and core component processes:

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J process-type=OC4J_imeeting
$ORACLE_HOME/imeeting/bin/rtcctl
rtcctl> stop
```

3. Edit the appropriate configuration file for your operating system (such as `/etc/security/limits.conf`), or use `ulimit` or `limit` to set the number of open files or file descriptors a process may have. The method you choose to set this depends on your operating system, and whether you wish to control this at runtime with a command, or to set limits in default configuration files for particular users or groups of users.

For example, to set the limit for members of the group called "users" in your `limits.conf` file on UNIX to 2000 open file descriptors, you could enter the following:

```
vi /etc/security/limits.conf
# Allow anyone in the 'users' group to open 2000 files.
@users          hard    nofile 2000
```

Or to set the limit for all users at runtime, you could use `ulimit` on a standard Bourne shell as follows:

```
ulimit -n 2000
```

See your operating system documentation for more information about the best way to set open file descriptors.

4. Restart the Oracle Real-Time Collaboration OC4J_imeeting and core component processes:

```
$ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OC4J process-type=OC4J_imeeting
$ORACLE_HOME/imeeting/bin/rtcctl
rtcctl> start
```

Tuning Oracle Voicemail & Fax

See Chapter 13, "Performance Tuning," in *Oracle Voicemail & Fax Administrator's Guide* for information on tuning the Oracle Voicemail & Fax system.

Tuning Oracle Mobile Collaboration

See Chapter 13, "Server Performance Monitoring" in the *Oracle Mobile Collaboration Administrator's Guide* for performance monitoring information.

Tuning Oracle Workspaces

Oracle Workspaces provides system properties for controlling application sizing and performance.

Setting Oracle Workspaces Properties

You can set the sizing and performance properties using Oracle Collaboration Suite Control. These properties are all stored in the `web.xml` file.

To set Oracle Workspaces environment properties:

1. From the Applications tier home page, select the `OC4J_OCSCClient` instance. The `OC4J_OCSCClient` home page is displayed.
2. Click the **Oracle Workspaces** link in the Deployed Applications table. The Application: Workspaces page is displayed.
3. Click the **workspaces** link in the Web Modules table. The **Web Module: workspaces** page is displayed.
4. Click the **Environment** link under the Properties list in the Administration section. The Environment page is displayed.
5. Make your changes to the Oracle Workspaces environment properties. Under the Environment Entries heading, you can view the various properties and override the default values.
6. When you are finished making changes, click **Apply**. Your environment properties changes will be applied. If you want to reject all changes you have made, click **Revert**.

The Oracle Workspaces properties are described in the following sections:

- [Adjusting Oracle Workspaces Sizing](#)
- [Adjusting Oracle Workspaces Performance](#)
- [Investigating Oracle Workspaces Performance](#)

Adjusting Oracle Workspaces Sizing

Oracle Workspaces provides the following system properties to control application sizing.

Database Connection Pool Size The following properties determine the initial, minimum, and maximum size of the database connection pool that Oracle Workspaces uses to access and manage workspace metadata. If Oracle Workspaces operations are sluggish, you can increase the values for each of these properties and test the result:

- `oracle.workspaces.db.connPoolInitialLimit`
The default value is 5
- `oracle.workspaces.db.connPoolMinLimit`
The default value is 5
- `oracle.workspaces.db.connPoolMaxLimit`
The default value is -1, indicating unlimited size

LDAP Connection Pool Size The following properties determine the initial and maximum sizes of the pool of LDAP connections. These connections are used to retrieve user

information from Oracle Internet Directory. If user lookup operations are sluggish, you can increase the values for each of these properties and test the result:

- `oracle.ocs.ldappool.initialsize`

The default value is 5

- `oracle.ocs.ldappool.maxsize`

The default value is 25

Discussions Service Connection Pool Size The following property determines the size of the connection pool used to access the Discussions service with administrator privileges. If operations are sluggish, you can increase the value of this property and test the result:

- `oracle.workspaces.discussions.adminConnPoolSize`

The default value is 5

Discussions Service on Behalf of Inbox Connection Pool Size The following property determines the size of the connection pool used to access the Discussions service with administrator privileges on behalf of the Inbox service that is built on top of the Discussions service. If operations such as creating and deleting an Inbox service are sluggish, you can increase the value of this property and test the result:

- `oracle.workspaces.email.adminConnPoolSize`

The default value is 5

Adjusting Oracle Workspaces Performance

Oracle Workspaces provides the following system properties to control application performance.

Database Connection Pool Wait Timeout The following property determines the number of seconds to wait when all cached connections are in use before trying to obtain a connection again:

- `oracle.workspaces.db.connPoolWaitTimeout`

The default value is 3

Database Connection Pool Inactivity Timeout The following property determines the number of seconds of inactivity before a physical database connection will be closed:

- `oracle.workspaces.db.connPoolInactivityTimeout`

The default value is 120

Calendar User Connection Pool The following properties determine the minimum and maximum number of calendar connections to maintain in the connection pool. If calendar operations are sluggish, you can these values and test the result:

- `oracle.workspaces.calendar.connPoolMinUser`

The default value is 10

- `oracle.workspaces.calendar.connPoolMaxUser`

The default value is 100

Calendar Connection Pool Blocking The true/false value of the following property determines whether Oracle Workspaces should wait or fail when attempting to obtain a calendar connection from a pool that is completely in use:

- `oracle.workspaces.calendar.connPoolBlocking`

The default value is true

Oracle Calendar Master Node Connection The following properties determine the minimum and maximum number of connections that the native Calendar service maintains to the calendar master node. If calendar operations are sluggish and you have already tried increasing the `connPoolMinUser` and `connPoolMaxUser` parameters, you can increase these values and test the result:

- `oracle.workspaces.calendar.connPoolMinMasternode`

The default value is 0

- `oracle.workspaces.calendar.connPoolMaxMasternode`

The default value is 15

JDBC Statement Caching The following property specifies whether JDBC statement caching is turned on or not. By default it is true. Statement caching consumes memory, but improves performance.

- `oracle.workspaces.db.statementCachingEnabled`

The default value is true

Workspaces Log Level The following property specifies the amount of detail written out to the logfile:

- `oracle.workspaces.log.level`

The default value is warn

The following log levels are available:

- **fatal:** Only serious errors are written to the log.
- **error:** All errors detected are written to the log.
- **assert:** All errors and any assertion conditions which fail are written to the log.
- **warn:** All errors, assertion failures, and warnings are written to the log.
- **info:** All errors, assertion failures, and warnings as well as informational messages are written to the log.
- **debug:** A lot of tracing information is written to the log to help debug the application. This setting can be very verbose.

Investigating Oracle Workspaces Performance

You can gather statistical metrics for Oracle Workspaces and use it to tune performance.

To gather metrics and statistics:

1. Run the following scripts to collect performance information into two files:

```
ORACLE_HOME/bin/dmstool -table ocw_webui_request | egrep
"Name:|processRequest.avg|maxActive|completed" > /tmp/<filename>
```

```
ORACLE_HOME/bin/dmstool -table -count 1 ocw_operation | egrep
```

```
"Name: |processRequest.avg|maxActive|completed" > /tmp/<file2name>
```

```
ORACLE_HOME/bin/dmstool -table -count 1 JVM
```

2. View the output from the scripts in file1name and file2name by opening them with a text editor. Samples of the output appear as follows:

From <file1name>:

```
numObjects.completed: 0 ops
processRequest.avg: 1439.0 msecs
processRequest.completed: 1 ops
processRequest.maxActive: 1 threads
Name: library.filesFolderList
```

From <file2name>:

```
numObjects.completed: 1 ops
processRequest.avg: 295.0 msecs
processRequest.completed: 1 ops
processRequest.maxActive: 1 threads
Name: files.listContents
```

The first place to look is in the file1name for the ocw_webui_request metrics. These are the responses from Web operations within the OC4J. Users will generally accept responses in the three to five second range. If the response takes longer than this, users will typically perceive that the response is slow. Get an overall average of the individual operations averages to get a feel for the full system. You can do this by using the following command:

```
cat <filename> | grep processRequest.avg | grep -v 0.0 | awk '{count+=1;sum+=$2;
print sum/count}'
```

If the average performance is poor, there are two possibilities; it could be that the whole system is slow, or it could be an individual component causing delays. Oracle Workspaces is integrated with other Oracle Collaboration Suite components; using the information in these files, it should be possible to isolate the problem component. Once this is done use the second file to see if which operations against the backend are slow (server side responses should take 0.5 seconds or less). Then attempt to improve these areas specifically.

The output from the dmstool -table -count JVM command should appear similar to the following example:

```
activeThreadGroups.maxValue: 3.0 groups
activeThreadGroups.minValue: 1.0 groups
activeThreadGroups.value: 3 groups
activeThreads.maxValue: 49.0 threads
activeThreads.minValue: 7.0 threads
activeThreads.value: 49 threads
cpuTime.value: not implemented msecs
freeMemory.maxValue: 17502.0 kbytes
freeMemory.minValue: 1314.0 kbytes
freeMemory.value: 17502 kbytes
startTime.value: 1117111720253 msecs
timeStamp.ts: 1117116037938 milliseconds
totalMemory.maxValue: 45380.0 kbytes
totalMemory.minValue: 1984.0 kbytes
totalMemory.value: 45380 kbytes
upTime.value: 4317683 msecs
Host: etclbs09.uk.oracle.com
```

```
Name: JVM
Parent: /
Process: OC4J_OCSCClient:OC4J:12504:6004
iasInstance: ocsapps.etclbs09.uk.oracle.com
uid: 1153237058
```

The main item of interest here is the JVM `totalmemory.maxvalue` coupled with the `freeMemory.value`. If the `totalmemory.maxvalue` is equal to the max value defined in `opmn.xml` then at some point during operation this maximum has been reached. If, during peak periods, `totalmemory.value` is close to the maximum and the `freeMemory.value` is very low, this indicates that the JVM heap memory may need to be increased, dependent on the physical memory available on the host.

Monitoring and Tuning the Oracle Collaboration Suite Database

Monitoring the health of a database and ensuring that it performs optimally is an important task for a database administrator. This section discusses the features and functionality included in Oracle Database that make it easy to proactively monitor database health, identify performance problems, and implement any corrective actions.

The following topics are covered:

- [Proactive Database Monitoring](#)
- [Diagnosing Performance Problems](#)
- [Using Advisors to Optimize Database Performance](#)

Proactive Database Monitoring

The Oracle Database makes it easy to proactively monitor the health and performance of your database. It monitors the vital signs (or metrics) related to database health, analyzes the workload running against the database, and automatically identifies any issues that need your attention as an administrator. The identified issues are either presented as alerts in Enterprise Manager or, if you prefer, can be sent to you through e-mail.

This section discusses the following topics:

- [Alerts](#)
- [Performance Self-Diagnostics: Automatic Database Diagnostics Monitor](#)
- [Monitoring General Database State and Workload](#)
- [Managing Alerts](#)

Alerts

Alerts help you monitor your database proactively. Most alerts are notifications when particular metrics thresholds are crossed. For each alert, you can set critical and warning threshold values. These threshold values are meant to be boundary values that when crossed indicate that the system is in an undesirable state. For example, when a tablespace becomes 97 percent full this can be considered undesirable and have Oracle generate a critical alert.

Other alerts correspond to database events such as Snapshot Too Old or Resumable Session suspended. These types of alerts indicate that the event has occurred.

In addition to notification, you can set alerts to perform some action such as running a script. For instance, scripts that shrink tablespace objects can be useful for a Tablespace Usage warning alert.

By default, Oracle enables the following alerts: Table Space Usage (warning at 85 percent full, critical at 97 percent full), Snapshot Too Old, Recovery Area Low on Free Space, and Resumable Session Suspended. You can modify these alerts or enable others by setting their metrics.

For more information, see ["Managing Alerts"](#) on page 10-21.

Performance Self-Diagnostics: Automatic Database Diagnostics Monitor

Oracle Database includes a self-diagnostic engine called the Automatic Database Diagnostic Monitor (ADDM). ADDM makes it possible for the Oracle Database to diagnose its own performance and determine how any identified problems can be resolved.

To facilitate automatic performance diagnosis using ADDM, Oracle Database periodically (once an hour by default) collects information about the database state and workload it is running. This information is gathered in the form of snapshots, which provide a statistical summary of the state of the system at any given point in time. These snapshots are stored in the Automatic Workload Repository, residing in the `SYSAUX` tablespace. The snapshots are stored in this repository for a set time (a week by default) before they are purged in order to make room for new snapshots.

ADDM examines data captured in AWR and performs analysis to determine the major problems on the system on a proactive basis and in many cases recommends solutions and quantifies expected benefits.

Generally, the performance problems ADDM can flag include the following:

- Resource bottlenecks, such as when your database is using large amounts of CPU time or memory, for example as a result of high load SQL statements
- Poor connection management, such as when your application is making too many log on attempts to the database
- Lock contention in a multiuser environment, when a lock to update data causes other sessions to wait, slowing down the database

For more information about using ADDM, see ["Diagnosing Performance Problems"](#) on page 10-26.

Monitoring General Database State and Workload

The Enterprise Manager home page enables you to monitor the health of your database. It provides a central place for general database state information and is updated periodically. This page reports information that is helpful for monitoring database state and workload.

The **General** section provides a quick view of the database, such as whether the database is Up or Down, the time the database was last started, instance name, host name, and the time of the most recent entry in the alert log.

The **Host CPU** section shows the percentage of CPU time used in the overall system. This chart breaks down CPU percentage into time used by the database and time used by other processes. If your database is taking up most of the CPU time, you can explore the cause further by looking at the **Active Sessions** summary. This summary tells you what the database processes are doing, such as which ones are using CPU, or waiting on I/O. You can drill down for more information by clicking a link, such as **CPU**.

If other processes are taking up most of your CPU time, this indicates that some other application running on the database machine may be the cause of the performance problems. To investigate this further, click the **Host** link under the General section. This link takes you to machine overview page where you can see some general information about the machine such as what operating system it is running, how long the machine has been up, and any potential problems. Clicking the Performance property page takes you to the machine performance summary page.

If you view the Performance Summary, you can see CPU utilization, memory utilization, and disk utilization over time. Below these graphs, you can also view the top ten processes in the CPU. The type of actions you can take to relieve this kind of load depends on your system, but can include eliminating unnecessary processes, adding memory, or adding CPUs.

On the Home page, the **Diagnostic Summary** summarizes the latest ADDM performance findings. This section also summarizes any critical or warning alerts listed in the Alerts section.

The **Alerts** table provides information about any alerts that have been issued along with the severity rating of each. An alert is a notification that a metric threshold has been crossed. For example, an alert can be triggered when a tablespace is running out of space.

When an alert is triggered, the name of the metric causing it is displayed in the Name column. The severity icon (Warning or Critical) is displayed, along with time of alert, alert value, and time the metric was last checked. You can click the message to learn more about the cause. For more information, see "[Alerts](#)" on page 10-19.

The **Performance Analysis** section provides a quick summary of the latest ADDM findings, highlighting the issues that are causing the most significant performance impact. This analysis can identify problems such as SQL statements that are consuming significant database time. For more information, see "[Performance Self-Diagnostics: Automatic Database Diagnostics Monitor](#)" on page 10-20.

Managing Alerts

The following sections describe how to manage alerts.

Viewing Metrics and Thresholds Metrics are a set of statistics for certain system attributes as defined by Oracle. They are computed and stored by the Automatic Workload Repository, and are displayed on the All Metrics page, which is viewable by clicking **All Metrics** under Related Links heading on the Database Home page (and some other pages). [Figure 10-2, "All Metrics Page"](#) shows a portion of the All Metrics page, displaying some of the metrics that AWR computes. When you click a specific metric link, a detail page appears, with more information about the metric. Online Help for this page gives you a description of the metric.

Figure 10-2 All Metrics Page


ORACLE Enterprise Manager 10g Database Control

Setup Preferences Help Logout Database

Database: OCSM14DB.us.oracle.com > All Metrics

All Metrics

Collected From Target Jun 25, 2005 3:47:29 PM

Expand All | Collapse All

Metrics	Thresholds	Collection Status
▼ OCSM14DB.us.oracle.com		
▶ Alert Log	Some	Last Collected Jun 25, 2005 12:57:24 PM
▶ Alert Log Content	None	Not Collected
▶ Alert Log Error Status	All	Last Collected Jun 25, 2005 3:42:24 PM
▶ Archive Area	Some	Last Collected Jun 25, 2005 3:04:35 PM
▶ Database Files	None	Last Collected Jun 25, 2005 3:41:17 PM
▶ Database Job Status	All	Last Collected Jun 24, 2005 12:58:31 PM
▶ Database Limits	Some	Last Collected Jun 25, 2005 3:43:17 PM
▶ Database Services	None	Last Collected Jun 25, 2005 3:42:17 PM
▶ Deferred Transactions	All	Last Collected Jun 9, 2005 1:59:26 PM
▶ Dump Area	Some	Last Collected Jun 25, 2005 3:04:35 PM
▶ Efficiency	None	Last Collected Jun 25, 2005 3:43:17 PM
▶ Invalid Objects	None	Last Collected Jun 9, 2005 1:05:35 PM
▶ Invalid Objects by Schema	All	Last Collected Jun 22, 2005 1:05:35 PM
▶ Recovery Area	None	Last Collected Jun 25, 2005 3:46:18 PM
▶ Response	All	Last Collected Jun 25, 2005 3:46:32 PM
▶ SGA Pool Wastage	None	Last Collected Jun 25, 2005 3:46:18 PM
▶ SQL Response Time	All	Last Collected Jun 25, 2005 3:44:15 PM
▶ Session Suspended	None	Not Collected
▶ Snapshot Too Old	None	Not Collected
▶ System Response Time Per Call	None	Last Collected Jun 25, 2005 3:42:17 PM
▶ Tablespaces Full	All	Last Collected Jun 25, 2005 3:19:24 PM
▶ Tablespaces Full (dictionary managed)	All	Last Collected Jun 13, 2005 8:19:24 AM

For each of these metrics, you are able to define warning and critical threshold values, and whenever the threshold is crossed, Oracle issues an alert.

Alerts are displayed on the Database Home page under the Alerts heading (or Related Alerts for non-database alerts such as a component of Oracle Net) as shown in [Figure 10-3, "Alerts Section of Database Home Page"](#).

Setting thresholds is discussed in ["Setting Metric Thresholds"](#) on page 10-23. Actions you might take to respond to alerts are discussed in ["Responding to Alerts"](#) on page 10-25.

Figure 10–3 Alerts Section of Database Home Page

Alerts							
Category		All		Go			
Severity	Category	Name	Message	Alert Triggered	Last Value	Last Value Collected	
	Database Limits	Current Open Cursors Count	Metrics "Current Open Cursors Count" is at 2688	Jun 13, 2005 12:47:49 PM	4,689,775	Jun 25, 2005 3:43:17 PM	
	Alert Log	Generic Alert Log Error	ORA-error stack (07445[kqdrds()+168], 01017) logged in /private/qatest/OCS_M14/OCS_Infra/admin/OCSM14DB/bdump/alert_QCSM14DB.log.	Jun 14, 2005 9:12:24 AM			
	User Audit	Audited User	User SYS logged on from dsunrdd16.	Jun 13, 2005 12:46:21 PM			
	User Audit	Audited User	User SYS logged on from dsunrdd16.us.oracle.com.	Jun 25, 2005 2:16:19 PM			
	Invalid Objects by Schema	Owner's Invalid Object Count	4 object(s) are invalid in the RTC_APP schema.	Jun 10, 2005 1:05:35 PM	8	Jun 22, 2005 1:05:35 PM	
	Invalid Objects by Schema	Owner's Invalid Object Count	4 object(s) are invalid in the RTC_REP schema.	Jun 22, 2005 1:05:35 PM	4	Jun 22, 2005 1:05:35 PM	

Related Alerts							
Severity	Target Name	Target Type	Category	Name	Message	Alert Triggered	Last Value
	dsunrdd16.us.oracle.com	Host	Filesystems	Filesystem Space Available (%)	Filesystem / has only 17.15% available space	Jun 9, 2005 1:05:15 PM	17.14
							Jun 25, 2005 1:20:15 PM

When the condition that triggered the alert is resolved and the metric's value is no longer outside the boundary, Oracle clears the alert. Metrics are important for measuring the health of the database and serve as input for self-tuning and recommendations made by Oracle advisors.

Setting Metric Thresholds Oracle provides a set of predefined metrics, some of which initially have thresholds defined for them. There may be times when you want to set thresholds for other metrics, or you want to alter existing threshold settings.

One means of setting a threshold was introduced in "Modifying a Tablespace" on page 6-30, where you could set warning and critical thresholds on the amount of space consumed in a tablespace.

A more general means of setting thresholds is available using the Edit Thresholds page.

The following steps describe how to set metric thresholds:

1. From the Database Home page, click **Manage Metrics** under the Related Links heading.

The Manage Metrics page is displayed. It displays the existing thresholds for metrics and any response actions that have been specified. You cannot edit any thresholds on this page.

2. Click **Edit Thresholds**.

The Edit Thresholds page, shown in Figure 10–4, "Edit Thresholds Page", is displayed. On this page you can enter new **Warning Threshold** and **Critical Threshold** values, or you can modify existing values. In the **Response Actions** field, you can enter an operating system command or a script that you want executed when an alert is issued because a threshold has been crossed.

For example, to modify the warning threshold for **Tablespace Space Used (%)** metric, you can enter 87 as the percentage. Under **Response Actions**, you can optionally specify a fully qualified path to an operating system script that will clean up or increase the size of the tablespace.

Oracle provides a number of alerts that are not enabled by default. You can enable them by specifying threshold values. For example, to enable the alert for **Cumulative Logons (for each second)**, enter 10 for warning and 25 for critical. This will cause the system to warn you when the number of logons per second exceeds 10.

You must click **OK** to save your changes.

Figure 10–4 Edit Thresholds Page

ORACLE Enterprise Manager 10g Database Control

Setup Preferences Help Logout Database

Database: OCSM14DB.us.oracle.com > Manage Metrics > Edit Thresholds

Edit Thresholds

You can set a warning and critical threshold for each of the metrics below. When a threshold is reached, an alert will be generated and the response action, if specified, executed. The response action can be any command or script, with a fully qualified path, that is accessible to the Management Agent. Cancel OK

TIP Some metrics do not allow a default set of thresholds for all their monitored objects. Click "Specify Multiple Thresholds" to set thresholds for specific objects.

Related Link [Response to Target Down](#) Copy Thresholds From Metric Snapshot Specify Multiple Thresholds

Select	Metric	Comparison Operator	Warning Threshold	Critical Threshold	Response Action
☒	Archive Area Used (%)	>	80		
☐	Archiver Hung Alert Log Error	Contains		ORA-	
☐	Archiver Hung Alert Log Error Status	>	0		
☐	Audited User	=	SYS		
☐	Average File Read Time (centi-seconds)	>			
☐	Average File Write Time (centi-seconds)	>			
☐	Average Users Waiting Count				
☐	Administrative	>	10		
☐	Application	>	10		
☐	Cluster	>	30		
☐	Commit	>	30		
☐	Concurrency	>	10		
☐	Configuration	>	10		
☐	Network	>	10		

- For more comprehensive management of threshold settings for the different alerts, click the radio button in the **Select** column for that metric, then click **Specify Multiple Thresholds**.

The Specify Multiple Thresholds: *metric_name* page is displayed that enables you to add or delete specific metric threshold and response action settings.

For example, to set the **Tablespace Space Used (%)** metric thresholds for individual tablespaces, select this metric then click **Specify Multiple Thresholds**. Enter the tablespace name and its warning and critical values. Click **Add Another Row** to specify additional thresholds. Click **OK** to save your changes.

Setting up Notification You can optionally direct Enterprise Manager to provide notification when events that require your intervention arise. For example, if you specify that you want e-mail notification for critical alerts, and you have a critical threshold set for the **system response time for each call** metric, then you could be sent an e-mail containing a message similar to the following:

```
Host Name=mydb.us.mycompany.com
Metric=Response Time per Call
Timestamp=08-NOV-2003 10:10:01 (GMT -7:00)
Severity=Critical
Message=Response time per call has exceeded the threshold. See the
latest ADDM analysis.
Rule Name=
Rule Owner=SYSMAN
```

The host name is a link to the Database Home page and in the message there is a link to the latest ADDM analysis.

By default, alerts in critical state such as DB Down, Generic Alert Log Error Status, and Tablespace Used are set up for notification. However, to receive these notifications, you must set up your e-mail information. You can do so as follows:

1. From any Database Control page, click the **Setup** link, which is visible in the header and footer area.
2. On the Setup page, select **Notification Methods**.
3. Enter the required information into the Mail Server portion of the Notifications Methods page. See the online help for assistance.

There are other methods of notification, including scripts and SNMP (Simplified Network Management Protocol) traps. The latter can be used to communicate with third-party applications.

Note: So far, you have set up a method of notification, but you have not set up an e-mail address to receive the notification. To do so, complete the following steps.

4. From any Database Control page, click the **Preferences** link, which is visible in the header and footer area.
5. On the Preferences page, select **General**. Enter your e-mail address in the **E-mail Addresses** section.
6. You can optionally edit notification rules, such as to change the severity state for receiving notification. To do so, select **Notification Rules**. The Notification Rules page appears. For more information about configuring notification rules, see *Oracle Enterprise Manager Advanced Configuration*.

Responding to Alerts When you receive an alert, follow any recommendations it provides, or consider running ADDM or another advisor, as appropriate to get more detailed diagnostics of system or object behavior.

For example, if you receive a Tablespace Space Usage alert, you might take a corrective measure by running the Segment Advisor on the tablespace to identify possible objects for shrinking. You can then shrink the objects to free space. See "[Reclaiming Wasted Space](#)" on page 6-31.

Additionally, as a response, you can set a corrective script to run as described in "[Setting Metric Thresholds](#)" on page 10-23.

Clearing Alerts Most alerts, such as the Out of Space alert, are cleared automatically when the cause of the problem disappears. However, other alerts such as Generic Alert Log Error are sent to you for notification and need to be acknowledged by you, the system administrator.

After taking the necessary corrective measures, you can acknowledge an alert by clearing or purging it. Clearing an alert sends the alert to the Alert History, which is viewable from the home page under Related Links. Purging an alert removes it from the Alert History.

To clear an alert such as Generic Alert Log Error, from the Home page under Alerts, click the Alert link. The Alert Log Errors page appears. Select the alert to clear and click **Clear**. To purge an alert, select it and click **Purge**. You can also **Clear Every Open Alert** or **Purge Every Alert** using these buttons.

Diagnosing Performance Problems

At times database performance problems arise that require your diagnosis and correction. Sometimes problems are brought to your attention by users who complain about slow performance. Other times you might notice performance spikes in the Host CPU chart on the home page.

In all cases, these problems are flagged by the Automatic Database Diagnostics Monitor (ADDM), which does a top-down system analysis every hour by default and reports its findings on the Database Home page.

Viewing Performance Analysis

ADDM runs automatically every hour to coincide with the snapshots taken by AWR. Its output consists of a description of each problem it has identified, and a recommended action.

Findings are displayed in two places on the home page:

- Under the **Performance Analysis** section on the Database Home page, as shown in Figure 10–5, "Performance Analysis".

You can drill down by clicking the finding. The Findings Details page appears describing the findings and recommended actions.

- Below the **Diagnostic Summary** heading next to Performance Findings shows the number of findings if any. Clicking this link takes you to the ADDM page.

Figure 10–5 Performance Analysis

Performance Analysis

Period Start Time **Jun 25, 2005 3:00:37 PM** Period Duration (minutes) **60.28**

⊙ Previous 1-5 of 7 Next 2 ⊙

Impact (%)	Finding	Recommendations
39.53	Time spent on the CPU by the instance was responsible for a substantial part of database time.	5 SQL Tuning
23.54	PL/SQL execution consumed significant database time.	3 SQL Tuning
22.85	SQL statements consuming significant database time were found.	5 SQL Tuning
14.35	Wait class "Application" was consuming significant database time.	
14.35	Wait event "SQL*Net break/reset to client" in wait class "Application" was consuming significant database time.	3 Application Analysis

Responding to Performance Findings

To respond to a performance finding, click the finding and follow the recommended actions, if any. A recommendation can include running an advisor.

For example, [Figure 10-5, "Performance Analysis"](#) shows a performance finding of SQL statements consuming significant database time were found, with an impact of 22.85 percent and recommended summary of SQL Tuning.

Clicking the finding link takes you to the Performance Finding Details page. Here the recommended action is to run the SQL Advisor, which you can do by clicking **Run Advisor Now**. The advisor runs and gives a recommendation in the form of precise actions for tuning the SQL statements for better performance.

Modifying Default ADDM Behavior

ADDM behavior and analysis is based on the Automatic Workload Repository (AWR), which collects system performance statistics and stores the data in the database. After default installation, the AWR captures data every hour and purges data over seven days old. You can modify both the snapshot frequency and the data retention period as desired.

You can view and alter these settings on the Workload Repository page:

- The retention period for snapshots. This is initially set to 7 days.
- The interval for snapshots. The default and recommended value is one hour.

To navigate to this page, from the Database Administration page, under Workload, select **Automatic Workload Repository**.

To change either of these settings, click **Edit** on the Workload Repository page. The Edit Settings page appears. Enter a new Snapshot retention period or new System Snapshot Interval. Click **OK**.

Running ADDM Manually

By default Oracle runs ADDM every hour. Performance findings from the last snapshot are listed on the Oracle Enterprise Manager Home page. This is described in ["Performance Self-Diagnostics: Automatic Database Diagnostics Monitor"](#) on page 10-20.

You can also invoke ADDM manually. Reasons for doing so include running it as a recommended action associated with an alert, running it in the middle of a snapshot period, or running it across multiple snapshots.

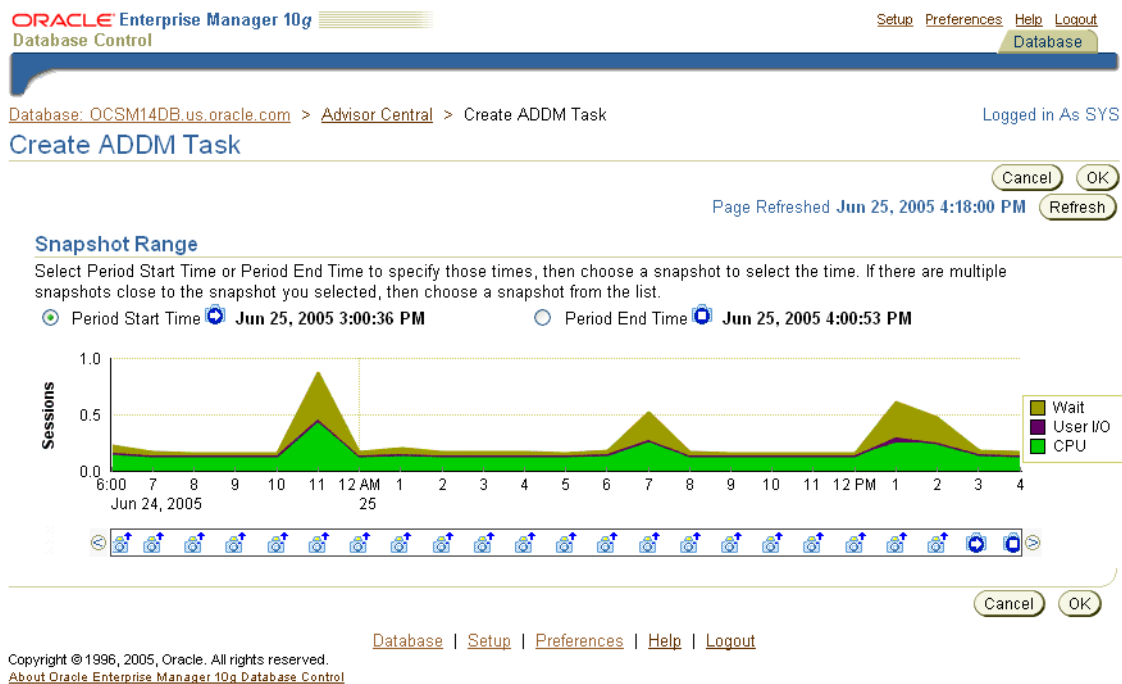
Note: If you need more frequent ADDM reporting, you can also modify the default snapshot interval. To do so, see ["Modifying Default ADDM Behavior"](#) on page 10-27.

From the Home page, under Related links you can navigate to the ADDM page by clicking **Advisor Central**, then **ADDM**. The Create ADDM Task page appears.

[Figure 10-6, "Create ADDM Task"](#) is a screen shot of Create ADDM Task page.

Increased session activity shows up as peaks in the graph. To analyze a period across multiple snapshots, select a start time and click **OK**, then choose an end time and click **OK**. The ADDM Task page appears detailing any findings.

Figure 10–6 Create ADDM Task



Using Advisors to Optimize Database Performance

Advisors are powerful tools for database management. They provide specific advice on how to address key database management challenges, covering a wide range of areas including space, performance, and undo management. In general, advisors produce more comprehensive recommendations than alerts. This is because alert generation is intended to be low cost and have minimal impact on performance, whereas advisors are user-invoked, consume more resources, and perform more detailed analysis. This, along with the what-if capability of some advisors, provides vital information for tuning that cannot be procured from any other source.

About Performance Advisors

This chapter deals primarily with the advisors that can improve performance. These advisors include the SQL Tuning, SQL Access, and Memory Advisors. [Table 10–5, "Performance Advisors"](#) describes these advisors.

Caution: You should not use the SQL Tuning Advisor or the SQL Access Advisor on the Oracle Collaboration Suite Database. The SQL statements used for Oracle Collaboration Suite are already optimized, and the kinds of changes which the SQL Advisors might advise could cause Oracle Collaboration Suite components to stop functioning correctly.

Other advisors such as the Undo and Segment Advisors are listed in [Table 10–6, "Other Advisors"](#).

For example, the shared pool memory advisor graphically displays the impact on performance of changing the size of this component of the SGA.

[Table 10–5, "Performance Advisors"](#) describes the performance advisors that Oracle provides. These advisors are described in this chapter.

Table 10–5 Performance Advisors

Advisor	Description
Automatic Database Diagnostic Monitor (ADDM)	ADDM makes it possible for the Oracle Database to diagnose its own performance and determine how any identified problems can be resolved. See "Performance Self-Diagnostics: Automatic Database Diagnostics Monitor" on page 10-20 and "Diagnosing Performance Problems" on page 10-26.
SQL Tuning Advisor	This advisor analyzes SQL statements and makes recommendations for improving performance. You should not use the SQL Tuning Advisor on the Oracle Collaboration Suite Database.
SQL Access Advisor	This advisor is intended to help tune schema to a given SQL workload. You should not use the SQL Access Advisor on the Oracle Collaboration Suite Database.
Memory Advisor ■ Shared Pool Advisor (SGA) ■ Buffer Cache Advisor (SGA) ■ PGA Advisor	The Memory Advisor is the main advisor for system memory and is responsible for optimizing memory on the instance as a whole. You have the option of having Oracle auto-tune memory. If you choose not to have Oracle auto-tune memory, then you can invoke the SGA Advisors or the PGA Advisor to obtain optimal settings for the components and total size of the SGA or PGA. See "Using the Memory Advisor" on page 10-30.

[Table 10–6, "Other Advisors"](#) describes other advisors Oracle provides. These are described elsewhere in this book.

Table 10–6 Other Advisors

Advisor	Description
Segment Advisor	The Segment Advisor provides advice on whether an object is a good candidate for a shrink operation based on the level of space fragmentation within that object. The advisor also reports on the historical growth trend of segments. You can use this information for capacity planning and for arriving at an informed decision about which segments to shrink. See "Reclaiming Wasted Space" on page 6-31.
Undo Advisor	The Undo Advisor helps in identifying problems in the undo tablespace and assists in correctly sizing the undo tablespace. The Undo Advisor can also be used to set the low threshold value of the undo retention period for any flashback requirements. See "Using the Undo Advisor" on page 6-35.

You can invoke an advisor from the Advisor Central home page, accessible through a link on the Database Home page. You can invoke advisors in other ways, often through recommendations from ADDM or alerts.

About the SQL Tuning Advisor

You should not use the SQL Tuning Advisor on the Oracle Collaboration Suite Database. The SQL statements used for Oracle Collaboration Suite are already optimized, and the kinds of changes which the SQL Tuning Advisor might advise could cause Oracle Collaboration Suite components to stop functioning correctly.

About the SQL Access Advisor

You should not use the SQL Access Advisor on the Oracle Collaboration Suite Database. The SQL statements used for Oracle Collaboration Suite are already optimized, and the kinds of changes which the SQL Access Advisor might advise could cause Oracle Collaboration Suite components to stop functioning correctly.

Using the Memory Advisor

The Memory Advisor helps you tune the size of your memory structures. You can use this advisor only when automatic memory tuning is disabled.

The memory advisor comprises three advisors that give you recommendations on the following memory structures:

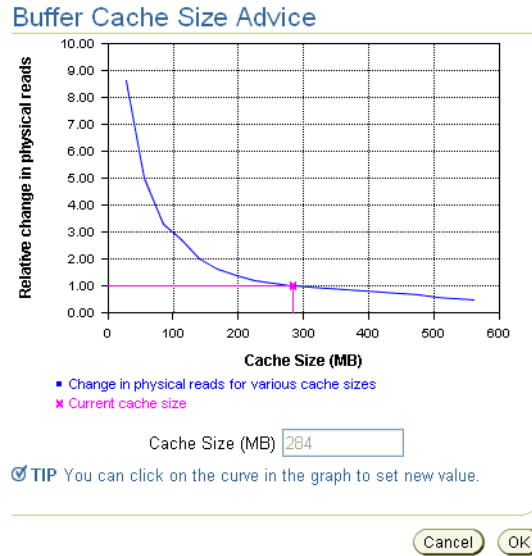
- Shared pool in SGA
- Buffer cache in SGA
- PGA

To invoke the Memory Advisors, click **Memory Advisor** on the Advisor Central page. The Memory Parameters: SGA page appears. This page gives breakdown of memory usage for the system global area (SGA). This memory area is a group of shared memory structures that contain data and control information for a single Oracle instance. The shared pool and buffer cache are part of this area. For more information on these structures, click **Help**.

The **Automatic Shared Memory Management** setting should be disabled in order to run the advisor. To run either the shared pool advisor or the buffer cache advisor, click **Advice** next to the field.

For example, to run the advisor on the buffer cache, click **Advice** next to the buffer cache field. The Buffer Cache Size Advice graph appears. Refer to [Figure 10–7, "Buffered Cache Size Advice"](#).

Relative change in physical reads is plotted against cache size. A lower number for physical reads is better for performance. In this example, the graph tells us that a cache size larger than 284M will not improve performance by much. Thus 284M is the recommended optimal buffered cache size.

Figure 10–7 Buffered Cache Size Advice

To run the PGA advisor, click the **PGA** property page. Running this advisor is similar to running the SGA advisors. Cache hit percentage is plotted against memory size. Higher hit ratios indicate better cache performance. The optimal zone for cache hit percentage is between 75 and 100 percent.

Backing Up and Recovering Oracle Collaboration Suite

This chapter contains the following sections:

- ["Oracle Collaboration Suite Backup and Recovery Strategy"](#)
- ["Understanding Database Backup and Recovery"](#)

Oracle Collaboration Suite Backup and Recovery Strategy

This section provides an introduction to backup and recovery concepts, an overview of Oracle's backup and recovery strategy in an enterprise environment, and assumptions and restrictions necessary to implementing this strategy. It contains the following topics:

- [Basics of Backup and Recovery](#)
- [Oracle Collaboration Suite Backup and Recovery Roadmap](#)
- [Oracle Collaboration Suite Backup and Recovery Using Recovery Manager \(RMAN\) and Other Customized Scripts](#)
- [Assumptions and Restrictions for all Oracle Collaboration Suite Backup and Recovery Operations](#)

Basics of Backup and Recovery

Because all organizations need to protect themselves from potential disaster resulting from data loss, backup and recovery is one of the most important aspects of administration.

Your Oracle Collaboration Suite environment is the framework within which you perform backup and recovery, and contains two tiers: the Infrastructure tier and the Applications tier.

These installations contain interdependent configuration information, applications, and data. During normal operation, the application server automatically synchronizes this information. However, in the event of system failure or data loss, the administrator has to restore the application server to a consistent state.

For this reason, it is important to visualize the Oracle Collaboration Suite environment as a single entity when performing backup and recovery, instead of approaching it as a set of independent installations. As a result, you must back up data across all installations at the same point in time. If you were backing up the Infrastructure on Mondays and the Applications tier installation on Tuesdays, in the event of data loss you would only be able to restore your separate tiers of the Oracle Collaboration Suite

to the state they had on the days when they were last saved. This would create consistency issues between the different components in the Oracle Collaboration Suite. If you backup critical data from all tiers at the same time, you can restore and recover all tiers to a consistent state.

The backup and recovery strategies and procedures in this document involve backing up the entire Oracle Collaboration Suite environment as a whole, and restoring it so that its state remains consistent.

Oracle Collaboration Suite Backup and Recovery Roadmap

The overall backup strategy should be comprised of a cold backup and partial online backups.

You should perform an initial complete **cold backup**, which includes everything necessary to restore your initial installation of your Oracle Collaboration Suite environment:

- Back up the Applications tier Oracle home
- Back up the Infrastructure Oracle home
- Back up Oracle Calendar and its associated files

Note: The Oracle Calendar server database is not stored on the Infrastructure tier of your Oracle Collaboration Suite deployment. The Applications tier houses the Oracle Calendar server database, and must be backed up separately when backing up Oracle Collaboration Suite.

Use the `unbdbbackup` utility to back up the Oracle Calendar server database, and configuration files; and the `unbdbrestore` utility to restore the entire Oracle Calendar server database or the `unirestore` utility to restore individual users.

For more information about `unbdbbackup`, `unbdbrestore` and `unirestore`, see “Calendar Server Utilities” in Chapter 6 of *Oracle Calendar Reference Manual*.

You should also perform regular **partial online backups** of your Oracle Collaboration Suite environment, which involves saving the configuration information across your entire Oracle Collaboration Suite environment at the same point in time:

- Back up the configuration files in the Applications tier Oracle home
- Back up the configuration files in the Infrastructure Oracle home
- Perform an online backup of the Infrastructure

Restore and recovery procedures for **data loss**, **host failure**, or **media failure** enable you to recover from failures that involve actual data loss. Depending on the type of loss, they can involve a variety of steps. In all cases, care must be taken to ensure that state is consistent across all installations:

- Restore Oracle static binaries or libraries from a complete cold backup
- Restore configuration files from the most recent partial online backup
- Restore and recover the Infrastructure to its latest state

Recovery strategies for **process or system outages** and **crashes** involve restarting processes that have stopped or failed. They do not involve data recovery.

More specifically, Oracle recommends that you use one of the following general strategies to implement backup and recovery within your organization. Both strategies have the following common characteristics:

- These strategies use complete recovery for the Infrastructure. Specifically, they restore the backup and then apply all online and archived redo logs generated after the restored backup. This recovers the database to the state it had at the time of the loss.
- These strategies use same-point-in-time recovery of the Applications tier and the Infrastructure tier. Regardless of where the loss occurred, the tiers are always restored together so they are synchronized as they were at the time of the most recent backup.

Oracle Collaboration Suite Backup and Recovery Using Recovery Manager (RMAN) and Other Customized Scripts

If your organization is using customized backup and recovery scripts, use them in conjunction with RMAN and Oracle Collaboration Suite Calendar utilities to back up Oracle Collaboration Suite. The general steps would then be as follows:

1. Use RMAN and/or customized scripts to back up and restore the Infrastructure databases.
2. Use customized scripts to backup and restore the Applications tier and its components.
3. Use Oracle Calendar backup and recovery utilities.

Assumptions and Restrictions for all Oracle Collaboration Suite Backup and Recovery Operations

Prerequisites to suite-level backup and recovery include:

- When restoring the Oracle Collaboration Suite, you should restore to the same host. When this is not possible, you can restore to a new host provided you first initialize it with the same system configuration as the original host, such as hostname, IP address, user names, directory paths, and operating system levels.
- You should turn on database archive logging since point-in-time recovery is a requirement.
- To perform backup or recovery, ensure that the following conditions are met for each tier:
 - Log in as the user that installed Oracle Collaboration Suite
 - Set the ORACLE_HOME environment variables.
 - Set the ORACLE_SID environment variable if you are performing a database backup.

Understanding Database Backup and Recovery

The Oracle Collaboration Suite Infrastructure tier includes an Oracle Database 10g Release 1 (10.1.0.5) Enterprise Edition instance. Performing backup and recovery on Oracle Collaboration Suite includes performing backup and recovery of that database.

It is therefore important to understand database backup and recovery. In particular, the following topics apply to Oracle Collaboration Suite backup and recovery:

- Using ARCHIVELOG mode, as discussed in "[Enabling ARCHIVELOG Mode](#)"
- Performing cold database backups, as discussed in "[Performing Cold Database Backups](#)"
- Performing online database backups, as discussed in "[Performing Online Database Backups](#)"
- Using the RMAN backup and recovery utility

See Also: The following books in the Oracle Database 10g Release 1 (10.1.0.5) documentation set if you are not experienced with database backup and recovery.

- *Recovery Manager Quick Start Guide*, Part Number B10769-01
- *Backup and Recovery Basics*, Part Number B10735-01
- *Recovery Manager Reference*, Part Number B10770-02
- *Backup and Recovery Advanced User's Guide*, Part Number B10734-01

You can find these volumes in the database document library, at:

<http://www.oracle.com/technology/documentation/>

Types of Database Backup

Since a database contains a wide variety of data, database administrators must decide what information they should copy when developing a backup and recovery strategy. The basic principle is to prioritize data depending on its importance and the degree to which it changes. For example, archive logs are crucial for recovering the database, so multiple copies should be maintained whenever possible.

Backups can be combined in a variety of ways, such as combining weekly whole database backups (to ensure a relatively current copy of original database information) with daily backups of the most accessed tablespaces. Another approach is to multiplex control file and archived redo logs as an additional safeguard. The following list describes the basic backup types:

- **Online Database Backup** An online backup or also known as an open backup, is a backup in which all read-write datafiles and control files have not been checkpointed with respect to the same log sequence number (SCN). For example, one read-write datafile header may contain an SCN of 100 while other read-write datafile headers contain an SCN of 95 or 90. Oracle cannot open the database until all of these header SCNs are consistent, or until all changes recorded in the online redo logs have been saved to the datafiles on disk. For databases that must be running non-stop, you have no choice but to perform online backups of a the entire database in ARCHIVELOG mode.
- **Offline Database Backup** In this backup, all datafiles and control files are consistent to the same point in time (or the same SCN). The only tablespaces in a consistent backup that are allowed to have older SCNs are read-only and offline-normal tablespaces, which are consistent with the other datafiles in the backup. This type of backup allows you to open the set of files created by the backup without applying redo logs because the data is already consistent. The only way to perform this type of backup is to shut down the database cleanly and make the backup while the database is closed. A consistent whole database

backup is the only valid backup option for databases running in NOARCHIVELOG mode.

- **Whole Database Backup** The most common type of backup, the whole database backup contains the control file along with all database files that belong to that database. If the database is operating in ARCHIVELOG mode, you also have the option of backing up different parts of the database over a period of time.
- **Tablespace Backups** A tablespace backup is a subset of the database. Tablespace backups are only valid if the database is operating in ARCHIVELOG mode. The only time a tablespace backup is valid for a database running in NOARCHIVELOG mode is when that tablespace is read-only or offline-normal.
- **Datafile Backups** A datafile backup contains a single datafile. This approach is not as common as tablespace backups, and is only valid for databases that are in ARCHIVELOG mode. The only time a datafile backup is valid for a database running in NOARCHIVELOG mode is if that datafile is the only file in a tablespace.
- **Control File Backups** A control file backup saves the database's control file. If the database is open, you can create a valid backup through the Recovery Manager (RMAN) or by issuing the following SQL statement:


```
ALTER DATABASE BACKUP CONTROLFILE TO LOCATION
```
- **Archived Redo Log Backups** Archived redo logs are necessary for successful media recovery. Depending on the disk space available and the number of transactions executed on the database, you should keep the maximum number of days of archive logs on disk, and you should back them up regularly to ensure a more complete recovery.
- **Configuration Files Backup** Configuration files may be of `spfile` or `init.ora`, password file, `tnsnames.ora`, and `sqlnet.ora`. Since these files do not change often, they require a less frequent backup schedule.

Types of Database Recovery

There are three basic types of recovery: instance recovery, crash recovery, and media recovery. Oracle performs both instance and crash recovery automatically at instance startup, but media recovery requires additional steps.

- An **instance recovery** is only possible in an Oracle Real Applications Cluster configuration; it occurs in an open database when one instance discovers that another instance has crashed. A surviving instance automatically uses the redo log to recover the committed data in the database buffers that were lost when the instance failed. Oracle also undoes any in-progress transactions on the failed instance and clears any locks held by the crashed instance after recovery is complete.
- A **crash recovery** occurs when either a single-instance database or all instances of a multi-instance database crash. An instance must open the database and then execute recovery operations. In general, the first instance to open the database after a crash or `SHUTDOWN ABORT` automatically performs crash recovery.
- A **media recovery** is executed on the user's command, usually in response to media failure. Online or archived redo logs can be used to make a restored backup current, or to update it to a specific point in time. Media recovery can restore the whole database, a tablespace or a datafile, and recover them to a specified time.

A restored backup can always be used to perform the recovery. There are two principal types of media recovery: complete and incomplete recovery. **Complete recovery**

involves using redo log data along with a backup of a database, tablespace, or datafile, to apply every change that took place after the most recent backup, and to ensure that the recovery is to the most current point in time. Typically, media recovery is performed after a media failure damages datafiles or the control file. If you do not recover the database to the most current time, you must specify how far to recover in one of the following ways:

- Tablespace point-in-time recovery (TSPITR) recovers one or more tablespaces to a point-in-time that is different from the rest of the database.
- Time-based recovery, also called point-in-time recovery (PITR), recovers the data up to a specified point in time.
- Cancel-based recovery which recovers data until the CANCEL command.
- Change-based recovery, or log sequence recovery, recovers data up to a specified SCN in the redo record if using O/S commands.

If using RMAN, log sequence recovery recovers up to a specified log sequence number. When performing an **incomplete recovery**, the user must reset the online redo logs when opening the database. The new version of the reset database is called a new incarnation. Opening the database with the RESETLOGS option is an instruction to discard some redo information.

Oracle Database Backup Methodology

While Oracle provides users with a choice of several basic methods for making backups, we recommend that you use the Recovery Manager (RMAN) for Oracle Collaboration Suite. RMAN is a tool specifically designed to establish a connection with a server process and automate the movement of data for backup and recovery operations. It is a powerful and versatile program that allows users to make either an RMAN backup or an image copy of the data. RMAN automatically establishes the names and locations of all the files that need to be backed up, and can also be used for incremental backups, saving only those blocks of data that have changed since a previous backup.

The basic RMAN commands are RESTORE and RECOVER. RMAN can be used to restore datafiles from backup sets or image copies, either to their current location or to a new location. If any archived redo logs are required to complete the recovery operation, RMAN automatically restores and applies them. In a recovery catalog, RMAN keeps a record containing all the essential information concerning every backup ever taken. If a recovery catalog is not used, RMAN uses the control file for necessary information.

The RMAN RECOVER command can be used to perform complete media recovery and apply incremental backups, and to perform incomplete media recovery. If you specify files or archived logs using the RMAN BACKUP command, RMAN creates an output that is a backup set, or file(s) in a proprietary-specific format. This format requires the use of the RMAN RESTORE command for recovery operations. In contrast, when the BACKUP AS COPY command is used to create an image copy of a file, the copy is in an instance-usable format; you do not need to invoke RMAN to restore or recover it.

Enabling ARCHIVELOG Mode

By default, the Infrastructure and database do not have ARCHIVELOG mode enabled. You should enable ARCHIVELOG mode before you perform your first complete cold backup. Otherwise, your backup control files will contain the NOARCHIVELOG mode setting. These steps should be used for both the Infrastructure and Applications tiers.

To enable ARCHIVELOG mode, follow these steps:

1. Set up archive logging parameters. On **Unix**, edit the file `INFRA_ORACLE_HOME/dbs/init.ora`:

- Uncomment the following line by removing the initial '#' character so it appears like this:

```
log_archive_start = true
```

- [Optional] The default destination directory for archive logs is `INFRA_ORACLE_HOME/rdbms`. If you would like to use a different directory, uncomment the following line and specify the directory:

```
log_archive_dest = '/disk1/archive'
```

- [Optional] The default filename format for archive logs is `threadsequence.ARC`. If you would like to use a different format, uncomment the following line and specify a format:

```
log_archive_format = arch%s.arc
```

On **Windows**, edit the file:

```
INFRA_ORACLE_HOME\..\admin\iasdb\pfile\init.ora
```

- Add the following line anywhere in the file:

```
log_archive_start = true
```

- [Optional] The default destination directory for archive logs is `INFRA_ORACLE_HOME\rdbms`. If you would like to use a different directory, add the following line and specify the directory:

```
log_archive_dest = ' C:\database_archives\'
```

- [Optional] The default filename format for archive logs is `threadsequence.ARC`. If you would like to use a different format, add the following line and specify a format:

```
log_archive_format = arch%s.arc
```

2. Set the `ORACLE_HOME` and `ORACLE_SID` variables. Make sure the `ORACLE_HOME` and `ORACLE_SID` environment variables are properly set.
3. Check for active users. Make sure nobody is using the database.
4. Shut down database. Perform a clean, normal shutdown of the database instance.

```
INFRA_ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> shutdown
```

5. Start up the database. Start up the instance and mount, but do not open, the database.

```
SQL> startup mount;
```

6. Enable database ARCHIVELOG mode.

```
SQL> alter database archivelog;
SQL> alter system set log_archive_start=true scope=spfile;
```

7. Shut down and restart the database instance.

```
SQL> shutdown
SQL> startup
```

8. Verify the database is now in ARCHIVELOG mode. Execute the following command and verify that the database log mode is 'Archive Mode' and automatic archival is enabled.

```
SQL> archive log list;
Database log mode Archive Mode
Automatic archival Enabled
Archive destination /private/oraocs/dbs/arch
Oldest on-line log sequence 19
Next log sequence to archive 21
Current log sequence 21
```

See Also: *Administrator's Guide* for Oracle Database 10g Release 1 (10.1.0.5), Part Number B10739-01, for more detailed information on the parameters in this section, and on setting up archive logging in general.

Performing Cold Database Backups

Take these steps to perform a cold database backup:

1. Leave the database open.
2. Set the ORACLE_HOME environment variable to the Infrastructure Oracle home.
3. Set the ORACLE_SID environment variable to the Infrastructure SID.
4. To backup the Infrastructure database, use RMAN or customized scripts.

Performing Online Database Backups

Take these steps to perform an online database backup:

1. Leave the database open.
2. Set the ORACLE_HOME environment variable to the Infrastructure Oracle home.
3. Set the ORACLE_SID environment variable to the Infrastructure SID.
4. To backup the Infrastructure database, use RMAN or customized scripts.

Part III

Reconfiguring Oracle Collaboration Suite

Depending on your deployment configuration, Oracle Collaboration Suite consists of one Infrastructure instance, one or more Oracle Collaboration Suite Databases, and one or more Applications tiers hosting your deployed Oracle Collaboration Suite applications.

Oracle Collaboration Suite is designed to be scalable. At any time, you can choose to expand your deployment in a number of flexible ways, to improve performance, expand capacity, improve availability, and configure and deploy Oracle Collaboration Suite applications that you did not deploy when you first installed Oracle Collaboration Suite.

Part III contains chapters that will guide you in your reconfiguration of Oracle Collaboration Suite.

Part III contains the following chapters:

- [Chapter 12, "Changing Infrastructure Services"](#)
- [Chapter 13, "Managing High-Availability Environments"](#)
- [Chapter 14, "Changing Oracle Collaboration Suite Network Configurations"](#)
- [Chapter 15, "Customizing Oracle Collaboration Suite"](#)

Changing Infrastructure Services

This chapter describes a number of procedures used for making various changes to your Oracle Collaboration Suite Infrastructure services. This chapter includes the following topics:

- [Overview of Procedures for Changing Infrastructure Services](#)
- [Changing the Oracle Internet Directory or HTTP \(SSO\) Ports on Identity Management](#)
- [Changing Oracle Internet Directory from Dual Mode to SSL Mode](#)
- [Moving Identity Management to a New Host](#)
- [Changing the OracleAS Metadata Repository Used by an Applications Tier](#)
- [Applications Tier Application Reconfiguration](#)

Overview of Procedures for Changing Infrastructure Services

All Oracle Collaboration Suite Applications tier instances use services that reside on the Infrastructure, such as Identity Management Services and the OracleAS Metadata Repository. If you have a single Infrastructure instance, all of your Oracle Collaboration Suite Applications tier instances will automatically be associated with that instance during installation. If you have multiple Infrastructure instances, or if you have upgraded from a previous version of Oracle Collaboration Suite, some Applications tier services may require manual association as part of the setup process. These procedures are described in detail in the *Oracle Collaboration Suite Installation Guide for Solaris Operating System* and *Oracle Collaboration Suite Installation Guide for Microsoft Windows*.

After installation, you may want to change the Infrastructure Services used by a Applications tier instance. For example, you may want to use an Identity Management Service on a different host. Or, you may want to use a different OracleAS Metadata Repository.

Changing the association between one or more Infrastructure Services and one or more Applications tier instances is called 're-association'.

You can perform Infrastructure re-association using the Infrastructure Page on the Oracle Collaboration Suite Control Console, shown in figure [Figure 12-1](#). Notice that the page allows you to change the Identity Management or the OracleAS Metadata Repository used by an Applications tier instance.

Figure 12–1 Oracle Collaboration Suite Control Console Infrastructure Page

You must perform re-association when you change any of the following:

- The HTTP Server (SSO) port number on an Identity Management installation
- The Oracle Internet Directory non-SSL or SSL port number
- The Oracle Internet Directory Mode (Dual-mode or SSL)
- The host that Identity Management or the OracleAS Metadata Repository resides on

If you are creating a new Infrastructure instance, you must first perform manual tasks in order to create and prepare the new Infrastructure service. This chapter provides the following supported procedures for changing Infrastructure services:

- [Changing the Oracle Internet Directory or HTTP \(SSO\) Ports on Identity Management](#)

Use this procedure if you need to change the Oracle Internet Directory or HTTP listener ports on an Identity Management installation. In addition to changing the port numbers, you must update Applications tier instances with the new port information, which requires changing Infrastructure services.

- [Changing Oracle Internet Directory from Dual Mode to SSL Mode](#)

Use this procedure if you would like to change the Oracle Internet Directory mode from non-SSL to SSL. In addition to changing the mode, you must update Applications tier instances with the new mode, which requires changing Infrastructure services.

- [Moving Identity Management to a New Host](#)

Use this procedure if you would like to move your Identity Management installation, and its associated OracleAS Metadata Repository, to a new host. After

you perform the move, you must update Applications tier instances with the new host information for Identity Management, which requires re-association.

- **Changing the OracleAS Metadata Repository Used by an Applications Tier**

Use this procedure if you would like to move the OracleAS Metadata Repository used for product metadata by Applications tier instances to a new host.

Changing the Oracle Internet Directory or HTTP (SSO) Ports on Identity Management

If you would like to change the Oracle Internet Directory non-SSL or SSL port on an Identity Management installation, refer to ["Changing Oracle Internet Directory Ports"](#) on page 14-27.

If you would like to change the Oracle HTTP Server non-SSL or SSL listen port on an Identity Management installation, which effectively changes the SSO port, refer to ["Changing the HTTP Server Port on Identity Management"](#) on page 14-30.

Changing Oracle Internet Directory from Dual Mode to SSL Mode

When you install Identity Management, you are asked to choose a mode for Oracle Internet Directory. The default mode is dual mode, which allows some components to access Oracle Internet Directory using non-SSL connections. During the installation, you can choose SSL mode, which specifies that all components must use SSL when connecting to the directory.

If you did not choose SSL mode during the installation, and would like to change to SSL mode after installation, you can follow the procedure in this section. It includes changing the mode of the Oracle Internet Directory, and updating Applications tier instances to use the new mode.

Before You Begin

Before beginning this procedure, you should shut down all Applications tiers using this instance of Oracle Internet Directory. Be sure to leave the Oracle Collaboration Suite Control (emctl) process running on all Applications tiers.

You can shut down the tiers using Oracle Collaboration Suite Control by navigating to each Applications tier home page and clicking **Stop All**.

Task 1: Change the Oracle Internet Directory Mode

Perform this task on the Infrastructure instance that hosts Oracle Internet Directory.

1. Create a file named `mod.ldif` that contains the following lines:

```
dn:cn=configset0,cn=osldlapd,cn=subconfigsubentry
changetype:modify
replace:orclsslenable
orclsslenable:1
```

2. Run the following command:

```
ldapmodify -D cn=orcladmin -w orcladmin_passwd -p oid_port -v -f mod.ldif
```

oid_port is the non-SSL Oracle Internet Directory port. This is listed as `OIDport` in `ORACLE_HOME/config/ias.properties`.

3. Stop the entire instance that hosts Oracle Internet Directory:

```
emctl stop iasconsole
opmnctl stopall
```

4. Edit the **ldap.ora** file:

```
(UNIX) ORACLE_HOME/ldap/admin/ldap.ora
(Windows) ORACLE_HOME\ldap\admin\ldap.ora
```

a. Modify the following line to remove the non-SSL port number:

```
DIRECTORY_SERVERS=(myhost.myco.com::sslport)
```

b. Save and close the file.

5. Edit the following file:

```
(UNIX) ORACLE_HOME/config/ias.properties
(Windows) ORACLE_HOME\config\ias.properties
```

a. Change the SSLOnly parameter as follows:

```
SSLOnly=true
```

b. Save and close the file.

6. Start the entire instance that hosts Oracle Internet Directory:

```
opmnctl startall
emctl start iasconsole
```

7. Reconfigure SSO to communicate to Oracle Internet Directory in SSL mode:

a. Obtain the ORASSO schema password:

```
ldapsearch -p oid_port -U 1 -h hostname -D "cn=orcladmin" -w orcladmin_  
password -b "orclresourcename=orasso, orclreferencename=global_db_name,  
cn=ias infrastructure databases, cn=ias, cn=products, cn=oraclecontext" -s  
base "objectclass=*" orclpasswordattribute
```

oid_port is the non-SSL Oracle Internet Directory port. This is listed as
OIDport in *ORACLE_HOME/config/ias.properties*.

global_db_name is the name of the entry for the OracleAS Metadata
Repository in the *tnsnames.ora* file: *ORACLE_*
HOME/network/admin/tnsnames.ora. For example: *asdb.myco.com*.

This command prints the ORASSO password in a line like the following:

```
orclpasswordattribute=LAetjdQ5
```

b. Change to the following directory:

```
(UNIX) cd ORACLE_HOME/sso/admin/plsql/sso
(Windows) cd ORACLE_HOME\sso\admin\plsql\sso
```

c. Run the following command:

```
sqlplus orasso/orasso_password @ssooconf.sql
```

Where **orasso_password** is the ORASSO schema password you obtained in
the previous step.

The following prompts appear. Press return for attributes you did not change,
and enter a new value for attributes that you changed.

```
* Enter value for new_oid_host:
```

Press return.

- * Enter value for new_oid_port:

Enter the Oracle Internet Directory SSL port number and press return.

- * Enter value for new_sso_server_password:

Press Return.

- * Enter value for new_ldapusessl:

Enter Y in this field, then press return. A message appears indicating that the value new_ldapusessl has been updated.

8. Restart the instance that hosts Oracle Internet Directory.

```
opmnctl stopall
opmnctl startall
```

Task 2: Change Applications Tier Instances to Use SSL Mode

In each Applications tier instance, run the Change Identity Management wizard and restart the instance:

1. Using the Application Server Control Console, navigate to the Instance Home Page for the Applications tier instance.
2. Click **Infrastructure**.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. On the Internet Directory page:
 - Host: Enter the fully-qualified name of the Oracle Internet Directory host.
 - Port: Enter the SSL Oracle Internet Directory port number.
 - Use only SSL connections with Internet Directory: Check this box.

Click **Next**.
5. On the Login page:
 - User Name: Enter cn=orcladmin, or the distinguished name of a user in the iASAdmins group.
 - Password: Enter the password for the user.

Click **Next**.
6. On the Validation page, you will receive informational messages regarding the validation of this operation. If you receive any error message, follow the instructions for investigating them. Otherwise, if the operation is valid, click **Finish**.
7. Edit ORACLE_HOME/ldap/admin/ldap.ora in the Applications tier Oracle home to remove the non-SSL port number. Change the following line from:


```
DIRECTORY_SERVERS = (replica_host:replica_oid_port:replica_ssl_oid_port)
```

to the following:

```
DIRECTORY_SERVERS = (replica_host::replica_ssl_oid_port)
```
8. When the operation is finished, you must perform an `opmnctl refresh`, and then restart the components in the Applications tier instance.

- a. Enter the following command from the Applications tier (after setting ORACLE_HOME to the Applications tier home):

```
ORACLE_HOME/opmn/bin/opmnctl reload
```

- b. Navigate to the Application Server Home Page
- c. Click **Start All**.

Note: Now that you have disabled the non-SSL Oracle Internet Directory port, you must provide the "-U 1" option when using LDAP command-line utilities (such as `ldapsearch`, `ldapmodify`, and `ldapaddmt`) to connect to the SSL port.

Moving Identity Management to a New Host

This section provides a procedure for moving Identity Management to a new host. This procedure involves creating a replica (or copy) of the original Identity Management instance on a different host, along with its own new OracleAS Metadata Repository, and then reassociating Applications tier instance to use the new Identity Management instance.

Note: You cannot simply change an Applications tier instance from one Identity Management to another. The new Identity Management must be a replica of the original, created using the instructions in this procedure.

Sample Uses for this Procedure

The following are sample uses for this procedure:

- You have an existing Identity Management and associated OracleAS Metadata Repository that is used by one or more Applications tier instances. Your organization intends to replace the current Identity Management host with a new system. You can use this procedure to create a replica of the Identity Management, along with its own OracleAS Metadata Repository, and change your Applications tier instances to use the new Identity Management. You can then retire the original host.
- You would like to create a failover environment for your Identity Management. You can use this procedure to create a replica of the current Identity Management, along with its own OracleAS Metadata Repository. You can keep the replica running so it stays in sync with the original Identity Management. You can perform regular exports of data in the original OracleAS Metadata Repository and save them. In the event that you lose the original Identity Management, you can import the data to the new OracleAS Metadata Repository, and change your Applications tier instances to use the new Identity Management. Refer to ["Strategy for Performing Failover with this Procedure"](#) on page 12-12 for more information.

Assumptions and Restrictions

- For both the original and new installations, the Identity Management and OracleAS Metadata Repository can exist in the same Oracle home, or in separate Oracle homes (same or different host). If they are in separate Oracle homes, perform the operations on each in their own Oracle home.

- For both the original and new installations, the Identity Management components (SSO, Oracle Internet Directory, DAS, and DIP) may exist in the same Oracle home, or may exist in separate Oracle homes (same or different host). If they exist in separate Oracle homes, perform the operations on each in their own Oracle home.
- The OracleAS Metadata Repository used by Applications tier instances for product metadata is not affected by this procedure.
 - If the Applications tier instances use product metadata in the same OracleAS Metadata Repository that the original Identity Management instance uses, they will continue to use that OracleAS Metadata Repository after they have been reassociated to use the new Identity Management instance. If you want, you can change them to use a different OracleAS Metadata Repository after you have finished moving Identity Management. Refer to ["Changing the OracleAS Metadata Repository Used by an Applications Tier"](#) on page 12-13.
 - If the Applications tier instances use a separate OracleAS Metadata Repository for product metadata, they will continue to use that OracleAS Metadata Repository after they have changed to the new Identity Management.
- This procedure does not take OracleAS Certificate Authority into consideration.

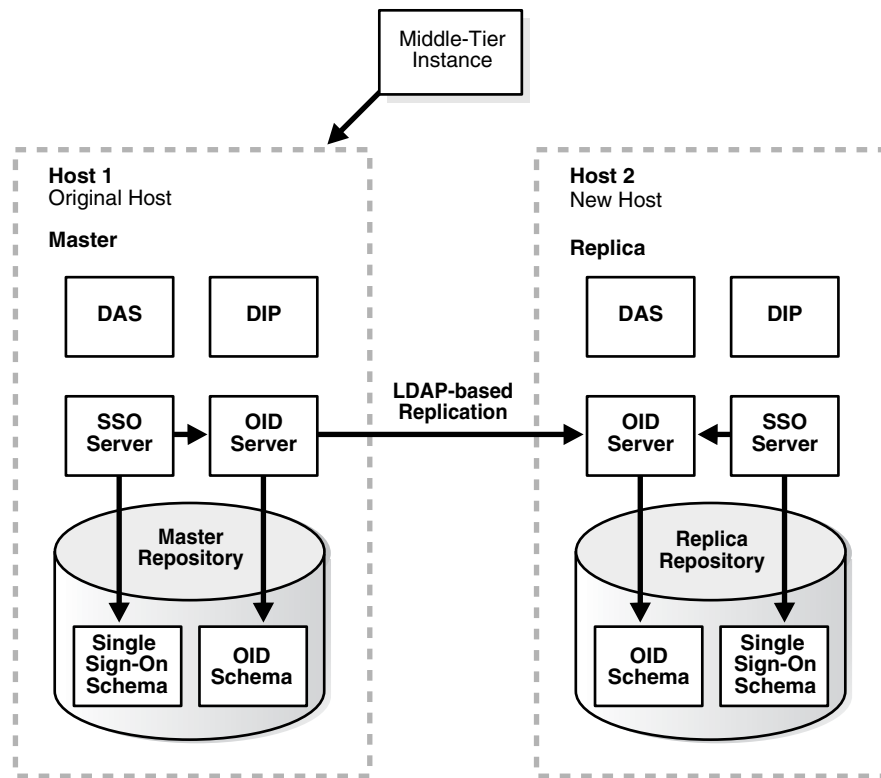
See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for information on updating OracleAS Certificate Authority when changing Identity Management services

Overview

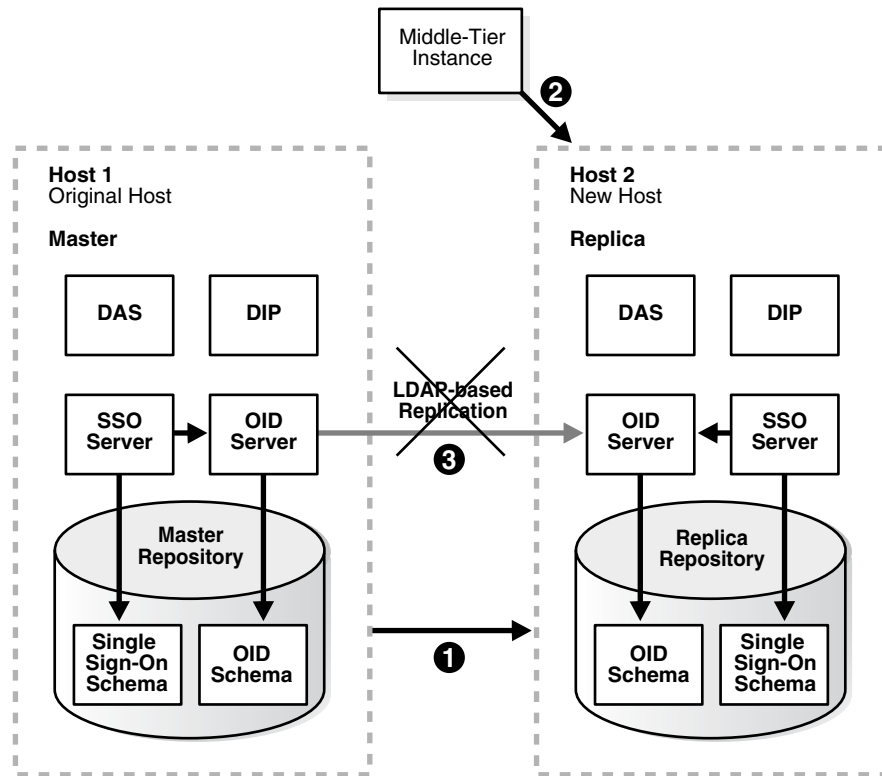
The following is an overview of the procedure for moving Identity Management to a new host:

1. You have an original Identity Management (also called the Master) used by one or more Applications tier instances. The Identity Management has a OracleAS Metadata Repository. You install and setup a new Identity Management (also called the Replica). This Identity Management has its own OracleAS Metadata Repository. The Oracle Internet Directory in the new Identity Management is an LDAP-based Replica of the original Oracle Internet Directory. Replication takes place constantly from the original Oracle Internet Directory to the new Oracle Internet Directory.

[Figure 12-2](#) shows a sample of this setup.

Figure 12–2 Original Host (Master) and New Host (Replica)

2. You perform the following steps to change to the new Identity Management. The steps are shown in [Figure 12–3](#).
 - Step 1: Migrate SSO and DIP data from the original OracleAS Metadata Repository (Master) to the new OracleAS Metadata Repository (Replica)
 - Step 2: Change the Applications tier instances to use the new OracleAS Metadata Repository.
 - Step 3: Stop the LDAP-based replication.

Figure 12-3 Changing from Original to New Identity Management

Procedure

To move Identity Management to a new host, complete the following tasks:

- [Task 1: Install and Set Up the New Identity Management and OracleAS Metadata Repository](#)
- [Task 2: Migrate OracleAS Single Sign-On and Directory Integration and Provisioning Data](#)
- [Task 3: Change Applications Tier Instances to the New Identity Management](#)
- [Task 4: Stop Replication](#)

Task 1: Install and Set Up the New Identity Management and OracleAS Metadata Repository

In this task, you install and set up the new Identity Management and its associated OracleAS Metadata Repository. The new Identity Management is an LDAP-based replica of the original Identity Management.

1. Read "[About LDAP-based Replicas](#)" on page 12-25 to learn about LDAP-based Replicas and how they are used for this procedure.
2. Follow the procedure in "[Installing and Setting Up an LDAP-Based Replica](#)" on page 12-27 to install and set up the new Identity Management and OracleAS Metadata Repository.
3. Stop all Applications tier instances that use Oracle Internet Directory (normally, this means all Applications tier instances). Using the Oracle Collaboration Suite Control, navigate to the Instance Home Page for each Applications tier instance and click Stop All. Be sure to leave Oracle Collaboration Suite Control running.

Task 2: Migrate OracleAS Single Sign-On and Directory Integration and Provisioning Data

In this task, you migrate the OracleAS Single Sign-On and Directory Integration and Provisioning Data from the original OracleAS Metadata Repository to the new OracleAS Metadata Repository. The source for the migration is the original OracleAS Metadata Repository (Master) and the target for the migration is the new OracleAS Metadata Repository (Replica).

This procedure contains the following tasks:

- [Migrate the OracleAS Single Sign-On Data](#)
- [Migrate the Directory Integration and Provisioning Data](#)

Note: Make sure the `ORACLE_HOME` and `ORACLE_SID` environment variables are set before you begin. This applies to all platforms.

Migrate the OracleAS Single Sign-On Data

To migrate the OracleAS Single Sign-On data:

1. Obtain the ORASSO schema password on the master:

```
MASTER_HOME/bin/ldapsearch -p master_oid_port -h
master_host -D "cn=orcladmin"
-w master_orcladmin_passwd -b
"orclresourcename=orasso, orclreferencename=master_global_db_name,
cn=ias infrastructure databases,
cn=ias, cn=products, cn=oraclecontext" -s base "objectclass=*"
orclpasswordattribute
```

This command prints the ORASSO password in a line like the following:

```
orclpasswordattribute=LAetjdQ5
```

2. Export the OracleAS Single Sign-On data from the master, ensuring that the `ORACLE_HOME` environment variable is set before you run this command:

```
MASTER_HOME/sso/bin/ssomig -export -s orasso -p
master_orasso_passwd -c master_db_name -log_d $MASTER_HOME/sso/log
```

`master_orasso_passwd` is the ORASSO password obtained in the previous step.

3. Copy the `ssomig.dmp` and `ssoconf.log` files from the master to the replica, preserving the exact full path for each file:

```
cp MASTER_HOME/sso/log/ssomig.dmp REPLICIA_HOME/sso/log/ssomig.dmp
cp MASTER_HOME/sso/log/ssoconf.log REPLICIA_HOME/sso/log/ssoconf.log
```

4. Obtain the ORASSO schema password on the replica:

```
REPLICIA_HOME/bin/ldapsearch -p replica_oid_port -h replica_host -D
"cn=orcladmin" -w replica_orcladmin_password -b "orclresourcename=orasso,
orclreferencename=replica_global_db_name, cn=ias infrastructure databases,
cn=ias, cn=products, cn=oraclecontext" -s base "objectclass=*"
orclpasswordattribute
```

5. Import the OracleAS Single Sign-On data to the replica:

```
REPLICIA_HOME/sso/bin/ssomig -import -overwrite -s
orasso -p replica_orasso_passwd -c replica_db_name -log_d
$REPLICIA_HOME/sso/log -discoforce
```

`replica_orasso_passwd` is the ORASSO password obtained in the previous step.

6. Validation step: Verify that the export and import of OracleAS Single Sign-On succeeded.

Verify that the OracleAS Single Sign-On migration tool reported success. You can also check the following log files for errors:

```
MASTER_HOME/sso/log/ssomig.log
REPLICA_HOME/sso/log/ssomig.log
```

See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for information on interpreting messages in the log files

Migrate the Directory Integration and Provisioning Data

To migrate your Directory Integration and Provisioning Data:

See Also: Directory Integration and Provisioning Data documentation in the *Oracle Internet Directory Administrator's Guide* for running the following commands using the HTTPS port in environments in which the Oracle Internet Directory HTTP port is disabled

1. Stop the Directory Integration and Provisioning Data server on the master:

```
MASTER_HOME/bin/oidctl server=odisrv instance=1 stop
```

2. Migrate the Directory Integration and Provisioning Data:

```
MASTER_HOME/bin/dipassistant reassociate -src_ldap_host
master_host -src_ldap_port
master_oid_port -dst_ldap_host
replica_host -dst_ldap_port replica_oid_port -src_ldap_passwd
master_orcladmin_passwd -dst_ldap_passwd replica_orcladmin_passwd
```

This command prints log messages to:

```
MASTER_HOME/ldap/odi/log/reassociate.log
```

3. Stop the Directory Integration and Provisioning Data server on the replica:

```
REPLICA_HOME/bin/oidctl server=odisrv instance=1 stop
```

4. Register the Directory Integration and Provisioning Data server on the replica:

```
REPLICA_HOME/bin/odisrvreg -D "cn=orcladmin" -w
replica_orcladmin_passwd -h replica_host -p replica_oid_port
```

5. Start the Directory Integration and Provisioning Data server on the replica:

```
REPLICA_HOME/bin/oidctl server=odisrv instance=1 flags="port=replica_oid_port"
start
```

Task 3: Change Applications Tier Instances to the New Identity Management

In each Applications tier instance, run the Change Identity Management wizard and restart the instance:

1. Using the Application Server Control Console, navigate to the Instance Home Page for the Applications tier instance.

2. Click **Infrastructure**.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the new Identity Management information.
5. Edit `ORACLE_HOME/ldap/admin/ldap.ora` in the Applications tier Oracle home to reflect the new Oracle Internet Directory information. Change the following line:

```
DIRECTORY_SERVERS = (replica_host:replica_oid_port:replica_ssl_oid_port)
```
6. When the wizard is finished, you must perform an `opmnctl reload`. Enter the following command from the Applications tier (after setting `ORACLE_HOME` to the Applications tier home):

```
ORACLE_HOME/opmn/bin/opmnctl reload
```
7. Navigate to the Application Server Home Page and start the Applications tier instance by clicking **Start All**.

If you have a problem changing the Applications tier instances to the new host, check to make sure replication is running and try again.

Task 4: Stop Replication

Stop the replication between the original Identity Management and the new Identity Management (replica) by running the following command in the new Identity Management Oracle home:

```
oidctl connect=global_db_name server=oidrepld instance=1 flags="-p oid_port" stop
```

global_db_name is the global db name of the new Identity Management. (This is referred to as *replica_db_name*.)

oid_port is the non-SSL Oracle Internet Directory port in the new Identity Management. (This is referred to as *replica_oid_port*.)

Strategy for Performing Failover with this Procedure

As mentioned in ["Sample Uses for this Procedure"](#) on page 12-6, you can modify this procedure to perform failover for Identity Management. This enables you to shift to the new Identity Management in case the original becomes unavailable or is lost in some manner.

To perform failover:

1. Install and set up the new Identity Management as described in [Task 1: Install and Set Up the New Identity Management and OracleAS Metadata Repository](#).
2. Export SSO and DIP data on a regular basis from the original OracleAS Metadata Repository. You do not need to import the data into the new OracleAS Metadata Repository. You only need to export the data and copy the files to the new OracleAS Metadata Repository Host. Refer to ["Task 2: Migrate OracleAS Single Sign-On and Directory Integration and Provisioning Data"](#) on page 12-10.
3. If you lose the original Identity Management:
 - a. Stop replication. Refer to [Task 4: Stop Replication](#).

- b. Import your most recent copy of the SSO and DIP data into the new Identity Management repository. Refer to ["Task 2: Migrate OracleAS Single Sign-On and Directory Integration and Provisioning Data"](#) on page 12-10.
- c. Change the Applications tier instances to use the new Identity Management. Refer to [Task 3: Change Applications Tier Instances to the New Identity Management](#).

Changing the OracleAS Metadata Repository Used by an Applications Tier

This section provides a procedure for changing the OracleAS Metadata Repository used by a Applications tier instance (re-association). This procedure involves making a copy of the original OracleAS Metadata Repository on a different host, and then reassociating the Applications tier instance with the new OracleAS Metadata Repository.

Note: You cannot simply change an Applications tier instance from one OracleAS Metadata Repository to another. The new OracleAS Metadata Repository must be a copy of the original, created using the instructions in this procedure.

Sample Uses for this Procedure

The following are sample uses for this procedure:

- You have an existing OracleAS Metadata Repository that is used by one or more Applications tier instances. Your organization intends to replace the current OracleAS Metadata Repository host with a new system. You can use this procedure to copy the OracleAS Metadata Repository to the new host and change your Applications tier instances to use the new OracleAS Metadata Repository. You can then retire the original host.
- You would like to move a OracleAS Metadata Repository from a host in your test environment, to a host in your Production Environment. You can use this procedure to copy the OracleAS Metadata Repository from the test to production host, and change your test Applications tier instances to use the new OracleAS Metadata Repository.

Assumptions and Restrictions

- The Applications tier instances must use Identity Management
- That Identity Management must not use the original OracleAS Metadata Repository for its Identity Management schemas; it must use a separate OracleAS Metadata Repository
- The original OracleAS Metadata Repository:
 - Must be used for product metadata and DCM management only (it cannot be used by Identity Management)
 - Must be registered with Oracle Internet Directory
- The new OracleAS Metadata Repository:

- Must not be registered with Oracle Internet Directory initially. During the procedure, you will register it with the same Oracle Internet Directory as the original OracleAS Metadata Repository.
- Must be created with the same Oracle home, datafile location, SID, and global database name as the original OracleAS Metadata Repository. You will eventually change the global database name to a unique name.
- This procedure does not take OracleAS Certificate Authority into consideration.

See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for information on updating OracleAS Certificate Authority when changing OracleAS Metadata Repository services

- If the OracleAS Metadata Repository is used for OracleAS Clusters, the cluster members will not be accessible until all members of the cluster have been reassociated with the new OracleAS Metadata Repository.

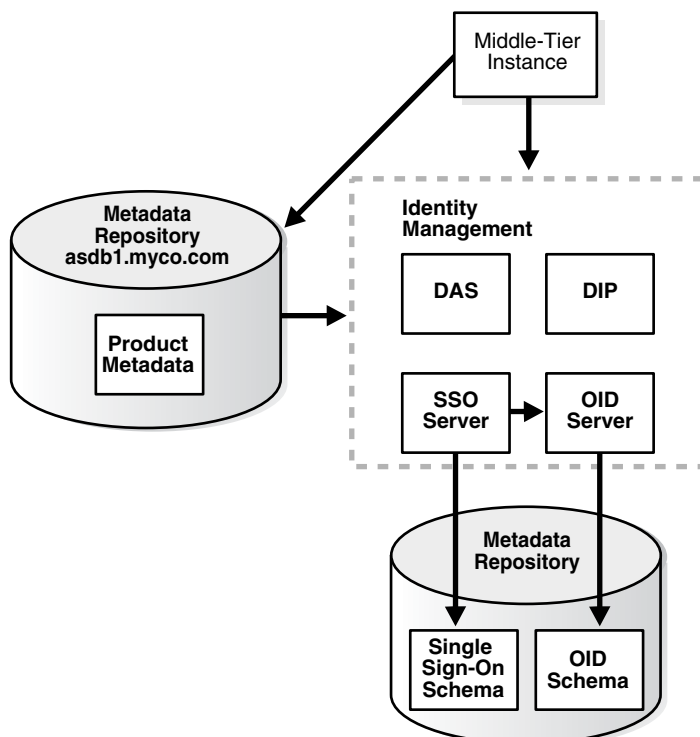
Overview

The following is an overview of the procedure for changing the OracleAS Metadata Repository used by a Applications tier:

1. You have an original OracleAS Metadata Repository. It is used by one or more Applications tier instances for product metadata. The Applications tier instances use Identity Management, and the OracleAS Metadata Repository is registered with Oracle Internet Directory in that Identity Management.

Figure 12–4 shows a sample original OracleAS Metadata Repository (asdb1.myco.com).

Figure 12–4 Original OracleAS Metadata Repository



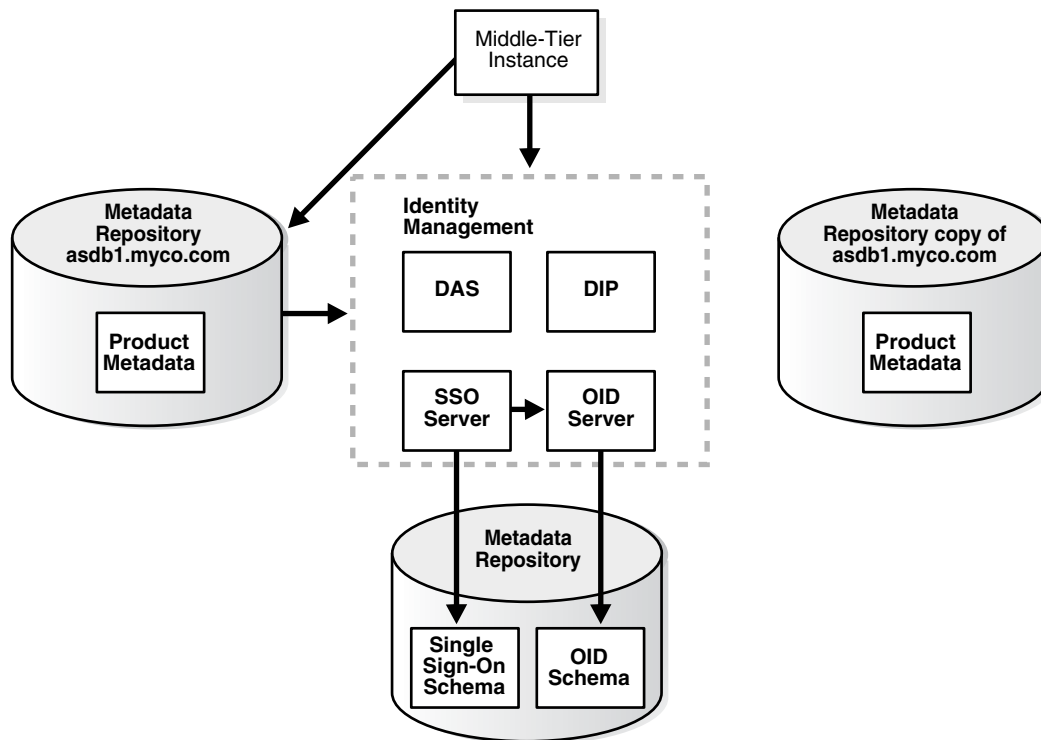
The following table shows sample attributes for the original OracleAS Metadata Repository:

Attribute	Original OracleAS Metadata Repository	New OracleAS Metadata Repository
Oracle home	/private/oraHome	N/A
Datafile location	/private/oraHome/oradata	N/A
SID	asdb1	N/A
Global db name	asdb1.myco.com	N/A
Registered with Oracle Internet Directory?	Yes	N/A

- You create a copy of the original OracleAS Metadata Repository by installing a new OracleAS Metadata Repository, backing up the original OracleAS Metadata Repository, and restoring to the new OracleAS Metadata Repository.

Figure 12–5 shows sample original and new Metadata Repositories.

Figure 12–5 Original OracleAS Metadata Repository and New OracleAS Metadata Repository



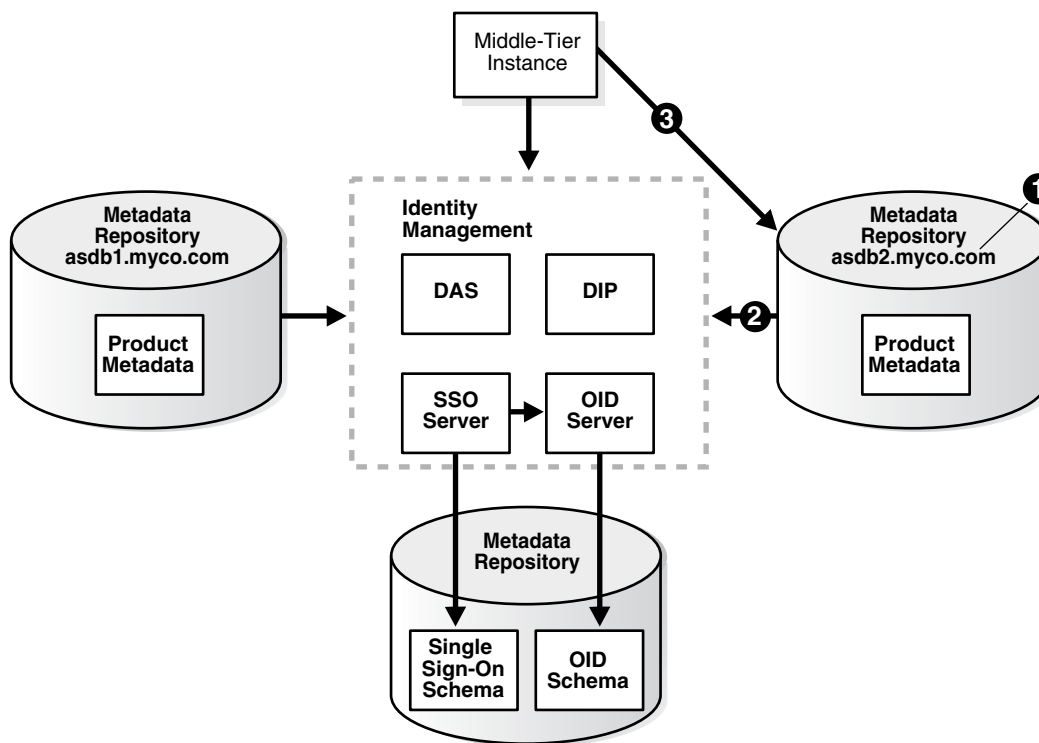
The following table shows sample attributes for the original and new Metadata Repositories:

Attribute	Original OracleAS Metadata Repository	New OracleAS Metadata Repository
Oracle home	/private/oraHome	/private/oraHome
Datafile location	/private/oraHome/oradata	/private/oraHome/oradata

Attribute	Original OracleAS Metadata Repository	New OracleAS Metadata Repository
SID	asdb1	asdb1
Global db name	asdb1.myco.com	asdb1.myco.com
Registered with Oracle Internet Directory?	Yes	No

3. You perform the following steps to change to the new OracleAS Metadata Repository. The steps are shown in [Figure 12–6](#).
- Step 1: Change the global db name of the new OracleAS Metadata Repository to a unique name (in this sample, `asdb2.myco.com`).
 - Step 2: Register the new OracleAS Metadata Repository with the same Oracle Internet Directory as the old OracleAS Metadata Repository.
 - Step 3: Change the Applications tier instances to use the new OracleAS Metadata Repository.

Figure 12–6 Changing from the Original to the New OracleAS Metadata Repository



Attribute	Original OracleAS Metadata Repository	New OracleAS Metadata Repository
Oracle home	/private/oraHome	/private/oraHome
Datafile location	/private/oraHome/oradata	/private/oraHome/oradata
SID	asdb1	asdb1
Global db name	asdb1.myco.com	asdb2.myco.com

Attribute	Original OracleAS Metadata Repository	New OracleAS Metadata Repository
Registered with Oracle Internet Directory?	Yes	Yes

4. If you are using the scenario where you no longer require the original OracleAS Metadata Repository, you can discard the original OracleAS Metadata Repository.

Procedure

This procedure for changing the OracleAS Metadata Repository associated with a Applications tier contains the following tasks:

- [Task 1: Install the New OracleAS Metadata Repository](#)
- [Task 2: Back Up the Original OracleAS Metadata Repository](#)
- [Task 3: Restore the Backup to the New OracleAS Metadata Repository](#)
- [Task 4: Configure Ultra Search Metadata in the New OracleAS Metadata Repository](#)
- [Task 5: Change the Global DB Name for the New OracleAS Metadata Repository](#)
- [Task 6: Register the New OracleAS Metadata Repository with Oracle Internet Directory](#)
- [Task 7: Change Applications tier Instances to the New OracleAS Metadata Repository](#)
- [Task 8: Update the Farm Name](#)

Before You Begin

If your Applications tier instances use OracleAS Portal and Oracle Ultra Search, you will need to supply the WKSYS schema password later in this procedure in [Task 4: Configure Ultra Search Metadata in the New OracleAS Metadata Repository](#). You should obtain this password now from the old OracleAS Metadata Repository.

Task 1: Install the New OracleAS Metadata Repository

Install the new OracleAS Metadata Repository as follows:

1. Make sure to install the OracleAS Metadata Repository into an Oracle home that has the same path as the old OracleAS Metadata Repository Oracle home
2. Use Oracle Universal Installer to install the OracleAS Metadata Repository
3. Choose to install an Infrastructure
4. Choose to install a OracleAS Metadata Repository only
5. Do not register the OracleAS Metadata Repository with Oracle Internet Directory
6. Specify the same SID and global db name as the old OracleAS Metadata Repository
7. Specify the same datafile location as the old OracleAS Metadata Repository

Task 2: Back Up the Original OracleAS Metadata Repository

In this task, you create a backup of the original OracleAS Metadata Repository. This task provides the steps for doing this using RMAN, however, if you are an experience

DBA, you can back up the OracleAS Metadata Repository according to your standard practices.

Perform all of the steps in this task on the original OracleAS Metadata Repository host.

1. Create directories to store backup files and log files. For example:

```
mkdir -p BACKUP_DIR/log_files
mkdir -p BACKUP_DIR/db_files
```

2. Make sure the original OracleAS Metadata Repository is up and running.
3. Make sure you have set the ORACLE_HOME and ORACLE_SID environment variables you run the SQL*Plus command.
4. Obtain the DBID of the original OracleAS Metadata Repository using SQL*Plus:

```
SQL> SELECT DBID FROM v$database;
```

Make note of this value; you will use it later in the procedure.

5. Create a file named *BACKUP_DIR/cold_backup.rcv* that contains the following lines. In the file, substitute the full path for *BACKUP_DIR*.

```
shutdown immediate;
startup mount;
configure controlfile autobackup on;
configure controlfile autobackup format for device type disk to 'BACKUP_DIR/db_
files/%F';

run {
allocate channel dev1 device type disk format
'BACKUP_DIR/db_files/%U';
backup database plus archivelog;
release channel dev1;
}
```

6. Run RMAN to back up the OracleAS Metadata Repository (the following is a single command; type it all on one line):

```
ORACLE_HOME/bin/rman target
cmdfile=BACKUP_DIR/cold_backup.rcv > BACKUP_DIR/log_files/backup.log
```

7. Copy the backup directories to the new host. You do not need to use the same path for *BACKUP_DIR* on the new host.

```
BACKUP_DIR/log_files
BACKUP_DIR/db_files
```

Task 3: Restore the Backup to the New OracleAS Metadata Repository

In this task you restore the backup to the new OracleAS Metadata Repository.

Perform all of the steps in this task on the new OracleAS Metadata Repository host.

1. Make sure the new OracleAS Metadata Repository is down:

```
sqlplus "sys/SYS_PASSWORD as sysdba"
SQL> shutdown immediate;
```

2. Regenerate the password file:

- On UNIX:

```
prompt> mv ORACLE_HOME/dbs/orapwORACLE_SID ORACLE_HOME/dbs/orapwORACLE_
SID.old
```

```
prompt> ORACLE_HOME/bin/orapwd file=ORACLE_HOME/dbs/orapwORACLE_SID
password=new_password
```

■ On Windows:

```
prompt> mv ORACLE_HOME\database\PWDORACLE_SID.ora ORACLE_
HOME\database\PWDORACLE_SID.ora.old
prompt> ORACLE_HOME\bin\orapwd file=ORACLE_HOME\database\PWDORACLE_SID.ora
password=new_password
```

new_password is the new SYS password. You can use the old SYS password, or set it to a new password.

3. Start the new OracleAS Metadata Repository but do not mount it:

```
SQL> startup nomount;
```

4. Create a file named *BACKUP_DIR/restore.rcv* that contains the following lines. In the file, substitute the full path for *BACKUP_DIR* and the *DBID* obtained in the previous task.

```
set dbid=DBID;
connect target /;
set controlfile autobackup format for device type disk to 'BACKUP_DIR/db_
files/%F';
restore controlfile from autobackup;
startup mount force;

run {
allocate channel dev1 device type disk format
'BACKUP_DIR/db_files/%U';
restore database;
release channel dev1;
alter database open resetlogs;
}
```

5. Run RMAN to restore the OracleAS Metadata Repository:

```
prompt> ORACLE_HOME/bin/rman cmdfile=BACKUP_DIR/restore.rcv > BACKUP_DIR/log_
files/restore.log
```

6. After you restore using RMAN, determine if the TEMP tablespace has a datafile by connecting to the database as a user with SYSDBA privileges and running the following command in SQL*Plus:

```
SQL> select file_name from dba_temp_files where tablespace_name like 'TEMP';
```

If the preceding command does not return any files, add a datafile:

```
SQL> alter tablespace "TEMP" add tempfile 'ORACLE_HOME/oradata/ \
db_name/temp01.dbf' size 5120K autoextend on next 8k maxsize unlimited;
```

Where *db_name* is the first portion of the new global db name.

Note that the above command creates a file called *temp01.dbf* and adds it to the TEMP tablespace. If the *temp01.dbf* file already exists in the directory, add a "reuse" clause to the command:

```
SQL> alter tablespace "TEMP" add tempfile 'ORACLE_HOME/oradata/ \
db_name/temp01.dbf' size 5120K reuse autoextend on next 8k maxsize unlimited;
```

Task 4: Configure Ultra Search Metadata in the New OracleAS Metadata Repository

Perform this task on the new OracleAS Metadata Repository.

1. Make sure the ORACLE_HOME and ORACLE_SID environment variables are set.
2. Run the following commands:

```
cd ORACLE_HOME/ultrasearch/admin
sqlplus "sys/SYS_PASSWORD as sysdba"
SQL> @wk0config.sql WKSYSPW JDBC_CONNSTR LAUNCH_ANYWHERE ""
```

Where:

WKSYSPW is the password of the WKSYS schema that you obtained at the beginning of this procedure.

JDBC_CONNSTR is the JDBC connection string *host:port:SID*, for example:
myhost:1521:testdb.

LAUNCH_ANYWHERE is TRUE if the OracleAS Metadata Repository is in Real Application Cluster mode, otherwise FALSE. For this procedure, you should set it to FALSE.

Task 5: Change the Global DB Name for the New OracleAS Metadata Repository

In this task, you change the global db name of the new OracleAS Metadata Repository to a new, unique name so you can register it with Oracle Internet Directory.

See Also: You can find more information on changing the global db name in article 137483.1 at <http://metalink.oracle.com>

Perform all of the steps in this task on the new OracleAS Metadata Repository host.

1. Run the following commands to set up the database:

```
sqlplus "sys/SYS_PASSWORD as sysdba"
SQL> alter system switch logfile;
SQL> alter database backup controlfile to trace resetlogs;
```

2. Check the spfile using SQL*Plus:

```
SQL> select value from v$parameter where name='spfile';
```

3. If the previous command returns no rows, you can skip this step.

If the previous command returns output like the following:

```
VALUE
-----
?/dbs/spfile@.ora
```

run the following command to create a pfile from the spfile:

```
SQL> create pfile='initORACLE_SID.ora' from spfile;
```

Where *ORACLE_SID* is the SID of the original and new OracleAS Metadata Repository.

4. Shut down the new OracleAS Metadata Repository:

```
SQL> shutdown immediate;
```

The database must be shut down with `SHUTDOWN NORMAL` or `SHUTDOWN IMMEDIATE`. You should not use `SHUTDOWN ABORT`.

5. Rename the spfile so the pfile will be used when the database instance is restarted:

```
cd ORACLE_HOME/dbs
mv spfileORACLE_SID.ora spfileORACLE_SID.ora.save
```

6. Edit the following file:

- On UNIX:

```
ORACLE_HOME/dbs/initORACLE_SID.ora
```

- On Windows:

```
ORACLE_HOME\database\initORACLE_SID.ora
```

Update the `db_name` to the new db name (the first portion of the new global db name). For example, if the new global db name is `asdb1.myco.com`, the value of `db_name` should be `asdb1`. Note that this is not necessarily (nor likely) the same value as the SID on the new OracleAS Metadata Repository.

7. Rename the following directory with the new `db_name`:

```
ORACLE_HOME/oradata/db_name
```

8. Rename the control files so they do not exist later when the new ones are created:

```
cd ORACLE_HOME/oradata/db_name

mv control01.ctl control01.ctl.old
mv control02.ctl control02.ctl.old
mv control03.ctl control03.ctl.old
```

9. Rename the following directory with the new `db_name`:

```
ORACLE_HOME/admin/db_name
```

10. Edit the following file:

- On UNIX:

```
ORACLE_HOME/admin/db_name/pfile/initORACLE_SID.ora
```

- On Windows:

```
ORACLE_HOME\admin\db_name\pfile\init.ora
```

Change all instances of the old db name to the new db name; do not update the SID. To do this, change the old db name in all directory paths and the `db_name` parameter. Do not update the `instance_name` parameter, because that is set to the SID.

11. Change to the trace file directory:

```
cd ORACLE_HOME/admin/db_name/udump
```

Note that the above is the default location for the trace file directory. This location can be overridden by the `user_dump_dest` parameter in `initORACLE_SID.ora` or `spfileORACLE_SID.ora`.

12. Locate the trace file; it has a name of the form `oraNNNNN.trc`, where `NNNNN` is a number. Choose the trace file with the most recent modification date.

13. Copy the contents of the trace file, starting from the line with "STARTUP NOMOUNT" down to the end of the file, into a new file named *BACKUP_DIR/ccf.sql*.
14. Edit *BACKUP_DIR/ccf.sql* as follows (an example of *ccf.sql* after performing the edits in this step is shown in [Example 12-1](#).)

- a. Update the following line with the new global db name and change "REUSE" to "SET":

Before modification:

```
CREATE CONTROLFILE REUSE DATABASE "OLD_GLOBAL_DB_NAME" RESETLOGS ...
```

After modification:

```
CREATE CONTROLFILE SET DATABASE "NEW_GLOBAL_DB_NAME" RESETLOGS ...
```

- b. Remove the following line:

```
# STANDBY LOGFILE
```

- c. Comment out the following lines, if they exist, with "REM", as shown:

```
REM RECOVER DATABASE USING BACKUP CONTROLFILE
```

```
REM VARIABLE RECNO NUMBER;
```

```
REM EXECUTE :RECNO := SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILE
AUTOBACKUP', 'ON');
```

```
REM VARIABLE RECNO NUMBER;
```

```
REM EXECUTE :RECNO := SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILEAUTOBACKUP
FORMAT FOR DEVICE TYPE', 'DISK TO
BACKUP_DIR/db_files/%F');
```

```
REM ALTER TABLESPACE TEMP ADD TEMPFILE 'ORACLE_HOME/TEMP01.DBF' SIZE
5242880 AUTOEXTEND ON MAXSIZE 4294950912 REUSE;
```

- d. Change all comment symbols (#) to "REM".

Example 12-1 Example *ccf.sql* File after Edits

```
STARTUP NOMOUNT
CREATE CONTROLFILE set DATABASE "<NEW DATABASE>" RESETLOGS ARCHIVELOG
MAXLOGFILES 50
MAXLOGMEMBERS 5
MAXDATAFILES 100
MAXINSTANCES 1
MAXLOGHISTORY 226
LOGFILE
GROUP 1 '/private1/inst/oradata/asdb/redo01.log' SIZE 50M,
GROUP 2 '/private1/inst/oradata/asdb/redo02.log' SIZE 50M,
GROUP 3 '/private1/inst/oradata/asdb/redo03.log' SIZE 50M
DATAFILE
'/private1/inst/oradata/asdb/system01.dbf',
'/private1/inst/oradata/asdb/undotbs01.dbf',
'/private1/inst/oradata/asdb/drsys01.dbf',
'/private1/inst/oradata/asdb/dcm.dbf',
'/private1/inst/oradata/asdb/portal.dbf',
'/private1/inst/oradata/asdb/ptldoc.dbf',
'/private1/inst/oradata/asdb/ptlidx.dbf',
```



```

'/privatel/inst/oradata/asdb/ptllog.dbf',
'/privatel/inst/oradata/asdb/oca.dbf',
'/privatel/inst/oradata/asdb/discoplct1.dbf',
'/privatel/inst/oradata/asdb/discoplmt1.dbf',
'/privatel/inst/oradata/asdb/oss_sys01.dbf',
'/privatel/inst/oradata/asdb/wcrsys01.dbf',
'/privatel/inst/oradata/asdb/uddisys01.dbf',
'/privatel/inst/oradata/asdb/ip_dt.dbf',
'/privatel/inst/oradata/asdb/ip_rt.dbf',
'/privatel/inst/oradata/asdb/ip_idx.dbf',
'/privatel/inst/oradata/asdb/ip_lob.dbf',
'/privatel/inst/oradata/asdb/attrsl_oid.dbf',
'/privatel/inst/oradata/asdb/battrsl_oid.dbf',
'/privatel/inst/oradata/asdb/gcatsl_oid.dbf',
'/privatel/inst/oradata/asdb/gdefaultl_oid.dbf',
'/privatel/inst/oradata/asdb/svrngl_oid.dbf',
'/privatel/inst/oradata/asdb/ias_meta01.dbf'
CHARACTER SET WE8MSWIN1252
;
REM Configure RMAN configuration record 1
REM VARIABLE RECNO NUMBER;
REM EXECUTE :RECNO := SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILE
AUTOBACKUP','ON');
REM Configure RMAN configuration record 2
REM VARIABLE RECNO NUMBER;
REM EXECUTE :RECNO := SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILE AUTOBACKUP
FORMAT FOR DEVICE TYPE','DISK TO /privatel/inst/backup_dir/db_files/%F');
REM Recovery is required if any of the datafiles are restored backups,
REM or if the last shutdown was not normal or immediate.
REM RECOVER DATABASE USING BACKUP CONTROLFILE
REM Database can now be opened zeroing the online logs.
ALTER DATABASE OPEN RESETLOGS;
REM No tempfile entries found to add.

```

15. Determine if the TEMP tablespace has a datafile by connecting to the database as a user with SYSDBA privileges and running the following command in SQL*Plus:

```
SQL> select file_name from dba_temp_files where tablespace_name like 'TEMP';
```

If the preceding command does not return any files, add a datafile:

```
SQL> alter tablespace "TEMP" add tempfile 'ORACLE_HOME/oradata/ \
db_name/temp01.dbf' size 5120K autoextend on next 8k maxsize unlimited;
```

Where *db_name* is the first portion of the new global db name.

Note that the above command creates a file called temp01.dbf and adds it to the TEMP tablespace. If the temp01.dbf file already exists in the directory, add a "reuse" clause to the command:

```
SQL> alter tablespace "TEMP" add tempfile 'ORACLE_HOME/oradata/ \
db_name/temp01.dbf' size 5120K reuse autoextend on next 8k maxsize unlimited;
```

16. Run the ccf.sql script:

```
SQL> @BACKUP_DIR/ccf.sql
```

17. Change the global db name in the database:

```
SQL> alter database rename global_name to NEW_GLOBAL_DB_NAME;
```

18. Update the service name and the global db name to the new global db name in the `tnsnames.ora` file and **listener.ora** file:

```
ORACLE_HOME/network/admin/tnsnames.ora
(UNIX) ORACLE_HOME/network/admin/listener.ora
(Windows) ORACLE_HOME\network\admin\listener.ora
```

Note that you should not change the SID.

19. Edit the following file:

```
(UNIX) ORACLE_HOME/config/ias.properties
(Windows) ORACLE_HOME\config\ias.properties
```

Change the `InfrastructureDBCommonName` parameter to the new global db name.

Task 6: Register the New OracleAS Metadata Repository with Oracle Internet Directory

In this task, you register the new OracleAS Metadata Repository with the same Oracle Internet Directory used by the original OracleAS Metadata Repository. To do this, you run Oracle Application Server Metadata Repository Creation Assistant (OracleAS Metadata Repository Creation Assistant), a wizard that guides you through the registration.

Note: OracleAS Metadata Repository Creation Assistant is available on the "OracleAS Metadata Repository Creation Assistant and Utilities" CD-ROM.

To register the new OracleAS Metadata Repository with Oracle Internet Directory, start up OracleAS Metadata Repository Creation Assistant on the host where the new OracleAS Metadata Repository is installed:

```
runRepca -OH ORACLE_HOME -REGISTER
```

Where `ORACLE_HOME` is the new OracleAS Metadata Repository Oracle home.

The wizard will guide you through the process.

See Also: *Oracle Application Server Installation Guide* for more information on registering the OracleAS Metadata Repository with Oracle Internet Directory

Task 7: Change Applications tier Instances to the New OracleAS Metadata Repository

On each Applications tier instance you want to change to the new OracleAS Metadata Repository, run the Change OracleAS Metadata Repository wizard and restart the instance:

1. Using the Application Server Control Console, navigate to the Instance Home Page for the Applications tier instance.
2. Make sure all components except Management are down. If not, click the **Stop All** button to stop them. Note that this will not stop Management.
3. Click **Infrastructure**.
4. On the Infrastructure Page, in the OracleAS Metadata Repository section, click **Change**.

5. Follow the steps in the wizard for supplying the new OracleAS Metadata Repository information.
6. When the wizard is finished, you must perform an `opmnctl reload`. Enter the following command from the Applications tier (after setting `ORACLE_HOME` to the Applications tier home):

```
ORACLE_HOME/opmn/bin/opmnctl reload
```

7. Navigate to the Application Server Home Page and start the Applications tier instance by clicking **Start All**.

Task 8: Update the Farm Name

Run the following command in the Oracle home of one of the Applications tier instances that you changed to use the new OracleAS Metadata Repository in the previous task:

```
ORACLE_HOME/dcm/bin/dcmctl resetFarmName new_farm_name
```

Where *new_farm_name* is the global db name of the new OracleAS Metadata Repository.

Note: You only need to run the command in one Applications tier instance. The command will update all other instances.

About LDAP-based Replicas

This section describes how to install and configure an LDAP-based replica. It contains the following topics:

- [What is an LDAP-based Replica?](#)
- [How is the LDAP-based Replica Used for Changing Infrastructure Services?](#)

What is an LDAP-based Replica?

Oracle Internet Directory replication is the process of copying and maintaining the same data (or naming context) on multiple directory servers. Simply put, replication is a means of having two identical directories that contain the same information. One directory is called the master (or supplier). This directory contains the master copy of the naming context. The other directory is called the replica (or consumer). The master supplies replication updates to the replica, which keeps the master and replica in sync.

There are different types of replicas. This procedure uses an LDAP-based replica, which means the protocol for transferring data between the master and the replica is LDAP.

See Also: *Oracle Internet Directory Administrator's Guide* for more information on directory replication and LDAP-based replicas

For the purposes of this procedure, the master and replica directories are part of a larger environment that includes the Identity Management installations that contain the directories, and the OracleAS Metadata Repository that support them. This is called the LDAP-based Replica Environment, and it contains the following:

Master—The Identity Management installation containing the Oracle Internet Directory that holds the master copy of the naming context. It supplies replication updates to the replica.

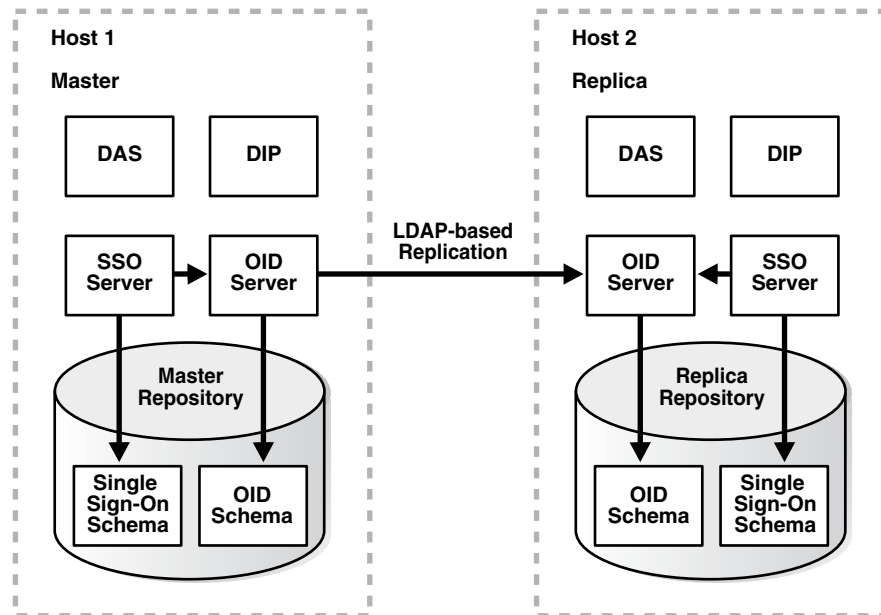
Master Repository—The OracleAS Metadata Repository that the master uses to store its Identity Management schemas.

Replica—The Identity Management installation containing the replicated Oracle Internet Directory.

Replica Repository—The Metadata Repository that the replica uses to store its Identity Management schemas.

Figure 12–7 illustrates the LDAP-based replica environment.

Figure 12–7 LDAP-based Replica Environment



How is the LDAP-based Replica Used for Changing Infrastructure Services?

Typically, an LDAP-based replica is used to provide high availability and improved performance for directory users. For the purposes of changing Infrastructure services, the LDAP-based Replica is used as follows:

- For "[Moving Identity Management to a New Host](#)" on page 12-6, the LDAP-based replica is created as a way of moving Identity Management from one host to another. The Master is the original Identity Management installation, and the Replica is the new Identity Management installation. In this case, replication is used to create an identical copy of the original Identity Management on a new host. You can then change your Applications tiers from the old Identity Management (Master) to the new Identity Management (Replica) and discard the Master.
- The replica can also be used to move from a test to production environment. The Master is the production Identity Management, and the Replica is the test Identity Management. When you are ready to merge your test environment into your production environment, you can migrate data from your test Identity Management (Replica) to your production Identity Management (Master) and change your Applications tiers from the test Identity Management to the production Identity Management. You can then discard the test Identity Management or continue to use it for testing.

Installing and Setting Up an LDAP-Based Replica

This section describes how to install and set up an LDAP-based replica environment.

Things to Know Before You Start

You should be aware of these important items before you start the procedure:

- This procedure uses a single Infrastructure Oracle home that contains Identity Management and the Metadata Repository. However, it is fine to split the Infrastructure installation so Identity Management is in one Oracle home and the Metadata Repository is in another Oracle home. You can also distribute the Identity Management components (OracleAS Single Sign-On, Oracle Internet Directory, Delegated Administration Services, Directory Integration and Provisioning) across different hosts. If you do this, perform the operations on each component in their respective Oracle homes.
- The replica always uses port 389 for the non-SSL Oracle Internet Directory port, and 636 for the SSL Oracle Internet Directory port, regardless of what is reported by Oracle Universal Installer, or printed in `ORACLE_HOME/install/portlist.ini`. Make sure no other processes are using ports 389 and 636 on the replica host before you start the procedure.
- Make sure you use the `ldapsearch` and `ldapmodify` commands that are in `ORACLE_HOME/bin`. (Some operating systems ship their own version of these commands—do not use those.)
- These procedures use the `remtool` and `oidpasswd` commands. The messages returned by these commands are in UTF-8 encoding and are unreadable in most non-English environments. To work around this, set the `NLS_LANG` environment variable to `american_american.character_set` before running these commands. Most character sets (for example, `US7ASCII`) will work.

See Also: *Oracle Application Server Globalization Guide*

- Make sure the `ORACLE_HOME` and `ORACLE_SID` environment variables are set. This applies to all platforms.

Procedure

This section contains the procedure for setting up an LDAP-based replica. It contains the following tasks:

- [Task 1: Obtain the Master and Master Repository](#)
- [Task 2: Install Applications Tier Instances \(Optional\)](#)
- [Task 3: Install and Configure the Replica](#)

Task 1: Obtain the Master and Master Repository

Most likely, you already have your Master and Master Repository. The Master and Master Repository are the installations you would like to move to a new host, and the LDAP-based replica will be the relocated installations.

If you are starting from scratch, you can install a Master and Master Repository as follows:

1. Install Oracle Collaboration Suite using Oracle Universal Installer.
2. Choose the Infrastructure Installation.

3. Choose to install Identity Management and OracleAS Metadata Repository.
4. Choose to configure the following components: Oracle Internet Directory, OracleAS Single Sign-On, Delegated Administration Services, and Directory Integration and Provisioning.

Task 2: Install Applications Tier Instances (Optional)

Most likely, you already have Applications tier instances using the Master for Identity Management services. This is fine, and, if desired, you can install and configure additional instances to use the Master now, or at the end of this procedure after you have configured the replica, or both.

These Applications tier instances can use the Master Repository for their product metadata, or they can use a different repository.

Task 3: Install and Configure the Replica

You can install and configure the Replica using Oracle Universal Installer. Be sure to install the Replica on a different host than the Master.

See Also: *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows* for information on installing an Oracle Internet Directory replica

When the installation has finished, replication is configured and all components are up and running. You can return to the main procedure.

Applications Tier Application Reconfiguration

As part of the re-association process, Applications tier applications which are affected need to be configured to use the Collaboration Suite Database instance on the new Infrastructure. The procedure for setup and reconfiguration varies for each type of Oracle Collaboration Suite application.

The following sections describe how to setup and reconfigure each standard Oracle Collaboration Suite Applications tier application:

- [Oracle Calendar Re-association](#)
- [Oracle Real-Time Collaboration Re-association](#)

Oracle Calendar Re-association

For Oracle Collaboration Suite, Oracle Calendar uses the Collaboration Suite Database component to store some of its data. Which Collaboration Suite Database is used by Calendar is determined when Calendar is first deployed. The re-association process described in this section allows you to change the Collaboration Suite Database component that Calendar uses from one physical instance to another. There will not be any data loss and the Calendar will work as it did with the original Collaboration Suite Database.

You must meet the following requirements before Calendar can be re-associated to the new Collaboration Suite Database:

- The version of the target Collaboration Suite Database must be the same or greater than the original Collaboration Suite Database

- The target Collaboration Suite Database must be registered to the same Infrastructure as Calendar.

To reassociate Calendar to a different Infrastructure instance, follow the procedure described in ["Changing the OracleAS Metadata Repository Used by an Applications Tier"](#) on page 12-13.

To reassociate Calendar with a new Infrastructure instance, you invoke a java class on the Calendar Applications tier installation.

The java jar file is found in `$ORACLE_HOME/ocal/jlib/ocal_clnt.jar`

The java class is `oracle.calendar.server.configuration.InitStorage`

Usage: `InitStorage -oh oraclehome -reassociate -sourcedatabase <source dbname> -sysp <sys password> -targetdatabase <target dbname> -D binddn -w bindpassword -oh <ORACLE_HOME path> -reassociate -sourcedatabase <Source DB Global Name> -targetdatabase <Target DB Global Name> -sysp <SYS password on source database> -D <OID Credentials> -w <OID credentials password>`

In the following example, [Example 12-2](#) on page 12-29, the original Collaboration Suite Database is `asdb.host1.domain.com` and the target Collaboration Suite Database is `asdb.host2.domain.com`. The Oracle Internet Directory login is `cn=orcladmin` and the Oracle Internet Directory password is `welcome1`.

Example 12-2 Reassociating Calendar with a new Collaboration Suite Database

```
$ORACLE_HOME/jre/java -classpath $ORACLE_HOME/ocal/jlib/ocal_clnt.jar:$ORACLE_
HOME/ldap/jlib/ldapjclnt10.jar:$ORACLE_HOME/jlib/ojmisc.jar:$ORACLE_
HOME/jdbc/lib/classes12.jar:$ORACLE_HOME/jdbc/lib/nls_charset12.jar:$ORACLE_
HOME/rdbms/jlib/aqapi.jar oracle.calendar.server.configuration.InitStorage -oh
$ORACLE_HOME -reassociate -sourcedatabase asdb.host1.domain.com -sysp welcome1
-targetdatabase asdb.host2.domain.com -D cn=orcladmin -w welcome1
```

Oracle Real-Time Collaboration Re-association

The following steps show how to reassociate Oracle Real-Time Collaboration 10g Release 1 (10.1.1) with an existing Release 9.0.4.1 Oracle Internet Directory.

1. Go to the existing Oracle Internet Directory page (`http://oid_hostname:port/pls/orasso`) and create a new partner application, with the following parameters:

- Name: `http://applications_tier_hostname`
- Home URL: `http://applications_tier_hostname:port`
- Success URL: `http://applications_tier_hostname:port/osso_login_success`
- Logout URL; `http://applications_tier_hostname:port/osso_logout_success`

2. Change to the `$ORACLE_HOME/Apache/Apache/conf/osso/` directory on the Applications tier.

```
cd $ORACLE_HOME/Apache/Apache/conf/osso
```

3. Using the information you set up for the partner application, create a text file named `my_file.conf.clr` with the following contents:

```
sso_server_version=v1.2
cipher_key=cipher_key
site_id=site_id
```

```

site_token=site_token
login_url=http://hostname:port/pls/orasso/orasso.wvso_app_admin.ls_login
logout_url=http://hostname:port/pls/orasso/orasso.wvso_app_admin.ls_logout
cancel_url=http://hostname

```

4. Enter the following command:

```

$ORACLE_HOME/Apache/Apache/bin/apobfuscate my_file.conf.clr my_obfuscated_
file.conf root

```

5. Use a text editor to open the mod_osso.conf file.
6. Change the following entries:

Original text:

```

<IfModule mod_osso.c>
    OsoIpCheck off
    OsoIdleTimeout off
    OsoConfigFile /rtc/m8e/apps/Apache/Apache/conf/osso/osso.conf
...

```

New text:

```

<IfModule mod_osso.c>
    OsoIpCheck off
    OsoIdleTimeout off
    OsoConfigFile /rtc/m8e/apps/Apache/Apache/conf/osso/<SomeName>.conf
...

```

7. Use the rtcctl utility to set the following properties on the Application tier.

```

rtcctl> setProperty -system true -pname ldaphost -pvalue old_release_hostname
rtcctl> setProperty -system true -pname ldapport -pvalue old_release_port
rtcctl> setProperty -system true -pname ldappassword -pvalue old_release_
password
rtcctl> setProperty -system true -pname UserProvisioningEnabled -pvalue false

```

8. Change to the \$ORACLE_HOME/j2ee/OC4J_imeeting/application-deployments/imeeting directory.
9. Use a text editor to open the orion-application.xml file.
10. Comment out the following section by adding the <!-- and --> opening and closing markers, as follows:

```

<!--      <jazn provider="LDAP" >
                <property name="s2s.auth.support" value="true" />
      </jazn>
-->

```

11. Stop and restart applications on the Applications tier:

```

$ORACLE_HOME/opmn/bin/opmnctl stopall
$ORACLE_HOME/opmn/bin/opmnctl startall

```

Managing High-Availability Environments

This chapter describes how to manage the high-availability environments in Oracle Collaboration Suite. Managing high-availability environments primarily consists of managing nodes of Real Application Clusters (RAC) and Oracle Collaboration Suite Applications. The chapter consists of the following sections:

- [Adding and Removing RAC nodes](#)
- [Adding or Deleting Nodes from Oracle Collaboration Suite Database](#)
- [Removing Nodes from Oracle Collaboration Suite Applications](#)
- [Configuring Manual Cold Failover for Oracle Calendar Server](#)
- [Starting and Stopping Oracle Collaboration Suite in a High-Availability Environment](#)

Adding and Removing RAC nodes

This section describes how to add and delete nodes and instances in Oracle RAC databases. The topics in this section are:

- [Overview of Node Addition Procedures](#)
- [Step 1: Connecting New Nodes to the Cluster](#)
- [Step 2: Extending Clusterware and Oracle Software to New Nodes](#)
- [Step 3: Preparing Storage for RAC on New Nodes](#)
- [Step 4: Adding Nodes at the Oracle RAC Database Layer](#)
- [Step 5: Adding Database Instances to New Nodes](#)
- [Step 5: Adding Database Instances to New Nodes](#)
- [Adding Nodes that Already Have Clusterware and Oracle Software to a Cluster](#)
- [Deleting Instances from Real Application Clusters Databases](#)
- [Deleting Nodes from Oracle Clusters on UNIX-Based Systems](#)
- [Deleting Nodes from Oracle Clusters on Windows-Based Platforms](#)

Overview of Node Addition Procedures

This section explains how to add nodes to clusters. The steps to add nodes to cluster are as follows:

- Set up the new nodes to be part of your cluster at the network level.

- Extend the Cluster Ready Services (CRS) home from an existing CRS home to the new nodes.
- Extend the Oracle database software with RAC components to the new nodes.
- Finally, make the new nodes members of the existing cluster database.

Note: If your clusterware supports, you can add nodes on some UNIX-based platforms without stopping existing nodes. Refer to your vendor-specific clusterware documentation for more information.

If the nodes, that you are adding to your cluster, do not have clusterware or Oracle software, then you must complete the following five steps. The procedures in the steps assume that you already have an operational UNIX-based or Windows-based RAC environment. The details of the steps appear in the following subsections.

- [Step 1: Connecting New Nodes to the Cluster](#)
- [Step 2: Extending Clusterware and Oracle Software to New Nodes](#)
- [Step 3: Preparing Storage for RAC on New Nodes](#)
- [Step 4: Adding Nodes at the Oracle RAC Database Layer](#)
- [Step 5: Adding Database Instances to New Nodes](#)

To add a node to your cluster, when the node is already configured with clusterware and Oracle software, follow the procedure described in [Adding Nodes that Already Have Clusterware and Oracle Software to a Cluster](#).

Step 1: Connecting New Nodes to the Cluster

Complete the following procedures to connect the new nodes to the cluster and to prepare them to support your cluster database:

- Making Physical Connections
- Installing Operating System
- Creating Oracle Users
- Checking the Installation

Making Physical Connections

Connect the hardware of the new nodes to the network infrastructure of your cluster. This includes establishing electrical connections, configuring network interconnects, configuring shared disk subsystem connections, and so on. Refer to your hardware vendor documentation for details about this step.

Installing Operating System

Install a cloned image of the operating system that matches the operating system on the other nodes in your cluster. This includes installing required service patches and drivers. Refer to your hardware vendor documentation for details about this process.

Creating Oracle Users

As `root` user on UNIX-based systems, create the Oracle users and groups using the same user ID and group ID as on the existing nodes. On Windows-based systems, perform the installation as an Administrator.

Checking the Installation

To verify that your installation is configured correctly, perform the following steps:

1. Ensure that the new nodes can access the private interconnect. This interconnect must be properly configured before you can complete the procedures in [Step 2: Extending Clusterware and Oracle Software to New Nodes](#).
2. If you are not using a cluster file system, then determine the location on which your cluster software was installed on the existing nodes. Make sure that you have at least 250MB of free space on the same location on each of the new nodes to install the CRS software. In addition, ensure you have enough free space on each new node to install the Oracle binaries.
3. Ensure that user equivalence is established on the new nodes.
4. Run the following platform-specific procedures:

- On UNIX-based systems:

Verify user equivalence to and from an existing node to the new nodes using `rsh` or `ssh`.

- On Windows-based systems:

Make sure that you can run the following command from each of the existing nodes of your cluster where the `host_name` is the public network name of the new node.

```
NET USE \\host_name\C$
```

You have the required administrative privileges on each node if the operating system responds if the following message is displayed:

```
Command completed successfully.
```

After completing the procedures in this section, your new nodes are connected to the cluster and configured with the required software to make them visible to the clusterware. Configure the new nodes as members of the cluster by extending the cluster software to the new nodes as described in [Step 2: Extending Clusterware and Oracle Software to New Nodes](#).

Note: Do not change a host name after CRS installation. This includes adding or deleting a domain qualification.

Step 2: Extending Clusterware and Oracle Software to New Nodes

The following topics describe how to add new nodes to the clusterware and to the Oracle database software layers using Oracle Universal Installer.

- Adding Nodes at the Vendor Clusterware Layer (UNIX Only)
- Adding Nodes at the Oracle Clusterware Layer (UNIX and Windows)

Adding Nodes at the Vendor Clusterware Layer (UNIX Only)

If you are using a Windows-based system, then skip this subsection and proceed to the next section. For UNIX-based systems, add the new nodes at the clusterware layer according to the vendor clusterware documentation. For systems using shared storage for the CRS home, ensure that the existing clusterware is accessible by the new nodes. Also ensure that the new nodes can be brought online as part of the existing cluster. Proceed to the next section to add the nodes at the clusterware layer.

Adding Nodes at the Oracle Clusterware Layer (UNIX and Windows)

On all platforms, complete the following steps. Oracle Universal Installer requires access to the private interconnect that you checked as part of the installation validation in Step 1.

1. On one of the existing nodes, navigate to the `CRS home/oui/bin` directory on UNIX-based systems or to the `CRS home\oui\bin` directory on Windows-based systems. On UNIX, run the `addNode.sh` script and on Windows run the `addNode.bat` script to start Oracle Universal Installer.
2. Oracle Universal Installer runs in the add node mode and the Oracle Universal Installer Welcome page appears. Click **Next** and the Specify Cluster Nodes for Node Addition page appears.
3. The upper table on the Specify Cluster Nodes for Node Addition page shows the existing nodes associated with the CRS home from which you launched Oracle Universal Installer. Use the lower table to enter the public and private node names of the new nodes.
4. If you are using vendor clusterware, then the public node names automatically appear in the lower table. Click **Next** and Oracle Universal Installer verifies connectivity on the existing nodes and on the new nodes. The verifications that Oracle Universal Installer performs include determining if the following conditions are true:
 - The nodes are up
 - The nodes are accessible by way of the network
 - The user has write permission to create the CRS home on the new nodes
 - The user has write permission to the Oracle Universal Installer inventory in the `oraInventory` directory on UNIX or `Inventory` directory on Windows
5. If Oracle Universal Installer detects that the new nodes do not have an inventory location, then:
 - On UNIX platforms Oracle Universal Installer displays a dialog box asking you to run the `oraInstRoot.sh` script on the new nodes.
 - On Windows platforms Oracle Universal Installer automatically updates the inventory location in the Registry key.

If any verifications fail, then Oracle Universal Installer redisplay the Specify Cluster Nodes for Node Addition page with a Status column in both tables indicating errors. Correct the errors or deselect the nodes that have errors and proceed. However, you cannot deselect existing nodes. You must correct problems on nodes that are already part of your CRS cluster before you can proceed with node addition. If all the checks succeed, then Oracle Universal Installer displays the Node Addition Summary page.

Note: Oracle recommends that you install CRS on every node in the cluster that has vendor clusterware installed.

6. The Node Addition Summary page displays the following information showing the products that are installed in the CRS home that you are extending to the new nodes.
 - The source for the add node process, which in this case is the CRS home
 - The private node names that you entered for the new nodes

- The new nodes that you entered
 - The required and available space on the new nodes
 - The installed products listing the products that are already installed on the existing CRS home
7. The Cluster Node Addition Progress page shows the status of the cluster node addition process. The table on this page has two columns showing the phase of the node addition process and the phase's status according to the following platform-specific content.

On UNIX-based systems, this page shows the following four Oracle Universal Installer phases:

- **Instantiate Root Scripts:** The root script `rootaddnode.sh` is instantiated with the public and private node names that you entered on the Cluster Node Addition page.
- **Copy the CRS Home to the New Nodes:** CRS home is copied to the new nodes unless the CRS home is on a cluster file system.
- **Run `rootaddnode.sh` and `root.sh`:** A dialog box is displayed prompting you to run `rootaddnode.sh` on the local node from which you are running Oracle Universal Installer. Then you are prompted to run `root.sh` on the new nodes.
- **Save Cluster Inventory:** The node list, associated with the CRS home and its inventory, is updated.

On Windows-based systems, this page shows the following three Oracle Universal Installer phases:

- **Copy CRS Home to New Nodes:** CRS home is copied to the new nodes unless the CRS home is on the Oracle Cluster File System.
- **Performs Oracle Home Setup:** The Registry entries are updated for the new nodes, services are created, and folder entries are created.
- **Save Cluster Inventory:** The node list, associated with the CRS home and its inventory, is updated.

For all platforms, the Status column of the Cluster Node Addition Progress page displays In Progress while the phase is in progress, Suspended when the phase is pending execution, and Succeeded after the phase completes. On completion, click **Exit** to end Oracle Universal Installer session. After Oracle Universal Installer displays the End of Node Addition page, click **Exit** to end the Oracle Universal Installer session.

8. On Windows-based systems, run the following command to identify the node names and node numbers that are currently in use:

```
CRS home\bin\olsnodes -n
```

Run the `crssetup.exe` command using the next available node names and node numbers to add CRS information for the new nodes. Use the following syntax for `crssetup.exe` where `I` is the first new node number, `nodeI` through `nodeI+n` is a list of the nodes that you are adding, `nodeI-number` through `nodeI+n-number` represent the node numbers assigned to the new nodes, and `pnI` through `pnI+1` is the list of private networks for the new nodes:

```
CRS home\bin\crssetup.exe add
-nn nodeI,nodeI-number,nodeI+1,nodeI+1-number,...nodeI+n,nodeI+n-number
-pn pnI,nodeI-number,pnI+1,nodeI+1-number,...pnI+n,nodeI+n-number
```

```
crssetup.exe add -nn nodeI,node number -pn pnodeI,node number
```

These are the private network names or Internet Protocol (IP) addresses that you entered in Step 3 of this procedure in the Specify Cluster Nodes for Node Addition page. For example:

```
crssetup.exe add -nn node3,3,node4,4 -pn node3_pvt,3,node4_pvt,4
```

On all platforms, run the `racgons` utility from the `bin` subdirectory of the CRS home to configure the Oracle Notification Services port number as follows:

```
racgons add_config new_node_name:4948
```

After you have completed the procedures in this section for adding nodes at the Oracle clusterware layer, you have successfully extended the CRS home from your existing CRS home to the new nodes. Proceed to [Step 3: Preparing Storage for RAC on New Nodes](#) to prepare storage for RAC on the new nodes.

Step 3: Preparing Storage for RAC on New Nodes

To extend an existing RAC database to your new nodes, configure storage for the new nodes so that the storage is the same as on the existing nodes. For example, the Oracle Cluster Registry (OCR) and the voting disk must be accessible by the new nodes using the same path as the other nodes use. In addition, the OCR and voting disk devices must have the same permissions on the new node as those on the existing nodes. Prepare the same type of storage on the new nodes as you are using on the other nodes in the RAC environment that you want to extend as follows:

- Automatic Storage Management (ASM)
If you are using ASM, then make sure that the new nodes can access the ASM disks with the same permissions as the existing nodes.
- Oracle Cluster File System (OCFS)
If you are using OCFS, then make sure that the new nodes can access the cluster file systems in the same way that the other nodes access them.
- Vendor Cluster File Systems
If your cluster database uses vendor cluster file systems, then configure the new nodes to use the vendor cluster file systems. Refer to the vendor clusterware documentation for the pre-installation steps for your platform.
- Raw Device Storage
If your cluster database uses raw devices, then prepare the new raw devices by following the procedures described in the following section.

Raw Device Storage Preparation for New Nodes

To prepare raw device storage on the new nodes, you need at least two new disk partitions to accommodate the redo logs for each new instance. Make these disk partitions the same size as the redo log partitions that you configured for the instances of existing nodes. Also create an additional logical partition for the undo tablespace for automatic undo management.

On operating systems, you can create symbolic links to your raw devices. Optionally, on all platforms you can create a raw device mapping file and set the `DBCA_RAW_CONFIG` environment variable so that it points to the raw device mapping file.

Configure Raw Storage on UNIX-Based Systems

Use your vendor-supplied tools to configure the required raw storage.

Configure Raw Partitions on Windows-Based Systems

Perform the following steps from one of the existing nodes of the cluster:

1. Create or identify an extended partition.
2. Click inside a unallocated part of the extended partition.
3. Select **Create** from the Partition menu. A dialog box appears in which you should enter the size of the partition. Ensure you use the same sizes as those you used on your existing nodes.
4. Click the newly created partition and select **Assign Drive Letter** from the Tool menu.
5. Select **Don't Assign Drive Letter**, and click **OK**.
6. Repeat steps 2 through 5 for the second and any additional partitions.
7. Select **Commit Changes Now** from the Partition menu to save the new partition information.
8. Create symbolic links so that the existing nodes and new nodes can recognize the new partitions you just created and the new nodes can recognize the pre-existing symbolic links to logical drives by following these steps:
 - a. Start the Object Link Manager (OLM) by entering the following command from the `CRS home\bin` directory on one of the existing nodes:


```
GUIOracleOBJManager
```
 - b. The OLM starts and automatically detects the symbolic links to the logical drives and displays them in the graphical user interface of OLM.
 - c. Recall the disk and partition numbers for the partitions that you created in the previous section. Look for the disk and partition numbers in the OLM page and perform the following tasks:
 - Right-click next to the box under the New Link column and enter the link name for the first partition.
 - Repeat the previous step for the second and any additional partitions.
For example, if your RAC database name is `db` and it consists of two instances running on two nodes and you are adding a third instance on the third node, then your link names for your redo logs should be `db_redo3_1`, `db_redo3_2`, and so on.
 - To enable automatic undo management for the instance of a new node, enter the link name for the logical partition for the undo tablespace that you created in the previous section. For example, if your RAC database name is `db` and if it has two instances running on two nodes and you are adding a third instance on a third node, then your link name for the undo tablespace should be `db_undotbs3`.
 - Select **Commit** from the Options menu. This creates the new links on the current node.
 - Select **Sync Nodes** from the Options menu. This makes the new links visible to all of the nodes in the cluster, including the new nodes.
 - Select **Exit** from the Options menu to exit Object Link Manager.

After completing the procedures in this section, you have configured your cluster storage so that the new nodes can access the Oracle software. Additionally, the existing nodes can access the new nodes and instances. Use Oracle Universal Installer as described in the procedures in Step 4 to configure the new nodes at the RAC database layer.

Step 4: Adding Nodes at the Oracle RAC Database Layer

To add nodes at the Oracle RAC database layer, run Oracle Universal Installer in add node mode to configure your new nodes. If you have multiple Oracle homes, then perform the following steps for each Oracle home that you want to include on the new nodes:

1. On an existing node from the `$ORACLE_HOME/oui/bin` directory on UNIX-based systems, run the `addNode.sh` script. From the `%ORACLE_HOME%\oui\bin` on Windows-based systems, run the `addNode.bat` script. This starts Oracle Universal Installer in the add node mode and displays the Oracle Universal Installer Welcome page. Click **Next** on the Welcome page and Oracle Universal Installer displays the Specify Cluster Nodes for Node Addition page.
2. The Specify Cluster Nodes for Node Addition page has a table showing the existing nodes associated with the Oracle home from which you launched Oracle Universal Installer. A node selection table appears on the bottom of this page showing the nodes that are available for addition. Select the nodes that you want to add and click **Next**.
3. Oracle Universal Installer verifies connectivity and performs availability checks on both the existing nodes and on the nodes that you want to add. Some of checks performed determine whether:
 - The nodes are up
 - The nodes are accessible by way of the network
 - The user has write permission to create the Oracle home on the new nodes
 - The user has write permission to the Oracle Universal Installer inventory in the `oraInventory` directory on UNIX or the `Inventory` directory on Windows on the existing nodes and on the new nodes
4. If the new nodes do not have an inventory set up, then on UNIX-based systems Oracle Universal Installer displays a dialog box asking you to run the `oraInstRoot.sh` script on the new nodes. On Windows-based systems Oracle Universal Installer automatically updates the Registry entries for the inventory location. If any of the other checks fail, then fix the problem and proceed or deselect the node that has the error and proceed. You cannot deselect existing nodes. You must correct problems on the existing nodes before proceeding with node addition. If all the checks succeed then Oracle Universal Installer displays the Node Addition Summary page.
5. The Node Addition Summary page has the following information about the products that are installed in the Oracle home that you are going to extend to the new nodes:
 - The source for the add node process, which in this case is the Oracle home
 - The existing nodes and new nodes
 - The new nodes that you selected
 - The required and available space on the new nodes

- The installed products listing all the products that are already installed in the existing Oracle home

Click **Finish** and Oracle Universal Installer displays the Cluster Node Addition Progress page.

6. The Cluster Node Addition Progress page shows the status of the cluster node addition process. The table on this page has two columns showing the phase of the node addition process and the phase's status according to the following platform-specific content.

On UNIX-based systems, the Cluster Node Addition Progress page shows the following four Oracle Universal Installer phases:

- **Instantiate Root Scripts:** The `root.sh` script in the Oracle home is instantiated by copying it from the local node
- **Copy the Oracle Home to the New Nodes:** The entire Oracle home from the local node to the new nodes is copied unless the Oracle home is on a cluster file system
- **Run `root.sh`:** The dialog box is displayed prompting you to run `root.sh` on the new nodes
- **Save Cluster Inventory:** The node list, associated with the Oracle home and its inventory, is updated

On Windows-based systems, the Cluster Node Addition Progress shows the following three Oracle Universal Installer phases:

- **Copy the Oracle Home To New Nodes:** The entire Oracle home is copied to the new nodes unless the Oracle home is on a cluster file system
- **Performs Oracle Home Setup:** The Registry entries are updated for the new nodes, services are created, and folder entries are created
- **Save Cluster Inventory:** The node list, associated with the Oracle home and its inventory, is updated

For all platforms, the Status column of the Cluster Node Addition Progress page displays Succeeded if the phase completes, In Progress if the phase is in progress, and Suspended when the phase is pending execution. After Oracle Universal Installer displays the End of Node Addition page, click **Exit** to end the Oracle Universal Installer session.

7. On UNIX-based systems only, run the `root.sh` script.
8. Run the Virtual IP Configuration Assistant (VIPCA) utility from the `bin` subdirectory of the Oracle home using the `-nodelist` option with the following syntax that identifies the complete set of nodes that are now part of your RAC database beginning with *Node1* and ending with *NodeN*:

```
vipca -nodelist Node1,Node2,Node3,...NodeN
```

Note: You must run the VIPCA utility as `root` user on UNIX-based systems, and as a user with Administrative privileges on Windows-based systems.

9. If the private interconnect interface names on the new nodes are not the same as the interconnect names that are on the existing nodes, then change the private interconnect configuration for the new nodes as described in this step, otherwise,

proceed to step 10. Change the configuration by executing the `oifcfg` utility with the `setif` option from the bin directory of the Oracle home using the following syntax where *subnet* is the subnet for the private interconnect of the RAC databases to which you are adding nodes. Specify the `-n nodename` option to enter node-specific configuration information for the new nodes. The syntax for `oifcfg` commands are as follows:

```
oifcfg iflist
```

```
oifcfg setif {-node nodename | -global} {if_name/subnet:if_type}...
```

```
oifcfg getif [-node nodename | -global] [ -if if_name[/subnet] [-type if_type]  
]
```

```
oifcfg delif [-node nodename | -global] [if_name[/subnet]]
```

```
oifcfg [-help]
```

A Cluster Ready Services (CRS) installation issues the `oifcfg` command as in the following example:

```
oifcfg setif -global eth0/146.56.76.0:public eth1/192.0.0.0:cluster_  
interconnect
```

This sets both networks to global. Therefore, you do not need to run the `oifcfg` command manually after you add a node unless the network interfaces differ.

10. Add a listener to the new node by running the Net Configuration Assistant (NetCA).

After completing the procedures in the previous section, you have defined the new nodes at the cluster database layer. You can now add database instances to the new nodes as described in Step 5.

Step 5: Adding Database Instances to New Nodes

Run the following procedures for each new node to add instances:

1. Start the Database Configuration Assistant (DBCA) by entering `dbca` at the system prompt from the bin directory in the `$ORACLE_HOME` on UNIX. On Windows-based systems, select **Start, Programs, Oracle - HOME_NAME, Configuration and Migration Tools, Database Configuration Assistant**.

The DBCA displays the Welcome page for RAC. Click **Help** on any DBCA page for additional information.
2. Select **Real Application Clusters** database, click **Next**, and the DBCA displays the Operations page.
3. Select **Instance Management**, click **Next**, and the DBCA displays the Instance Management page.
4. Select **Add Instance** and click **Next**. The DBCA displays the List of Cluster Databases page that shows the databases and their current status, such as **ACTIVE**, or **INACTIVE**.
5. From the List of Cluster Databases page, select the active RAC database to which you want to add an instance. If your user ID is not operating-system authenticated, then the DBCA prompts you for a user ID and password for a database user that has SYSDBA privileges. If the DBCA prompts you, then enter a valid user ID and password and click **Next**. The DBCA displays the List of Cluster

Database Instances page showing the names of the existing instances for the RAC database that you selected.

6. Click **Next** to add a new instance and the DBCA displays the Adding an Instance page.
7. On the Adding an Instance page, enter the instance name in the field at the top of this page if the instance name that the DBCA provides does not match your existing instance name sequence. Then select the new node name from the list, click **Enter the services information for the new node's instance**, click **Next**, and the DBCA displays the Services Page.
8. Enter the services information for the instance of the new node, click **Next**, and the DBCA displays the Instance Storage page.
9. If you are using raw devices or raw partitions, then on the Instance Storage page select the Tablespaces folder and expand it. Then select the undo tablespace storage object and a dialog box appears on the right-hand side. Change the default data file name to the raw device name for the tablespace.
10. If you are using raw devices or raw partitions or if you want to change the default redo log group file name, then on the Instance Storage page select and expand the Redo Log Groups folder. For each redo log group number that you select, the DBCA displays another dialog box.
 - For UNIX-based systems, enter the raw device name.
 - On Windows-based systems, enter the symbolic link name.
11. If you are using a cluster file system, then click **Finish** on the Instance Storage page. If you are using raw devices on UNIX-based systems or disk partitions on Windows-based systems, then repeat step 10 for all of the other redo log groups, click **Finish**, and the DBCA displays a Summary dialog box.
12. Review the information on the Summary dialog box and click **OK**. Click **Cancel** to end the instance addition operation. The DBCA displays a progress dialog box showing the DBCA performing the instance addition operation. When the DBCA completes the instance addition operation, the DBCA displays a dialog box asking whether you want to perform another operation.
13. Click **No** and exit the DBCA, or click **Yes** to perform another operation. If you click **Yes**, then the DBCA displays the Operations page.

After you have completed the procedures in this section, the DBCA has successfully added the new instance to the new node and completed the following steps:

- Created and started an ASM instance on each new node if the existing instances were using ASM
- Created a new database instance on each new node
- For Windows-based systems, created and started the required services
- Created and configured high-availability components
- Configured and started node applications for the GSD, [Oracle Net Services](#) listener, and Enterprise Manager agent
- Created the Oracle Net configuration
- Started the new instance
- Created and started services if you entered services information on the Services Configuration page

After adding the instances to the new nodes using the steps described in this section, perform any needed service configuration procedures.

Updating Path Environment Variables on New Nodes on Windows-Based Systems

When you add a new node, you must update the Path environment variable on each new node on Windows-based systems.

1. Navigate to **Start, Settings, Control Panel, System, Advanced, Environment Variables**.
2. In the System variables dialog box, select the Path variable and ensure that the value for the Path variable contains Oracle home\BIN, where Oracle home is your new Oracle home. If the variable does not contain this value, then click **Edit** and add this value to the start of the path variable definition in the Edit System Variable dialog box. Click **OK** in the Environment Variables page, then click **OK** in the System Properties page, and then close the Control Panel.
3. Click **OK** in the Environment Variables page, then click **OK** in the System Properties page, and then close the Control Panel.

Connecting to iSQL*Plus after Adding a Node on Windows-Based Platforms

After you add a node to a RAC database on Windows platforms, you must manually create the following directories in the ORACLE_BASE\ORACLE_HOME\oc4j\j2ee\isqlplus directory before you can run iSQL*Plus on the new node:

- connectors
- log
- persistence
- tldcache

After you create these directories, you can start iSQL*Plus either by running `isqlplusctl start` at the command prompt or by starting iSQL*Plus from the Windows Control Panel Services tool. If you try to connect to the iSQL*Plus URL without creating these directories, then you will not be able to connect.

Adding Nodes that Already Have Clusterware and Oracle Software to a Cluster

To add nodes to a cluster that already have clusterware and Oracle software installed on them, you must configure the new nodes with the Oracle software that is on the existing nodes of the cluster. To do this, you must run two versions of an Oracle Universal Installer process. One version is for the clusterware and other one for the database layer as described in the following procedures:

1. Add new nodes at the Oracle clusterware layer by running Oracle Universal Installer from the CRS home on an existing node according to the following platform-specific procedures.
 - On UNIX run the following command:

```
CRS home/oui/bin/addNode.sh -noCopy
```
 - On Windows run the following command:

```
CRS home\oui\bin\addNode.bat -noCopy
```

2. Add new nodes at the Oracle software layer by running Oracle Universal Installer from the Oracle home as follows:

- On UNIX, run the following command:

```
$ORACLE_HOME/oui/bin/addNode.sh -noCopy
```

- On Windows, run the following command:

```
%ORACLE_HOME%\oui\bin\addNode.bat -noCopy
```

In the `-noCopy` mode, Oracle Universal Installer performs all add node operations except for the copying of software to the new nodes.

Note: Oracle recommends that you back up your voting disk and OCR files after you complete the node addition process.

Adding a Node on a Shared Oracle Home

If you are using Oracle Universal Installer to add a node on a shared Oracle home, then an error similar to the following may appear:

```
Alert: The following file(s) have been modified on the disk:
y:\oracle\rac\inventory\ContentsXML\comps.xml y:\oracle\rac\inventory
\ContentsXML\libs.xml
Proceeding with the installation may corrupt some important data. You should
stop this session and restart OUI. Do you want to stop this session now?
```

Ignore this error and click **No** and continue.

Deleting Instances from Real Application Clusters Databases

The procedures in this section explain how to use the DBCA to delete an instance from a RAC database. To delete an instance:

1. Start the DBCA on a node other than the node that hosts the instance that you want to delete. On the DBCA Welcome page select **Oracle Real Application Clusters Database**, click **Next**, and the DBCA displays the Operations page.
2. On the DBCA Operations page, select Instance Management, click **Next**, and the DBCA displays the Instance Management page.
3. On the Instance Management page, Select **Delete Instance**, click **Next**, and the DBCA displays the List of Cluster Databases page.
4. Select a RAC database from which to delete an instance. If your user ID is not operating-system authenticated, then the DBCA also prompts you for a user ID and password for a database user that has SYSDBA privileges. If the DBCA prompts you for this, then enter a valid user ID and password. Click **Next** and the DBCA displays the List of Cluster Database Instances page. The List of Cluster Database Instances page shows the instances associated with the RAC database that you selected and the status of each instance.
5. Select a remote instance to delete and click **Finish**.
6. If you have services assigned to this instance, then the DBCA Services Management page appears. Use this feature to reassign services from this instance to other instances in the cluster database.

7. Review the information about the instance deletion operation on the Summary page and click **OK**. Otherwise, click **Cancel** to cancel the instance deletion operation. If you click **OK**, then the DBCA displays a Confirmation dialog box.
8. Click **OK** on the Confirmation dialog box to proceed with the instance deletion operation and the DBCA displays a progress dialog box showing that the DBCA is performing the instance deletion operation. During this operation, the DBCA removes the instance and the Oracle Net configuration of the instance. When the DBCA completes this operation, the DBCA displays a dialog box asking whether you want to perform another operation.
9. Click **No** and exit the DBCA or click **Yes** to perform another operation. If you click **Yes**, then the DBCA displays the Operations page.

At this point, you have accomplished the following:

- Deregistered the selected instance from its associated Oracle Net Services listeners
- Deleted the selected database instance from the instance's configured node
- Deleted the selected instance's services for Windows-based systems
- Removed the Oracle Net configuration
- Deleted the Oracle Flexible Architecture directory structure from the instance's configured node.

Deleting Nodes from Oracle Clusters on UNIX-Based Systems

Use the following procedures to delete nodes from Oracle clusters on UNIX-based systems:

1. If there are instances on the node that you want to delete, then run the procedures in the [Deleting Instances from Real Application Clusters Databases](#) before executing these procedures. If you are deleting more than one node, then delete the instances from all the nodes that you are going to delete.
2. If you use ASM, then perform the procedures in the following section, [ASM Instance Clean-Up Procedures for Node Deletion](#).
3. If this is the Oracle home from which the node-specific listener named `LISTENER_nodename` runs, then use NetCA to remove this listener and its CRS resources. If necessary, re-create this listener in another home.
4. After you have deleted the instances from the nodes that you want to delete, delete the node applications for each node by running the following command from the Oracle home (not the CRS home) where `node1`, `node2` are the nodes that you are removing from your cluster:

```
rootdeletenode.sh node1,node2
```

5. On the same node that you are deleting, run the command `runInstaller -updateNodeList ORACLE_HOME=Home location CLUSTER_NODES=node1,node2,...nodeN` where `node1` through `nodeN` is a comma-delimited list of nodes that are remaining in the cluster. This list must exclude the nodes that you are deleting. The `runInstaller` command is located in the directory `$ORACLE_HOME/oui/bin`. Executing this command does not launch an installer GUI.
6. If you are not using a cluster file system for the Oracle home, then on the node that you are deleting, remove the Oracle database software by executing the `rm` command. *Make sure that you are in the correct Oracle home of the node that you are*

deleting when you run the `rm` command. Run this command on all the nodes that you are deleting.

7. On the node that you are deleting, run the command `CRS Home/install/rootdelete.sh` to disable the CRS applications that are on the node. Only run this command once and use the `nosharedhome` argument if you are using a local file system. The default for this command is `sharedhome` which prevents you from updating the permissions of local files such that they can be removed by the `oracle` user.

If the `ocr.loc` file is on a shared file system, then run the command `CRS home/install/rootdelete.sh remote sharedvar`. If the `ocr.loc` file is not on a shared file system, then run the `CRS home/install/rootdelete.sh remote nosharedvar` command. If you are deleting more than one node from your cluster, then repeat this step on each node that you are deleting.
8. Run `CRS Home/install/rootdeletenode.sh` on any remaining node in the cluster to delete the nodes from the Oracle cluster and to update the Oracle Cluster Registry (OCR). If you are deleting multiple nodes, then run the command `CRS Home/install/rootdeletenode.sh node1,node1-number,node2,node2-number,... nodeN,nodeN-number` where `node1` through `nodeN` is a list of the nodes that you want to delete, and `node1-number` through `nodeN-number` represents the node number. To determine the node number of any node, run the command `CRS Home/bin/olsnodes -n`. To delete only one node, enter the node name and number of the node that you want to delete.
9. `<CRS home>/install/rootdeletenode.sh node1,node1-number`
10. On the same node and as the `oracle` user, run the command `CRS home/oui/bin/runInstaller -updateNodeList ORACLE_HOME=CRS home CLUSTER_NODES=node1,node2,... nodeN` where `node1` through `nodeN` is a comma-delimited list of nodes that are remaining in the cluster.
11. If you are not using a cluster file system, then on the node that you are deleting, remove the Oracle CRS software by executing the `rm` command. Make sure that you run the `rm` command from the correct Oracle CRS home. Run the `rm` command on every node that you are deleting.

ASM Instance Clean-Up Procedures for Node Deletion

Perform the following procedure to remove the ASM instances as follows:

1. If this is the Oracle home which from which the ASM instance runs, then remove the ASM configuration by completing the following steps. Run the command `srvctl stop asm -n node` for all nodes on which this Oracle home exists. Run the command `srvctl remove asm -n node` for all nodes on which this Oracle home exists.
2. If you are using a cluster file system for your ASM Oracle home, then run the following commands on the local node:

```
rm -r $ORACLE_BASE/admin/+ASM
rm -f $ORACLE_HOME/dbs/*ASM*
```

3. If you are not using a cluster file system for your ASM Oracle home, then run the `rm` or `delete` commands mentioned in the previous step on each node on which the Oracle home exists.
4. Remove `oratab` entries beginning with `+ASM`.

Note: Oracle recommends that you back up your voting disk and OCR files after you complete the node deletion process.

Deleting Nodes from Oracle Clusters on Windows-Based Platforms

The following procedures are used to delete nodes from Oracle clusters on Windows-based platforms.

Perform the following steps on a node other than the node you want to delete:

1. Use the Database Configuration Assistant (DBCA) to delete the instance.
2. Use NetCA to delete the listener.
3. If the node that you are deleting has an ASM instance, then delete the ASM instance using the `srvctl stop asm` and `srvctl remove asm` commands.
4. Run the command `srvctl stop nodeapps -n nodename of the node to be deleted` to stop the node applications.
5. Run the command `srvctl remove nodeapps -n nodename of the node to be deleted` to remove the node applications.
6. Stop `isqlplus` if it is running.
7. Run the command `setup.exe -updateNodeList ORACLE_HOME=Oracle_home ORACLE_HOME_NAME=Oracle_home_name CLUSTER_NODES=remaining nodes where remaining nodes is a list of the nodes that are to remain part of the cluster.`

Perform the following steps on the deleted RAC node:

1. Run the command `setup.exe -updateNodeList -local -noClusterEnabled ORACLE_HOME=Oracle_home ORACLE_HOME_NAME=Oracle_home_name CLUSTER_NODES=" "`. Note that you do not need a value for " " after the `CLUSTER_NODES=` entry in this command. If you delete more than one node, then you must run this command on every deleted node to remove the Oracle home if you have a non-shared Oracle home (non-cluster file system) installation.
2. On the same node, delete the Windows Registry entries and ASM services using `Oradim`.
3. From the deleted RAC node, run the command `Oracle_home\oui\bin\setup.exe` to start Oracle Universal Installer. Select **Deinstall Products** and select the Oracle home that you want to de-install.
4. Then to delete the CRS node, from a remaining node, run the command `crssetup del -nn node_name of the deleted node, node number`
5. Then run the command `setup.exe -updateNodeList ORACLE_HOME=CRS home ORACLE_HOME_NAME=CRS home name CLUSTER_NODES=remaining nodes where remaining nodes is a list of the nodes that are to remain in the cluster.`
6. Then on the deleted CRS node, run the command `setup.exe -updateNodeList -local -noClusterEnabled ORACLE_HOME=CRS home ORACLE_HOME_NAME=CRS home name CLUSTER_NODES=" "`
7. Remove the Oracle home manually from the new node if the home is not shared and then manually remove the `HKLM/software/Oracle` registry keys and the Oracle services.

8. After adding or deleting nodes from your Oracle Database 10g with RAC environment, and after you are sure that your system is functioning properly, make a backup of the contents of the voting disk using the `dd.exe` utility. The `dd.exe` utility is part of the MKS toolkit.

ASM Instance Cleanup Procedures after Node Deletion on Windows-Based Platforms

The procedure of node deletion requires the following additional steps on Windows-based systems to remove the ASM instances:

1. If this is the Oracle home from which the node-specific listener named `LISTENER_nodename` runs, then use NetCA to remove this listener and its CRS resources. If necessary, re-create this listener in another home.
2. If this is the Oracle home from which the ASM instance runs, then remove the ASM configuration by running the following command for all nodes on which this Oracle home exists:

```
srvctl stop asm -n node
```

Then run the following command for the nodes that you are removing:

```
srvctl remove asm -n node
```

3. If you are using a cluster file system for your ASM Oracle home, then run the following commands on the local node:

```
rd -s -q %ORACLE_BASE%\admin\+ASM
delete %ORACLE_HOME%\database\*ASM*
```

4. If you are not using a cluster file system for your ASM Oracle home, then run the `delete` command mentioned in the previous step on each node on which the Oracle home exists.
5. Run the following command on each node that has an ASM instance:

```
oradim -delete -asmsid +ASMnode_number
```

Note: Oracle recommends that you back up your voting disk and OCR files after you complete the node deletion process.

Adding or Deleting Nodes from Oracle Collaboration Suite Database

This section describes how to remove nodes from Oracle Collaboration Suite Applications. The steps are as follows:

- [Step 1: Modify the RAC Database Connect String in Oracle Internet Directory](#)
- [Step 2: Modify the Crawler's Connect String Through the Search Admin Application](#)
- [Step 3: Bounce the Oracle Collaboration Suite Applications Tier Processes](#)

Step 1: Modify the RAC Database Connect String in Oracle Internet Directory

The steps to modify the RAC database connect string in Oracle Internet Directory to reflect the new node list are as follows:

1. On the infrastructure machine, open `$ORACLE_HOME/bin/oidadmin` and delete the `cn=OracleContext, cn=<RAC database name>` entry under Entry Management. You must delete its subentries one by one first.
2. On the RAC database system, populate `$ORACLE_HOME/install/OCSdbSchemaReg.ini` with the correct values after addition or deletion. Then, run `OCSdbSchemaReg.sh -f OCSdbSchemaReg.ini`. This will put the new correct string in Oracle Internet Directory.

You can use your original `OCSdbSchemaReg.ini` file but you must modify the line named `our $hostList` appropriately to reflect your new node configuration before running this step. For example, before any changes are done, the node list in `OCSdbSchemaReg.ini` is as follows:

```
our $hostList =  
"rac1vip1.us.oracle.com:1521,rac2vip1.us.oracle.com:1521,rac3vip1.us.oracle.com:  
:1521";
```

After adding node `rac4vip1.us.oracle.com`, the node list in `OCSdbSchemaReg.ini` is as follows:

```
our $hostList =  
"rac1vip1.us.oracle.com:1521,rac2vip1.us.oracle.com:1521,rac3vip1.us.oracle.com:  
:1521,rac4vip1.us.oracle.com:1521";
```

After deleting node `rac3vip1.us.oracle.com`, the node list in `OCSdbSchemaReg.ini` is as follows:

```
our $hostList = "rac1vip1.us.oracle.com:1521,rac2vip1.us.oracle.com:1521";
```

3. Next, run `OCSdbSchemaReg.sh -f OCSdbSchemaReg.ini`. This will put the new correct string in Oracle Internet Directory.

Step 2: Modify the Crawler's Connect String Through the Search Admin Application

When RAC uses the Cluster File System (CFS), the Ultra Search crawler can be launched from any of the RAC nodes, as long as at least one RAC node is up and running. When RAC is not using CFS, the Ultra Search crawler always runs on a specified node. If this node stops operating, then you must run the `wk0reconfig.sql` script to move Ultra Search to another RAC node. In the `wk0reconfig.sql` script, `instance_name` is the name of the RAC instance that Ultra Search uses for crawling. After connecting to the database, to get the name of the current instance, run the following command:

```
SELECT instance_name FROM v$instance
```

`connect_url` is the JDBC connection string that guarantees a connection only to the specified instance. An example is as follows:

```
(DESCRIPTION=  
  (ADDRESS_LIST=  
    (ADDRESS= (PROTOCOL=TCP)  
              (HOST=<nodename>  
              (PORT=<listener_port>)))  
  )  
  (CONNECT_DATA= (SERVICE_NAME=<service_name>)))
```

Step 3: Bounce the Oracle Collaboration Suite Applications Tier Processes

From the Oracle Collaboration Suite Application tier, run the following commands.

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
```

```
$ORACLE_HOME/ocas/bin/ocasctl -stopall  
$ORACLE_HOME/opmn/bin/opmnctl startall  
$ORACLE_HOME /ocas/bin/ocasctl -start -t ochecklet -p 8020 -n 1  
$ORACLE_HOME /ocasctl -start -t ocas -p 8010 -n 5
```

The default ports are 8010, 8020. The valid range is 8010-8020.

Removing Nodes from Oracle Collaboration Suite Applications

The steps for removing nodes from multiple Oracle Collaboration Suite Applications tiers that are front ended by a load balancer are as follows:

1. Shutdown all Oracle Collaboration Suite Applications on the node of the Oracle Collaboration Suite Applications tier, that has to be removed, as follows:

```
opmnctl stopall
```

After shutting down Oracle Collaboration Suite Applications, the load balancer routes all requests to the active nodes assuming that the load balancer monitors have been setup correctly.

2. Remove the node the load balancer virtual server node pool.

Configuring Manual Cold Failover for Oracle Calendar Server

In an Oracle Collaboration Suite high-availability environment, Oracle Calendar Server can be setup in an active-passive configuration which is also known as cold failover cluster configuration.

In an Oracle Calendar Server cold failover cluster configuration, in the event of a failure of an active node, if you want an automated cold failover for Oracle Calendar Server, then you must use vendor clusterware. Manual cold failover is done when the vendor clusterware is not installed. The steps for the manual cold failover configuration are as follows:

1. Ensure that the Calendar Server virtual IP address is inaccessible by pinging it. If it is still accessible, then it may not be necessary to execute a cold failover. Validate that the system is truly down and also that it requires a cold failover before proceeding. If it is necessary and the calendar server virtual IP is still accessible, then bring down the virtual IP address on the node where it is active.
2. Mount the shared storage to the destination node which is the original passive node.
3. Bring up the virtual IP address on the destination node.
4. Mount the Oracle Calendar Server shared storage containing the ORACLE_HOME of Oracle Calendar Server on the destination node.
5. Start the Oracle Calendar Server.

Starting and Stopping Oracle Collaboration Suite in a High-Availability Environment

This section describes how to stop and start Oracle Collaboration Suite in a high-availability environment. Set up the environment for the correct ORACLE_HOME when you log on to each tier before the stop and start processes. On Infrastructure tiers, also set the ORACLE_SID.

See Also: [Chapter 2, "Starting and Stopping Oracle Collaboration Suite"](#) for detailed instructions for starting and stopping non-high-availability environments.

Stopping Oracle Collaboration Suite

The steps for stopping Oracle Collaboration Suite in a high-availability environment are as follows:

1. Log on to each Applications tier node and run the following commands:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/ocas/bin/ocasctl -stopall
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/bin/lsnrctl stop listener_es
```

2. For the Oracle Calendar Server node, run the following commands:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/bin/emctl stop iasconsole
```

3. For each Identity Management Infrastructure tier, run the following commands:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/bin/emctl stop iasconsole
```

4. For each RAC database tier, run the following command:

```
emctl stop dbconsole
```

From any RAC database node, run the command:

```
ORACLE_HOME/bin/srvctl stop database -d $dbname
ORACLE_HOME/bin/srvctl stop nodeapps -n $nodename
```

In the preceding commands, \$dbname is the name of the database and \$nodename is the machine name.

Starting Oracle Collaboration Suite

The steps for starting Oracle Collaboration Suite in a high-availability environment are as follows:

1. In each RAC database tier, run the following command:

```
emctl start dbconsole
```

From any RAC database node, run the command:

```
ORACLE_HOME/bin/srvctl start database -d $dbname
ORACLE_HOME/bin/srvctl start nodeapps -n $nodename
```

In the preceding commands, \$dbname is the name of the database and \$nodename is the machine name.

2. Log on to each Identity Management Infrastructure tier and run the following commands:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/bin/emctl stop iasconsole
```

In a Distributed Identity Management Architecture, ensure that the Oracle Internet Directory tier is started before the OracleAS Single Sign-On tier.

3. Oracle Calendar Server is set up separately from the Applications tier in its own `ORACLE_HOME`. For the Oracle Calendar Server node, ensure that the virtual IP is up and run the following commands:

```
ORACLE_HOME/opmn/bin/opmnctl startall  
ORACLE_HOME/bin/emctl start iasconsole
```

4. For each of the Applications tier instances, run the following commands by logging in as root and also ensure that port 25 is not in use:

```
ORACLE_HOME/bin/tnslsnr listener_es -user $uid -group $gid  
ORACLE_HOME/opmn/bin/opmnctl startall  
ORACLE_HOME/ocas/bin/ocasctl -start -t ochecklet -p 8020 -n 1  
ORACLE_HOME/ocasctl -start -t ocas -p 8010 -n 5  
ORACLE_HOME/bin/emctl start iasconsole
```

Note: This step assumes that you are using the default port (port 25) for the Oracle Mail listener. On UNIX systems, port 25 is a privileged port, so you must log in as root. If you have installed the listener on a non-privileged port, you do not need to log in as root. On Windows systems, you do not need to log in as root.

Changing Oracle Collaboration Suite Network Configurations

This chapter provides procedures for changing the network configuration of an Oracle Collaboration Suite host.

This chapter contains the following sections:

- [Introduction to Changing Oracle Collaboration Suite Ports](#)
- [Changing Applications Tier Ports](#)
- [Changing Infrastructure Ports](#)
- [Changing a Hostname, Domain Name, or IP Address](#)

Introduction to Changing Oracle Collaboration Suite Ports

Many Oracle Collaboration Suite components and services use ports. As an administrator, it is important to know the port numbers used by these services, and to ensure that the same port number is not used by two services on your host.

From time to time, you may need to change the port number used by a component of Oracle Collaboration Suite. Most commonly, this is because you have another application or service that needs to use a port which is already in use by Oracle Collaboration Suite.

Most port numbers are assigned during installation. Every Oracle Collaboration Suite component and service has an allotted port range, which is the set of port numbers Oracle Collaboration Suite attempts to use when assigning a port. Oracle Collaboration Suite starts with the lowest number in the range and performs the following checks:

- Is the port used by another Oracle Collaboration Suite installation on the host?
The installation may be up or down at the time; Oracle Collaboration Suite can still detect if the port is used.
- Is the port used by a process that is currently running?
This could be any process on the host, even a non-Oracle Collaboration Suite process.

If the answer to any of the preceding questions is yes, Oracle Collaboration Suite moves to the next highest port in the allotted port range and continues checking until it finds a free port.

You can override this behavior for some ports, and specify a port number assignment during installation. You can also specify a port range. To do this, you edit a template

file called `staticports.ini`, and launch Oracle Universal Installer with special options. Alternatively, you can specify port ranges directly in the Oracle Universal Installer screens.

See Also: [Appendix A, "Default Port Numbers and Ranges"](#) for a complete list of allotted port ranges.

Refer to "2.5.4 Using Custom Ports (The Static Ports Feature)" in *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows* for directions on overriding port assignments during installation with `staticports.ini`.

Viewing Port Numbers

You can view port numbers on the Oracle Collaboration Suite Control Console Ports page. Click the **Ports** tab on the Oracle Collaboration Suite home page. The Ports page displays the current port numbers and is updated any time you change a port number. For selected components, it also provides links to pages that allow you to change port numbers.

Note: Immediately after installation, you can view port number assignments in:

(UNIX) `ORACLE_HOME/install/portlist.ini`
(Windows) `ORACLE_HOME\install\portlist.ini`

This file is a static file generated during installation. If you change a port number, it is not updated in this file, so you can only rely on this file immediately after installation.

Changing Applications Tier Ports

This section provides instructions for changing port numbers in Applications tier instances. The instructions explain how to change the port number, and update any other components that might be affected.

See Also: ■ [Appendix A, "Default Port Numbers and Ranges"](#) for more information about Oracle Collaboration Suite port numbers

- ["Changing the Oracle Content Services Port Number"](#) in Chapter 2 of *Oracle Content Services Administrator's Guide*

Note: You can change a port number to any number you want, as long as it is an unused port. You do not have to use a port in the allotted port range for the component.

This section contains the following topics:

- [Changing Oracle Enterprise Manager Ports](#)
- [Changing OC4J Ports](#)
- [Changing the Oracle HTTP Server Listen Port](#)
- [Changing the OracleAS Web Cache Listen Port](#)

- [Changing the OracleAS Web Cache Administration Port](#)
- [Changing the OracleAS Web Cache Invalidation Port](#)
- [Changing the OracleAS Web Cache Statistics Port](#)
- [Changing the DCM Discovery Port](#)
- [Changing the Java Object Cache Port](#)
- [Changing the Log Loader Port](#)
- [Changing OPMN Ports \(ONS Local, Request, and Remote\)](#)
- [Changing the Oracle HTTP Server Diagnostic Port](#)
- [Changing the Port Tunneling Port](#)
- [Changing OracleAS Portal Ports](#)
- [Changing Oracle Mobile Collaboration Ports](#)
- [Specifying Ports for DMS-Monitored Services](#)

Changing Oracle Enterprise Manager Ports

After you have installed Oracle Collaboration Suite, you can change the following Oracle Enterprise Manager 10g ports associated with your Oracle Collaboration Suite instance:

- The Oracle Management Agent port, which the port used for communications with the Management Agent
- The Oracle Collaboration Suite Control Console port, which is the port used in the Oracle Collaboration Suite Control Console URL. For example:

`http://appserver1.acme.com:1156`

- The Oracle Application Server Containers for J2EE (OC4J) Remote Method Invocation (RMI) port used by the Oracle Collaboration Suite Control OC4J instance

From the Ports page of the Oracle Collaboration Suite home page, you can view the current port values for these components, as well as the valid port number range for each component.

See Also: ["Viewing Port Numbers"](#) on page 14-2

However, you cannot modify the Oracle Enterprise Manager 10g port numbers from the Ports page. Instead, use the following procedure to change the Oracle Collaboration Suite Control ports:

1. Change directory to the `bin` directory in the tier Oracle home.
2. Stop the Oracle Collaboration Suite Control.

On UNIX systems, enter the following command:

```
emctl stop iasconsole
```

On Windows systems, use the Services control panel to stop the Oracle Collaboration Suite Control service.

3. Use the following command to change one of the Oracle Enterprise Manager 10g port values:

```
emctl config {agent port | iasconsole {port | rmiport}} port_number
```

For example, to change the port used by the Oracle Collaboration Suite Control Console:

```
emctl config iasconsole port 1812
```

4. Start Oracle Collaboration Suite Control.

On UNIX systems, enter the following command:

```
emctl start iasconsole
```

On Windows systems, use the Services control panel to start the Oracle Collaboration Suite Control service.

[Table 14–1](#) describes the configuration changes that are automatically performed when you use the `emctl config` command to change an Oracle Collaboration Suite Control port number.

Table 14–1 Changing Oracle Collaboration Suite Control Ports Using the `emctl` Command Line

Port	Command Line	Actions Performed
Oracle Collaboration Suite Control port	<code>emctl config iasconsole port <i>port_number</i></code>	Changes the port value assigned to the StandaloneConsoleURL property in following configuration file: <code>ORACLE_HOME/sysman/emd/targets.xml</code> (UNIX) <code>ORACLE_HOME\sysman\emd\targets.xml</code> (Windows) Changes the port value assigned to the web-site tag in the following configuration file: <code>ORACLE_HOME/sysman/j2ee/config/emd-web-site.xml</code> (UNIX) <code>ORACLE_HOME\sysman\j2ee\config\emd-web-site.xml</code> (Windows)
Oracle Management Agent port	<code>emctl config agent port <i>port_number</i></code>	Changes the value assigned to the EMD_URL property in the following configuration file: <code>ORACLE_HOME/sysman/config/emd.properties</code> (UNIX) <code>ORACLE_HOME\sysman\config\emd.properties</code> (Windows)
OC4J Remote Method Invocation (RMI) port	<code>emctl config iasconsole rmiport <i>port_number</i></code>	Changes the port values in the following configuration files: <code>ORACLE_HOME/sysman/j2ee/config/rmi.xml</code> (UNIX) <code>ORACLE_HOME\sysman\j2ee\config\rmi.xml</code> (Windows) <code>ORACLE_HOME/bin/emctl.pl</code> (UNIX) <code>ORACLE_HOME\bin\emctl.pl</code> (Windows)

Changing OC4J Ports

This section describes how to change the following OC4J port numbers:

- AJP
- JMS
- RMI
- IIOP
- IIOPS1 (Server only)

- IIOPS2 (Server and client)

By default, Oracle Application Server does not use a single port number for each type of OC4J port. Instead, it uses a port range for each type of OC4J port and that range is the same for all OC4J instances on the host. During runtime, each OC4J instance on the host is assigned a single free port from the range. For example, if the default AJP range for every OC4J instance on a host is 3301-3400, then each OC4J instance is assigned a single free port from that range for its AJP port.

When changing an OC4J port number, you typically specify a new port range. The range may be a simple port range (3301-3400), a comma separated list of ports (3301, 3304, 3307), or a combination of both (3301-3380, 3383, 3390-3400). By default, the ranges contain 100 ports. If you specify a range that is too narrow, you may encounter problems when starting OC4J instances. The AJP and RMI port ranges are required; the others are optional.

You can change OC4J port ranges using the Oracle Collaboration Suite Control or manual steps:

- Using the Oracle Collaboration Suite Control:

1. Navigate to the Oracle Collaboration Suite home page.
2. Click **Ports**.
3. On the Ports page, locate the OC4J Instance and OC4J port range you would like to change. Click the icon in the Configure column.
4. On the Server Properties page, enter the new port range in the appropriate field. Click **Apply**.
5. On the Confirmation page, click **Yes**, you would like to restart now.

- Using manual steps:

1. Open the `opmn.xml` file:

```
(UNIX) ORACLE_HOME/opmn/conf/opmn.xml
(Windows) ORACLE_HOME\opmn\conf\opmn.xml
```

2. Locate the element for the OC4J instance that contains the port range you would like to change. For example, if you want to change a port range for the home instance, locate this element:

```
<process-type id="home" ...>
```

3. Within the OC4J instance element, there is a `port` element for each type of port. For example:

```
<port id="ajp" range="3301-3400"/>
<port id="rmi" range="3201-3300"/>
<port id="jms" range="3701-3800"/>
<port id="iiop" range="3401-3500"/>
<port id="iiops1" range="3501-3600"/>
<port id="iiops2" range="3601-3700"/>
```

4. Modify the range parameter for the port you would like to change, and then save the file.
5. Reload OPMN:

```
opmnctl reload
```

6. Start the OC4J instance that contains the port number you changed:

```
opmnctl startproc process-type=OC4J_instance
```

For example, if you changed a port number in the home instance:

```
opmnctl startproc process-type=home
```

7. Run the following command:

```
dcmctl updateConfig
```

Changing the Oracle HTTP Server Listen Port

To change the Oracle HTTP Server Listen ports, you change the Oracle HTTP Server Listen directive. When you do this, there are often dependencies that must also be set. For example, if you are using OracleAS Web Cache to improve the performance of your Oracle Collaboration Suite instance, you must modify the OracleAS Web Cache origin server settings whenever you modify the Oracle HTTP Server listen ports.

To be sure the port dependencies are modified correctly, you can use a single command to change the Oracle HTTP Server listen port. The `portconfig` command automatically modifies the necessary configuration files within the Oracle home and optionally restarts the required components within the Oracle home.

The following sections describe how to define the `portconfig` command and then use it to modify the Oracle HTTP Server HTTP or HTTPS port:

- [Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 on UNIX Systems](#)
- [Using the portconfig Command to Change the Oracle HTTP Server Listen Port](#)

Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 on UNIX Systems

Perform this step before you change the Oracle HTTP Server listen port if you are on a UNIX system and you are changing the listen port to a number less than 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Collaboration Suite). On UNIX systems, if you change the Oracle Collaboration Suite HTTPS listen port number to a privileged port (with a value less than 1024), you must enable Oracle Application Server to run as root, as follows:

1. Log in as root.
2. Run the following commands in the Applications tier Oracle home:

```
cd $ORACLE_HOME/Apache/Apache/bin
chown root .apachectl
chmod 6750 .apachectl
```

Using the portconfig Command to Change the Oracle HTTP Server Listen Port

Use the following procedure to change the Oracle HTTP Server HTTP or HTTPS port:

1. Set the `ORACLE_HOME` environment variable to the home directory of the instance where the Oracle HTTP Server resides.

For example:

```
setenv ORACLE_HOME /dev0/private/oracle/appserv1/ (UNIX)
set ORACLE_HOME=D:\oracle\appserv1\ (Windows)
```

2. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
3. Create an alias (on UNIX systems) or a DOSKEY macro (on Windows systems) to represent the `portconfig` command.

For example, to execute the command as an alias on UNIX systems, enter the following command on one line:

```
alias portconfig '$ORACLE_HOME/jdk/bin/java -cp
$ORACLE_HOME/sysman/webapps/emd/WEB-INF/lib/emd.jar:
$ORACLE_HOME/dcm/lib/dcm.jar: $ORACLE_HOME/sso/lib/ossoreg.jar
oracle.sysman.ias.sta.tools.PortConfigCmdLine \!'
```

Similarly, to execute the command as DOSKEY macro on Windows systems, enter the following at the DOS command line on one line:

```
doskey portconfig=%ORACLE_HOME%\jdk\bin\java -cp
%ORACLE_HOME%\sysman\webapps\emd\WEB-INF\lib\emd.jar;
%ORACLE_HOME%\dcm\lib\dcm.jar; %ORACLE_HOME%\sso\lib\ossoreg.jar
oracle.sysman.ias.sta.tools.PortConfigCmdLine $*
```

4. Use the newly created `portconfig` command on one line, as follows:

```
portconfig -oracleHome ORACLE_HOME -oldPort old_port
-newPort new_port [-sso -url http://applications_tier_host:port -user
http_server_admin_user [-site name_of_sso_partner_application]
[-admin mod_osso_admin_user] [-vHost path_to_mod_osso_configuration_file]]
[-webCache] {-start | -restart}
```

For example, on UNIX systems:

```
portconfig -oracleHome $ORACLE_HOME -oldPort 7777 -newPort 7778 -webCache
```

For example, on Windows systems:

```
portconfig -oracleHome %ORACLE_HOME% -oldPort 7777 -newPort 7778 -webCache
```

[Table 14-2](#) describes the arguments available when you use the `portconfig` command to automatically change the Oracle HTTP Server Listen port.

Table 14-2 Arguments for the `portconfig` Command

Argument	Description
<code>-oracleHome</code>	The Oracle home of the instance. The <code>portconfig</code> command modifies only components that are part of the selected Oracle home. You can use an environment variable to represent the Oracle home.
<code>-oldPort</code>	The old (current) value of the Oracle HTTP Server Listen port.
<code>-newPort</code>	The new value for the Oracle HTTP Server Listen port.

Table 14–2 (Cont.) Arguments for the portconfig Command

Argument	Description
-webCache	When this argument is included on the command line, the dependent OracleAS Web Cache port assignment will be changed automatically. Specifically, the port number of the origin server will be updated automatically so it points to the new Oracle HTTP Server listen port. The port number of the origin server is the port on which OracleAS Web Cache forwards requests to Apache (the HTTP Server Listen Port). This is different from the OracleAS Web Cache Listen Port, which is the port on which end users will normally access Oracle Collaboration Suite. Note: The <code>portconfig</code> command updates the OracleAS Web Cache instance only if it resides in the current Oracle home.
-start	When you use this optional argument, the <code>portconfig</code> command performs the configuration changes, and then stops and starts the instance. The instance must be stopped and started—or restarted—before the port changes will take effect. Note that during startup, all enabled components of the tier are started, even those that were originally down before you ran the <code>portconfig</code> command to change the Oracle HTTP Server Listen port. Compare with the <code>-restart</code> argument. Each time you run the command you can use the <code>-restart</code> or <code>-start</code> options, but not both.
-restart	When you use this optional argument, the <code>portconfig</code> command performs the configuration changes, and then restarts the instance. The instance must be restarted—or stopped and started—before the port changes will take effect. With this option, only already running components are restarted after the configuration changes are complete. Components that were down before you ran the <code>portconfig</code> command to change the Oracle HTTP Server Listen port will remain down. Compare with the <code>-start</code> argument. Each time you run the command you can use the <code>-restart</code> or <code>-start</code> options, but not both.
-debug	Use this optional argument if you want to display debugging information as the command executes. This argument can be useful if you are troubleshooting a problem or working with Oracle Support.
-sso	Use this optional argument when the Listen port you are changing is protected by OracleAS Single Sign-On. The <code>portconfig</code> command re-registers <code>mod_osso</code> with the new Oracle HTTP Server Listen port value. When you use the <code>-sso</code> argument, then you must include the <code>-url</code> and <code>-user</code> arguments. In addition, you can optionally use the <code>-site</code>, <code>-admin</code> and <code>-vHost</code> arguments. For more information about registering <code>mod_osso</code>, see "Configuring and Administering Partner Applications" in the <i>Oracle Application Server Single Sign-On Administrator's Guide</i>.
-url	This argument is required when you use the <code>-sso</code> argument. Use this argument to provide the new Oracle HTTP Server URL, which is also used by OracleAS Single Sign-On and uses the new Listen port. For example: <pre>http://apps2.acme.com:7778</pre> This URL is passed as the <code>-mod_osso_url</code> parameter in the <code>ssoreg.sh</code> and <code>ssoreg.bat</code> scripts.

Table 14–2 (Cont.) Arguments for the portconfig Command

Argument	Description
-user	This argument is required when you use the -sso argument. Use this argument to enter the name of the account that is used to start Oracle HTTP Server. On UNIX systems, this is usually root. On Windows, it is usually SYSTEM. The value provided with this argument is passed as the -u parameter in the ssoreg.sh and ssoreg.bat scripts.
-site	This argument is optional; however, it can be used only when you also use the -sso argument. Use this argument to enter the site name of OracleAS Single Sign-On partner application. The site name is displayed by the OracleAS Single Sign-On administration pages. The value of this argument is passed as the -site_name parameter in the ssoreg.sh and ssoreg.bat scripts. If the -site argument is not specified, the instance name is passed to ssoreg.sh and ssoreg.bat scripts as the value of the -site_name parameter.
-admin	This argument is optional; however, it can be used only when you also use the -sso argument. Use this argument to enter the account name of the mod_osso administrator. This value is displayed in the OracleAS Single Sign-On administration pages. In most cases, this value should be the same as the distinguished name (DN) of the user who installed Oracle Collaboration Suite. The value of this argument is passed as the -admin_info parameter in the ssoreg.sh and ssoreg.bat scripts.
-vHost	This argument is optional; however, it can be used only when you also use the -sso argument. Use this argument to enter the path to the osso.conf file for the virtual host being configured. For example: <pre>\$ORACLE_HOME/Apache/Apache/conf/osso/vh_name/osso.conf</pre> Use this argument only when you are registering an HTTP virtual host with the OracleAS Single Sign-On server. The value of this argument is passed as the -config_file parameter, along with the -virtualhost parameter, in the ssoreg.sh and ssoreg.bat scripts.

5. Update the Oracle Internet Directory Service Registry entries for all affected applications, changing the URIs to use the new port number.

For complete instructions on editing the Oracle Internet Directory Service Registry, see ["Using Oracle Directory Manager to Edit the Oracle Internet Directory Service Registry"](#) on page 7-10.

6. Restart the Applications tier instance:

(UNIX)

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/opmn/bin/opmnctl startall
ORACLE_HOME/bin/emctl start iasconsole
```

(Windows)

```
ORACLE_HOME\bin\emctl stop iasconsole
ORACLE_HOME\opmn\bin\opmnctl stopall
ORACLE_HOME\opmn\bin\opmnctl startall
ORACLE_HOME\bin\emctl start iasconsole
```

Changing the OracleAS Web Cache Listen Port

This section describes how to change the OracleAS Web Cache HTTP or HTTPS listen port. It involves changing the OracleAS Web Cache port number and updating other components in the Applications tier with the new port number. The relevant tasks include the following:

- [Task 1: Enable OracleAS Web Cache to Run as Root for Ports Less Than 1024 on UNIX](#)
- [Task 2: Change the OracleAS Web Cache Listen Port](#)
- [Task 3: Change the OracleAS Web Cache Logical Site Port](#)
- [Task 4: Update the Oracle HTTP Server Port Directive](#)
- [Task 5: Update the Oracle Collaboration Suite Control Console](#)
- [Task 6: Update mod_osso](#)
- [Task 7: Update OracleAS Portal Configuration](#)
- [Task 8: Update Web Providers](#)
- [Task 9: Update Oracle Mobile Collaboration](#)
- [Task 10: Restart the Applications Tier Instance](#)
- [Task 11: Run the Collaborative Portlets Configuration Assistant](#)

Task 1: Enable OracleAS Web Cache to Run as Root for Ports Less Than 1024 on UNIX

Perform this task only if you are changing the port to a number less than 1024.

By default, OracleAS Web Cache runs as a non-root user (the user that installed Oracle Collaboration Suite). On UNIX systems, if you change the OracleAS Web Cache listen port number to a privileged port (with a value less than 1024), you must enable OracleAS Web Cache to run as root, as follows:

1. Log in as the user that installed Oracle Collaboration Suite and stop OracleAS Web Cache:

```
opmnctl stopproc ias-component=WebCache
```

2. Log in as root.
3. Run the following command in the Applications tier Oracle home:

```
ORACLE_HOME/webcache/bin/webcache_setuser.sh setroot user_ID
```

The parameter *user_ID* is the user ID associated with the OracleAS Web Cache processes. This is usually the user that installed Oracle Collaboration Suite. This user is listed on the Process Identity section of the Security page of Oracle Collaboration Suite Control Console. Navigate as follows:

From the OracleAS Web Cache Home page, select the **Administration** tab. Then select **Properties -> Web Cache -> Security -> Process Identity**.

4. Log in as the user that installed Oracle Collaboration Suite and start OracleAS Web Cache:

```
opmnctl startproc ias-component=WebCache
```

Task 2: Change the OracleAS Web Cache Listen Port

Take the following steps:

1. Using the Oracle Collaboration Suite Control Console, navigate to the Web Cache home page.
2. Click the **Administration** tab to display the Administration page.
3. On the Administration page, click **Ports** to display the Ports page.
4. In the **Listen Ports** section, locate the appropriate port that has HTTP or HTTPS in the **Protocol** column.
5. Enter the new port number in the **Port** field.
6. Click **OK** to apply changes.
7. When prompted, click **Restart Web Cache** to restart the cache.

Task 3: Change the OracleAS Web Cache Logical Site Port

If the OracleAS Web Cache listen port is the same as the logical site port, update the logical site port as follows:

1. On the Administration page, click **Sites** to display the Sites page.
2. Locate the appropriate sites using the old port number. If there is no site using the old port number, then the OracleAS Web Cache listener and site do not share the same port number.
3. For each site using the old port number:
 - a. Click **Edit**.
 - b. In the Edit Named Site or Edit Unnamed Site page, enter the new port number in the **Port** field.
4. Click **OK** to apply changes.
5. When prompted, click **Restart Web Cache** to restart the cache.

Task 4: Update the Oracle HTTP Server Port Directive

If you are changing the OracleAS Web Cache HTTP listen port to be the same as the logical site port, update the `Port` directive in the Oracle HTTP Server `httpd.conf` file:

1. Open the `httpd.conf` file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/httpd.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\httpd.conf
```

2. Update the `Port` directive with the new port number, and then save the file.
Do not modify the `Listen` directive. The OracleAS Web Cache port must be the same as the Oracle HTTP Server Port directive.

3. Run the following command:

```
dcmctl updateConfig -ct ohs
```

If you are changing the OracleAS Web Cache HTTPS listen port, update the `Port` directive in the Oracle HTTP Server `ssl.conf` file:

1. Open the `ssl.conf` file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/ssl.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\ssl.conf
```

2. Update the `SSL Port` directive with the new port number, and then save the file.

Do not modify the `Listen` directive. The OracleAS Web Cache SSL port must be the same as the Oracle HTTP Server SSL Port directive.

3. Run the following command:

```
dcmctl updateConfig -ct ohs
```

Task 5: Update the Oracle Collaboration Suite Control Console

Update the Oracle Collaboration Suite Control Console with the new port number:

1. Open the `targets.xml` file:

```
(UNIX) ORACLE_HOME/sysman/emd/targets.xml
(Windows) ORACLE_HOME\sysman\emd\targets.xml
```

2. Update each occurrence of the old OracleAS Web Cache listen port number with the new port number, and then save the file.

Depending on your configuration, this file may not contain any occurrences of the OracleAS Web Cache listen port, or it may contain many occurrences. The listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old OracleAS Web Cache listen port number, and replace them with the new port number.

3. Reload the Oracle Collaboration Suite Control:

```
emctl reload
```

Task 6: Update mod_osso

If you have registered your virtual host as an OracleAS Single Sign-On partner application, follow these steps to re-register your virtual host with the new port number:

1. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
2. Re-register `mod_osso` with the new port number by running the following command in the Applications tier Oracle home:

UNIX:

```
ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path applications_tier_oracle_home
-site_name applications_tier_hostname:new_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
```

Windows:

```
ORACLE_HOME\sso\bin\ssoreg.bat
-oracle_home_path applications_tier_oracle_home
-site_name applications_tier_hostname:new_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
```

For example, if you want to change the OracleAS Web Cache listen port to 7779 on Applications tier host `myhost`:

```
$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path /disk1/oracleas
-site_name myhost:7779
```

```
-config_mod_osso TRUE
-mod_osso_url http://myhost.mydomain:7779
```

See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering `mod_osso`

3. If you are changing the OracleAS Web Cache HTTPS listen port, perform the following steps. These steps do not apply if you are changing the OracleAS Web Cache HTTP listen port.

- a. Open the `mod_osso.conf` file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/mod_osso.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\mod_osso.conf
```

- b. Replace references to `osso.conf` with `applications_tier_hostname.applications_tier_domain.https-osso.conf`, and save the file.

For example, if you have the following entry in the `mod_osso.conf` file:

```
/disk1/oracleas/Apache/Apache/conf/mod_osso.conf
```

You would make the following change for the HTTPS listen port on Applications tier host `myhost.mydomain`:

```
/disk1/oracleasApache/Apache/conf/myhost.mydomain.https-osso.conf
```

4. If you are changing the OracleAS Web Cache HTTPS listen port, perform these additional steps:

- a. Open the `mod_osso.conf` file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/mod_osso.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\mod_osso.conf
```

- b. Replace references to `osso.conf` with `applications_tier_hostname.applications_tier_domain.https-osso.conf`, and save the file.

For example, if you have the following entry in the `mod_osso.conf` file:

```
$ORACLE_HOME/Apache/Apache/conf/mod_osso.conf
```

You would make the following change for OracleAS Web Cache HTTPS listen port on Applications tier host `myhost.mydomain`:

```
$ORACLE_HOME/Apache/Apache/conf/myhost.mydomain.https-osso.conf
```

Task 7: Update OracleAS Portal Configuration

If you are changing the OracleAS Web Cache HTTP listen port in a configuration with OracleAS Portal, update OracleAS Portal configuration with the new port number:

1. Using the Oracle Collaboration Suite Control, navigate to the Portal home page.
2. In the **Administration** section, click **Portal Web Cache Settings**.
3. In the **Listening Port** field, enter the new port number.
4. Click **Apply**.

If you are changing the OracleAS Web Cache HTTPS (SSL) listen port in a configuration with OracleAS Portal, update OracleAS Portal configuration with the new port number:

1. Update OracleAS Portal configuration:
 - a. Using the Application Server Control Console, navigate to the Portal home page.
 - b. In the **Administration** section, click **Portal Web Cache Settings**.
 - c. In the **Listening Port** field, enter the new port number.
 - d. From the **Listening Port SSL Enabled** list, select **Yes**.
 - e. Click **Apply**.
2. Update the `httpsports` parameter in the following file:
`ORACLE_HOME/j2ee/OC4J_Portal/applications/portal/portal/WEB-INF/web.xml`
3. Restart the OC4J_Portal:
 - a. Using the Oracle Collaboration Suite Control Console, navigate to the OC4J: OC4J_Portal home page.
 - b. In the General section, click **Start**.

See Also: *Oracle Application Server Portal Configuration Guide* for more information on updating the Portal Web Cache Settings
4. Re-register the OracleAS Portal. To do this:
 - a. Ensure that the `ORACLE_HOME` environment variable is set.
 - b. Register the URLs using the Portal Dependency Settings tool (available in `ORACLE_HOME/portal/conf`) :


```
ptlconfig -dad dadname -wc -site
```


where `dadname` is the name of the OracleAS Portal Database Access Descriptor.

Task 8: Update Web Providers

If you are using Web Providers with OracleAS Portal, you must update them as follows (note that locally hosted Web Providers run on the same Applications tier instance as OracleAS Portal):

1. Log in to OracleAS Portal as the administrator (for example, `ocsadmin`).
2. Click the **Administer** tab.
3. Click the **Portlets** sub-tab.
4. Repeat this step for all locally hosted Web Providers registered in your Portal:
 - a. In the Remote Providers portlet, enter the provider name in the **Name** field. Click **Edit**.
 - b. Click the **Connection** tab.
 - c. In the **URL** field, update the port to the new port number. Click **Apply**.
 - d. Click **OK**.

Task 9: Update Oracle Mobile Collaboration

If you have Oracle Mobile Collaboration configured, update Oracle Mobile Collaboration with the new port number:

1. Re-register Oracle Mobile Collaboration with OracleAS Single Sign-On by running the following command on the Applications tier host:

```
(UNIX) ORACLE_HOME/wireless/bin/reRegisterSSO.sh new_wireless_url oracle_home
administrator_dn
(Windows) ORACLE_HOME\wireless\bin\reRegisterSSO.bat
new_wireless_url oracle_home administrator_dn
```

In the example:

- *new_wireless_url*: Wireless HTTP URL with the new OracleAS Web Cache listen port.
- *oracle_home*: Applications tier Oracle home whose OracleAS Web Cache port you are changing.
- *administrator_dn*: Oracle Internet Directory administrator.

For example, if you have changed the OracleAS Web Cache listen port to 7779 on the Applications tier installation in `/home/oracle` on UNIX host `myhost`:

```
ORACLE_HOME/wireless/bin/reRegisterSSO.sh http://myhost:7779/ptg/rm
/home/oracle cn=orcladmin
```

2. Update the Wireless HTTP and HTTPS configuration information:
 - a. Navigate to the Oracle Mobile Collaboration home page on the Oracle Collaboration Suite Control Console.
 - b. Select the **Site Administration** link.
 - c. In the **General Configuration** section, select the **HTTP, HTTPS Configuration** link.
 - d. In the **URL** section, update each URL that contains the OracleAS Web Cache listen port with the new port number.
 - e. Click **OK**.
3. Update the instance URLs:
 - a. Navigate to the Oracle Mobile Collaboration home page on the Oracle Collaboration Suite Control Console.
 - b. In the **Instance Configuration** section, select the **Instance URLs** link.
 - c. On the Instance URLs page:
 - If **Use the Oracle Mobile Collaboration Site URLs** is selected, you do not need to make any changes to this page.
 - If **Use the Oracle Mobile Collaboration Instance URLs** is selected, update each URL that contains the OracleAS Web Cache listen port with the new port number.
 - d. Click **OK**.
4. Update the Oracle Internet Directory Service Registry with the new port number. Perform the following steps:
 - a. Start the Oracle Directory Manager and enter connection information for your instance of Oracle Internet Directory:

```
ORACLE_HOME/bin/oidadmin
```

```
Host: <infrahost.yourdomain.com>
Port: 389
Username: cn=orcladmin
Password: <password>
```

- b. To access the Service Registry, select **Entry Management, cn=OracleContext, cn=Services**.
- c. Select each configured component in the System Objects pane to display its attributes. Components which have been configured will contain a cn=VirtualServices object, which in turn contains one or more child objects. These child objects contain virtual services URIs, including port numbers.
- d. Check each component, changing each URI containing connection information to the old OracleAS Web Cache Listen Port to the new port number. Save your changes and close Oracle Directory Manager.

Task 10: Restart the Applications Tier Instance

Restart the Applications tier instance:

```
emctl stop iasconsole
opmnctl stopall
opmnctl startall
emctl start iasconsole
```

Task 11: Run the Collaborative Portlets Configuration Assistant

Run the Collaborative Portlets Configuration Assistant. This will rebuild Collaborative Portlets with the new connection information.

To run the Collaborative Portlets Configuration Assistant, refer to ["Changing the Host or Port on an Applications Tier hosting Oracle Collaborative Portlets"](#) on page 5-43.

Changing the OracleAS Web Cache Administration Port

The tasks to change the OracleAS Web Cache administration port include the following:

- [Task 1: Change the OracleAS Web Cache Administration Port](#)
- [Task 2: Update OracleAS Portal](#)

Task 1: Change the OracleAS Web Cache Administration Port

To change the OracleAS Web Cache administration port on any installation type:

1. Using the Oracle Collaboration Suite Control, navigate to the Web Cache home page.
2. Click the **Administration** tab to display the Administration page.
3. On the Administration page, click **Ports** to display the Ports page.
4. In the **Operation Ports** section, locate the **Administration** row.
5. Enter the new port number in the **Port** field.
6. Click **OK** to apply changes.
7. When prompted, click **Restart Web Cache** to restart the cache.

Task 2: Update OracleAS Portal

If you have OracleAS Portal configured, update OracleAS Portal configuration with the new port number:

1. Using the Oracle Collaboration Suite Control Console, navigate to the Portal home page.
2. In the **Administration** section, click **Portal Web Cache Settings**.
3. In the **Administration Port** field, enter the new port number.

See Also: *Oracle Application Server Portal Configuration Guide* for more information on updating the Portal Web Cache Settings

Changing the OracleAS Web Cache Invalidation Port

The tasks to change the OracleAS Web Cache invalidation port include the following:

- [Task 1: Change the OracleAS Web Cache Invalidation Port](#)
- [Task 2: Update OracleAS Portal](#)
- [Task 3: Update Web Providers](#)

Task 1: Change the OracleAS Web Cache Invalidation Port

To change the OracleAS Web Cache invalidation port on any installation type:

1. Using the Oracle Collaboration Suite Control Console, navigate to the Web Cache home page.
2. Click the **Administration** tab to display the Administration page.
3. On the Administration page, click **Ports** to display the Ports page.
4. In the **Operation Ports** section, locate the **Invalidation** row.
5. Enter the new port number in the **Port** field.
6. Click **OK** to apply changes.
7. When prompted, click **Restart Web Cache** to restart the cache.

Task 2: Update OracleAS Portal

If you have OracleAS Portal configured, update OracleAS Portal with the new port number:

1. Using the Oracle Collaboration Suite Control Console, navigate to the Portal home page.
2. In the **Administration** section, click **Portal Web Cache Settings**.
3. In the **Invalidation Port** field, enter the new port number.

See Also: *Oracle Application Server Portal Configuration Guide* for more information on updating the Portal Web Cache Settings

Task 3: Update Web Providers

If you are using Web Providers with OracleAS Portal, you must update them to use the new port as follows:

1. Open the `cache.xml` file:
 - (UNIX) `ORACLE_HOME/portal/conf/cache.xml`
 - (Windows) `ORACLE_HOME\portal\conf\cache.xml`

2. Update the `port` attribute to the new port, and then save the file.
3. Restart OC4J_Portal:
 - a. Using the Oracle Collaboration Suite Control Console, navigate to the OC4J: OC4J_Portal home page.
 - b. In the **General** section, click **Start**.

Changing the OracleAS Web Cache Statistics Port

To change the OracleAS Web Cache statistics port on any installation type:

1. Using the Oracle Collaboration Suite Control Console, navigate to the Web Cache home page.
2. Click the **Administration** tab to display the Administration page.
3. On the Administration page, click **Ports** to display the Ports page.
4. In the **Operation Ports** section, locate the **Statistics** row.
5. Enter the new port number in the **Port** field.
6. Click **OK** to apply changes.
7. When prompted, click **Restart Web Cache** to restart the cache.

If you change the statistics protocol to HTTPS, it is not possible to view performance statistics in Enterprise Manager until a [certificate](#) is uploaded in Base64 format named `b64InternetCertificate.txt` to `ORACLE_HOME/sysman/config` on UNIX and `ORACLE_HOME\sysman\config` on Windows.

Changing the DCM Discovery Port

This section describes how to change the DCM Discovery port number in any installation type. To change the DCM Discovery port number:

1. Open the `dcmCache.xml` file:

```
(UNIX) ORACLE_HOME/dcm/config/dcmCache.xml
(Windows) ORACLE_HOME\dcm\config\dcmCache.xml
```
2. Under the `<communication>` element, update the `discovery-port` parameter in the `<coordinator>` element with the new port number, and then save the file.

For example:

```
<coordinator discovery-port="7110" original="true" />
```

3. In every Oracle Collaboration Suite tier in the farm, stop the Oracle Collaboration Suite Control Console and stop the DCM daemon:

```
emctl stop iasconsole
opmnctl stopproc ias-component=dcm-daemon
```

It is important that you make sure all Oracle Collaboration Suite Control Console instances and DCM daemons in the farm are stopped before you proceed to the next step.

4. In every instance in the farm, start the DCM daemon and the Oracle Collaboration Suite Control Console:

```
opmnctl startproc ias-component=dcm-daemon
```



```
emctl start iasconsole
```

Changing the Java Object Cache Port

This section describes how to change the Java Object Cache port number in any installation type. To change the Java Object Cache port number:

1. Open the `javacache.xml` file:

```
(UNIX) ORACLE_HOME/javacache/admin/javacache.xml
(Windows) ORACLE_HOME\javacache\admin\javacache.xml
```

2. Under the `<communication>` element, update the `discovery-port` parameter in the `<coordinator>` element with the new port number, and then save the file.

For example:

```
<coordinator discovery-port="7010" />
```

3. Restart all OC4J instances which contain J2EE applications that use JavaCache:

```
dcmctl restart -co OC4J_INSTANCE
```

Changing the Log Loader Port

This section describes how to change the Log Loader port on any installation type. To change the Log Loader port:

1. Stop the Log Loader:
 - a. Using the Oracle Collaboration Suite Control Console, navigate to the Oracle Collaboration Suite home page for the instance whose Log Loader port you would like to change.
 - b. Click **Logs** in the upper-right corner.
 - c. On the View Logs page, click **Search Log Repository**.
 - d. On the View Logs page, click **Log Loader**.
 - e. On the Log Loader page, click **Stop**.
2. Change the Log Loader port number:
 - a. On the Log Loader page, in the Administration section, click **Log Loader Properties**.
 - b. On the Log Loader Properties page, enter the new port number in the Log Loader Port field.
 - c. Click **Apply**.
3. Start the Log Loader:
 - a. At the top of the Log Loader Properties page, click **Log Loader** to get back to the Log Loader page.
 - b. On the Log Loader page, click **Start**.

Changing OPMN Ports (ONS Local, Request, and Remote)

This section describes how to change any of the following port numbers:

- ONS Local port
- ONS Request port

- ONS Remote port

To change these ports:

1. Stop the Oracle Collaboration Suite Control Console, OPMN and all OPMN-managed processes:

```
emctl stop iasconsole
opmnctl stopall
```

2. Open the `opmn.xml` file:

```
(UNIX) ORACLE_HOME/opmn/conf/opmn.xml
(Windows) ORACLE_HOME\opmn\conf\opmn.xml
```

3. Under the `<notification-server>` element, modify the `local`, `remote`, or `request` parameter, as desired, in the `<port>` element, and then save the file.

For example:

```
<port local="6101" remote="6201" request="6004"/>
```

4. Start OPMN:

```
opmnctl start
```

5. Reload OPMN:

```
opmnctl reload
```

6. If this is an Infrastructure with Oracle Internet Directory, start Oracle Internet Directory:

```
opmnctl startproc ias-component=OID
```

7. Start the rest of the processes:

```
opmnctl startall
emctl start iasconsole
```

8. Update DCM:

```
dcmctl updateConfig -ct opmn
```

Changing the Oracle HTTP Server Diagnostic Port

This section describes how to change the Oracle HTTP Server Diagnostics port number in any installation type. To change the Oracle HTTP Server Diagnostics port number:

1. Open the `dms.conf` file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/dms.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\dms.conf
```

2. Change the old port number to the new port number everywhere it appears in the file, and then save the file. This update includes the `Listen` directive, `OpmnHostPort` directive, `Redirect` directive, and the `VirtualHost`.

3. Restart Oracle HTTP Server:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl startproc ias-component=HTTP_Server
```

Changing the Port Tunneling Port

This section describes how to change the Port Tunneling port on any installation type. To change the Port Tunneling port number:

1. Open the `opmn.xml` file:

```
(UNIX) ORACLE_HOME/opmn/conf/opmn.xml
(Windows) ORACLE_HOME\opmn\conf\opmn.xml
```

2. Under the `<ias-component id="IASPT">` element, update the range parameter in the `<port>` element with the new range. For example:

```
<port id="ajp" range="7501-7503"/>
```

Note that the port number range specified in `opmn.xml` overrides any port number specified in `iaspt.conf`. So you only need to update the port number in `opmn.xml`.

3. Restart OPMN:

```
opmnctl reload
emctl stop iasconsole
opmnctl stopall
opmnctl startall
emctl start iasconsole
```

Changing OracleAS Portal Ports

OracleAS Portal uses the OracleAS Web Cache HTTP server port on the instance.

See Also: ["Changing the OracleAS Web Cache Listen Port"](#) on page 14-10

Changing Oracle Mobile Collaboration Ports

Oracle Mobile Collaboration uses the OracleAS Web Cache HTTP server port on the instance.

See Also: ["Changing the OracleAS Web Cache Listen Port"](#) on page 14-10

Specifying Ports for DMS-Monitored Services

Dynamic monitoring services (DMS) collect performance metrics for the following Oracle Voicemail & Fax services: Routing, Retrieval, Recording, Telephony Monitor, and Message Delivery Monitor. By default, Oracle Voicemail & Fax assigns 46080 as the port number to the first process, and keeps assigning subsequent ports to each new process. There is no predefined range of ports. If you do not need to manage your port access, use the default port and the open-ended port range.

If you want to use a specific port range, you will need to edit the `%ORACLE_HOME%\opmn\conf\opmn.xml` file.

To specify a port range for the Oracle Voicemail & Fax Services:

1. Open the `opmn.xml` file in an XML editor or text editor.
2. Find the process type ID for the Oracle Voicemail & Fax service. The following are the process type ID values for the monitored services:
 - `MsgDeliveryMonitorService`

- RecordingService
 - RetrievalService
 - RoutingService
 - TelephonyMonitorService
3. In the `<data>` tag, append the following to the end of the string of values for the `id="java-options"` attribute:

```
-Doracle.dms.publisher.classes=oracle.dms.http.Httpd  
-Doracle.dms.httpd.port.start=first_port_number  
-Doracle.dms.httpd.port.len=number_of_ports
```

where:

Parameter	Description
<i>first_port_number</i>	First port number assigned to this service
<i>number_of_ports</i>	Total number of ports assigned to this service

In the following example, a starting port of 56080 and a total of 50 ports is assigned to the Routing Service:

```
<process-type id="RoutingService" module-id="oracle_ovf_routing"  
status="enabled">  
  <module-data>  
    <category id="start-parameters">  
      <data id="java-options" value="..."  
-Doracle.dms.publisher.classes=oracle.dms.http.Httpd  
-Doracle.dms.httpd.port.start=56080  
-Doracle.dms.httpd.port.len=50"/>
```

Note: Be careful not to change any of the other attributes in the `<data>` tag.

4. Specify the ports for each of the Oracle Voicemail & Fax Services monitored by DMS.

Note: Be sure that the port ranges for the services do not overlap with each other or with other port specifications for this system.

Changing Infrastructure Ports

This section contains the following topics:

- [Changing the OracleAS Metadata Repository Net Listener Port](#)
- [Changing Oracle Internet Directory Ports](#)
- [Changing the HTTP Server Port on Identity Management](#)

Changing the OracleAS Metadata Repository Net Listener Port

First, determine if it is necessary to change the OracleAS Metadata Repository listener port number. If you are concerned about the fact that you have another database on

your host using the same port, it is possible that the OracleAS Metadata Repository and the other database can use the same port.

The following are guidelines for port usage by multiple databases on the same host:

- Multiple Oracle9i and Oracle Database10g databases can share the same Oracle Net listener port. If you install a OracleAS Metadata Repository on a host that contains Oracle9i and Oracle Database 10g databases, they can all use port 1521. There is no need to change the OracleAS Metadata Repository port number.
- If the other databases on your system are Oracle8i databases running the Net8 listener, then the OracleAS Metadata Repository must use a different port. They cannot share the same port.

Note: If you want to run two listeners that use the same key value on one host, refer to [Section , "Changing the KEY value for an IPC Listener"](#)

If you determine that you would like to change the OracleAS Metadata Repository Listener Port, follow the steps in this section. An OracleAS Metadata Repository may be used in several different ways. Use the following table to determine the steps that are required for changing your type of OracleAS Metadata Repository:

If the OracleAS Metadata Repository is used as follows:	Follow these tasks to change its Oracle Net listener port:
■ Identity Management Repository, Product Metadata Repository, and Management (DCM) Repository ■ Registered with Oracle Internet Directory	Task 1: Stop Applications Tier Instances Task 2: Change the OracleAS Metadata Repository Oracle Net Listener Port Task 3: Update Oracle Internet Directory Task 4: Update OracleAS Single Sign-On Task 5: Update OracleAS Certificate Authority Task 6: Update the Application Server Control Console Task 7: Update Applications Tier Instances
■ Identity Management Repository only ■ Registered with Oracle Internet Directory	Task 1: Stop Applications Tier Instances Task 2: Change the OracleAS Metadata Repository Oracle Net Listener Port Task 3: Update Oracle Internet Directory Task 4: Update OracleAS Single Sign-On Task 5: Update OracleAS Certificate Authority Task 6: Update the Application Server Control Console
■ Product Metadata and Management (DCM) Repository ■ Registered with Oracle Internet Directory	Task 1: Stop Applications Tier Instances Task 2: Change the OracleAS Metadata Repository Oracle Net Listener Port Task 3: Update Oracle Internet Directory Task 7: Update Applications Tier Instances

Task 1: Stop Applications Tier Instances

Stop all Applications tier instances that use the Metadata Repository by running the following command in each Applications tier Oracle home:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl stopall
```

```
(Windows) ORACLE_HOME\opmn\bin\opmnctl stopall
```

Task 2: Change the OracleAS Metadata Repository Oracle Net Listener Port

On the OracleAS Metadata Repository (Infrastructure tier) host:

1. Make sure your ORACLE_HOME environment variable and ORACLE_SID are set.

2. If OPMN is running, stop it:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl stopall  
(Windows) ORACLE_HOME\opmn\bin\opmnctl stopall
```

3. Stop the OracleAS Metadata Repository listener:

```
lsnrctl stop
```

4. Open the listener.ora file:

```
(UNIX) ORACLE_HOME/network/admin/listener.ora  
(Windows) ORACLE_HOME\network\admin\listener.ora
```

- a. Under the LISTENER entry, update the value for PORT.

- b. Add the following SID_DESC entry to the SID_LIST_LISTENER entry:

```
(SID_DESC =  
  (GLOBAL_DBNAME = service_name)  
  (ORACLE_HOME = oracle_home_path)  
  (SID_NAME = sid)  
)
```

5. Edit the tnsnames.ora file. The default location is:

```
(UNIX) ORACLE_HOME/network/admin/tnsnames.ora  
(Windows) ORACLE_HOME\network\admin\tnsnames.ora
```

- a. Update the PORT value in each entry that applies to OracleAS Metadata Repository.

- b. Add an entry like the following:

```
newnetport =  
  (DESCRIPTION =  
    (ADDRESS = (PROTOCOL = tcp) (HOST = hostname) (PORT = port)))
```

In the example, *hostname* is the fully-qualified hostname and *port* is the new port number.

6. Start the OracleAS Metadata Repository listener:

```
lsnrctl start
```

7. Using SQL*Plus, log in to the OracleAS Metadata Repository as the SYSTEM user with SYSDBA privileges and run the following command:

```
SQL> alter system set local_listener='newnetport' scope=spfile;
```

8. Restart OracleAS Metadata Repository:

```
SQL> shutdown  
SQL> startup
```

Task 3: Update Oracle Internet Directory

On the Identity Management host, update Oracle Internet Directory with the new Oracle Net listener port number:

1. Restart the OracleAS Metadata Repository OPMN process by running the following command on the Infrastructure:

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OID
```

2. Start Oracle Directory Manager:

```
(UNIX) ORACLE_HOME/bin/oidadmin
```

```
(Windows) Start > Programs > Oracle Collaboration Suite - OracleHome >  
Integrated Management Tools > Oracle Directory Manager
```

3. Log in to Oracle Directory Manager.
4. In the System Objects frame:
 - a. Expand **Entry Management**.
 - b. Expand **cn=Oracle Context**.
 - c. Select the DBName for the OracleAS Metadata Repository. For example, if the DBName is the default, `orcl`, select **cn=ORCL**.
5. On the Properties tab, update the PORT parameter in the `orclnetdescstring` field with the new port number.
6. Click **Apply**.
7. Start OPMN in the Oracle Internet Directory Oracle home:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl startall
```

```
(Windows) ORACLE_HOME\opmn\bin\opmnctl startall
```

Task 4: Update OracleAS Single Sign-On

On the OracleAS Single Sign-On host:

1. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
2. Update OracleAS Single Sign-On with the new repository port number by running the following command in the OracleAS Single Sign-On Oracle home:

```
ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoca.jar reassoc -repos  
$ORACLE_HOME
```

3. In the OracleAS Single Sign-On Oracle home, restart OC4J:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=OC4J
```

```
(Windows) ORACLE_HOME\opmn\bin\opmnctl restartproc ias-component=OC4J
```

Task 5: Update OracleAS Certificate Authority

If the Identity Management installation has OracleAS Certificate Authority:

1. Run the following command:

```
(UNIX) ORACLE_HOME/oca/bin/ocactl updateconnection
```

```
(Windows) ORACLE_HOME\oca\bin\ocactl updateconnection
```

2. Restart OracleAS Certificate Authority:

```
ocactl stop
ocactl start
```

If you are not sure if OracleAS Certificate Authority is configured, examine the Oracle Collaboration Suite home page to see if it is listed in the Components section.

Task 6: Update the Application Server Control Console

Update the Application Server Control Console with the new port number:

1. In the Identity Management Oracle home, edit the following file:

```
(UNIX) ORACLE_HOME/sysman/emd/targets.xml
(Windows) ORACLE_HOME\sysman\emd\targets.xml
```

2. Update the old OracleAS Metadata Repository port number with the new port number, and then save the file.

Locate the `oracle_ldap` target and update the `PORT` parameter in the `ConnectDescriptor` value with the new port number. The easiest way to find this is to search the file for the old port number.

3. Reload the Oracle Collaboration Suite Control Console:

```
emctl reload
```

Task 7: Update Applications Tier Instances

In each Applications tier Oracle home that uses OracleAS Metadata Repository:

1. Update the following file with the new Oracle Net listener port number:

```
(UNIX) ORACLE_HOME/network/admin/tnsnames.ora
(Windows) ORACLE_HOME\network\admin\tnsnames.ora
```

2. Check the following file:

```
(UNIX) ORACLE_HOME/Apache/modplsql/conf/dads.conf
(Windows) ORACLE_HOME\Apache\modplsql\conf\dads.conf
```

Locate the line that begins with `PlsqlDatabaseConnectString`.

- If the line ends with `ServiceNameFormat` or `SIDFormat`, update the line with the new OracleAS Metadata Repository port number, save the file, and restart Oracle HTTP Server.
 - If the line ends with `NetServiceNameFormat`, you do not need to do anything.
3. Start the Applications tier instance:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl startall
(Windows) ORACLE_HOME\opmn\bin\opmnctl startall
```

Changing the KEY value for an IPC Listener

It is not possible to run two listeners at the same time that are configured to use the same KEY value in their IPC protocol address. By default, the OracleAS Metadata Repository listener has its IPC KEY value set to `EXTPROC`. Hence, if your computer has another IPC listener that uses the `EXTPROC` key, you should configure the OracleAS Metadata Repository listener to use some other key value such as `EXTPROC1`.

To change the KEY value of an IPC listener:

1. Stop the listener (make sure your ORACLE_HOME environment variable is set first):

```
lsnrctl stop
```

2. Edit the `listener.ora` and `tnsnames.ora` files. In each file, change the line that says:

```
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC))
```

to something like:

```
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1))
```

3. Restart the listener:

```
lsnrctl start
```

Changing Oracle Internet Directory Ports

This section describes how to change the Oracle Internet Directory HTTP or HTTPS port on an Identity Management installation. When you change this port number, you must update any Applications tier instances that use the Identity Management installation.

The following procedures contain complete instructions for updating the Oracle Internet Directory port number on Identity Management, including updating other components in the Infrastructure and updating the Applications tier instances that use the port. The relevant tasks are as follows:

- [Task 1: Prepare the Applications Tier Instances](#)
- [Task 2: Prepare the Infrastructure Instances](#)
- [Task 3: Change the Oracle Internet Directory Port](#)
- [Task 5: Restart the Identity Management Instance](#)
- [Task 6: Update the Applications Tier Instances to Use the New Port Number](#)

Task 1: Prepare the Applications Tier Instances

Follow this task only if the Identity Management installation is being used by Applications tier instances. On each Applications tier instance, stop the Applications tier instance as follows:

1. On the Oracle Collaboration Suite home page of the Oracle Collaboration Suite Control Console, click **Stop All**.
2. Leave the Oracle Collaboration Suite Control Console running.

It is important that you leave the Oracle Collaboration Suite Control Console running in each of the Applications tier instances while you perform this procedure.

Task 2: Prepare the Infrastructure Instances

1. Make sure that Identity Management and its associated OracleAS Metadata Repository are up and running on the Infrastructure whose port number you are changing.
2. If any Applications tier instances use a different OracleAS Metadata Repository for their product metadata and DCM repositories, make sure those are up. In short, make sure all Metadata Repositories in your environment are up.

Task 3: Change the Oracle Internet Directory Port

1. On the Oracle Internet Directory host:
 - a. Create a file named `mod.ldif` with the following contents. You can create the file in any directory:

For For Oracle Internet Directory non-SSL port:

```
dn:cn=configset0, cn=osldapd, cn=subconfigsubentry
changetype:modify
replace:orclnonsslport
orclnonsslport:new_nonssl_port_number
```

For For Oracle Internet Directory SSL port:

```
dn:cn=configset0, cn=osldapd, cn=subconfigsubentry
changetype:modify
replace:orclsslport
orclsslport:new_ssl_port_number
```

- b. Run the following command:

For For Oracle Internet Directory non-SSL port:

```
ldapmodify -D cn=orcladmin -w password -p oid_port -f mod.ldif
```

For For Oracle Internet Directory SSL port:

```
ldapmodify -D cn=orcladmin -w password -p oid_port -U SSLAuth -f mod.ldif
```

Note that `oid_port` is the old Oracle Internet Directory port number. If you are changing the Oracle Internet Directory SSL port, provide the additional `-U` argument to specify the SSL authentication mode. Use one of the following values for `SSLAuth`: 1 for no authentication required; 2 for one-way authentication required; 3 for two-way authentication required.

2. On the Oracle Internet Directory host, stop the entire instance that contains Oracle Internet Directory, as well as the Oracle Collaboration Suite Control Console:

```
emctl stop iasconsole
opmnctl stopall
```

3. Perform this step in the Oracle Internet Directory Oracle home. If you have OracleAS Metadata Repository installed in other Oracle homes that are registered with this Oracle Internet Directory, perform this step in each of those Oracle homes as well.

- a. Open the `ldap.ora` file:

```
(UNIX) ORACLE_HOME/ldap/admin/ldap.ora
(Windows) ORACLE_HOME\ldap\admin\ldap.ora
```

- b. Modify the following line to contain the new port number, and then save the file.

```
DIRECTORY_SERVERS=(myhost.myco.com:non_ssl_port:ssl_port)
```

- c. Open the `ias.properties` file:

```
(UNIX) ORACLE_HOME/config/ias.properties
(Windows) ORACLE_HOME\config\ias.properties
```

- d. Change the value of `OIDport` (for an Oracle Internet Directory non-SSL port change) or `OIDsslport` (for an Oracle Internet Directory SSL port change) to the new port number, and then save the file.
4. On the Oracle Internet Directory host, start the instance that contains Oracle Internet Directory, as well as the Oracle Collaboration Suite Control Console:

```
opmnctl startall
emctl start iasconsole
```

5. Perform this step in the OracleAS Single Sign-On Oracle home:
 - a. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
 - b. Run the following command in the OracleAS Single Sign-On Oracle home:

```
ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoca.jar reassoc
-repos $ORACLE_HOME
```

Task 4: Reconfigure OracleAS Certificate Authority

Follow this task if you are using OracleAS Certificate Authority:

1. If OracleAS Certificate Authority is running in a different Oracle home, do the following step in the OracleAS Certificate Authority Oracle home:
 - a. Open the `ias.properties` file:


```
(UNIX) ORACLE_HOME/config/ias.properties
(Windows) ORACLE_HOME\config\ias.properties
```
 - b. Change the value of `OIDport` (for an HTTP port change) or `OIDsslport` (for an HTTPS port change) to the new port number, and then save the file.
2. Update OracleAS Certificate Authority with the new Oracle Internet Directory port number by running the following command in the OracleAS Certificate Authority Oracle home:

```
ocactl changesecurity -server_auth_port port_number
```

In the example, `port_number` is the OracleAS Certificate Authority Server Authentication Virtual Host (SSL) port; the default is 4400.

See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for more information

Task 5: Restart the Identity Management Instance

Restart the Identity Management instance:

```
emctl stop iasconsole
opmnctl stopall
opmnctl startall
emctl start iasconsole
```

Task 6: Update the Applications Tier Instances to Use the New Port Number

On each Applications tier instance that uses the Identity Management installation, run the Change Identity Management Services wizard and start the instance:

1. Using the Oracle Collaboration Suite Control Console, navigate to the Oracle Collaboration Suite home page for the Applications tier instance.

2. Click the **Infrastructure** link.
3. On the Infrastructure page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the new Identity Management information (the new port number).
5. When the wizard is finished, you must perform an opmnctl reload. Enter the following command from the Applications tier (after setting ORACLE_HOME to the Applications tier home):

```
ORACLE_HOME/opmn/bin/opmnctl reload
```
6. Navigate to the Oracle Collaboration Suite home page and start the Applications tier instance by clicking **Start All**.

Changing the HTTP Server Port on Identity Management

This section describes how to change the Oracle HTTP Server HTTP or HTTPS listen port on an Identity Management installation. When you change this port number, you also effectively change the OracleAS Single Sign-On port number. This means you must update any Applications tier instances that use the OracleAS Single Sign-On port.

The following procedure contains complete instructions for updating the Oracle HTTP Server port number on Identity Management, including updating other components in the Infrastructure and updating the Applications tier instances that use the port. The relevant tasks are as follows:

- [Task 1: Prepare the Applications tier Instances](#)
- [Task 2: Prepare the Infrastructure Instances](#)
- [Task 3: Modify the Oracle HTTP Server Listen and Port Directives](#)
- [Task 4: Enable Oracle HTTP Server to Run as Root for Ports Less Than 1024 on UNIX](#)
- [Task 5: Update the Oracle Collaboration Suite Control Console](#)
- [Task 6: Update OracleAS Single Sign-On](#)
- [Task 7: Re-register mod_osso](#)
- [Task 8: Update Oracle Delegated Administration Services](#)
- [Task 9: Update OracleAS Certificate Authority](#)
- [Task 10: Restart the Identity Management Instance](#)
- [Task 11: Restart OracleAS Certificate Authority](#)
- [Task 12: Update the Applications Tier Instances to Use the New Port Number](#)

Task 1: Prepare the Applications tier Instances

Follow this task only if the Identity Management installation is being used by Applications tier instances. On each Applications tier instance that uses Identity Management, stop the Applications tier instance as follows:

1. On the Oracle Collaboration Suite home page of the Oracle Collaboration Suite Control Console, click **Stop All**.
2. Leave the Oracle Collaboration Suite Control Console running.

It is important that you leave the Oracle Collaboration Suite Control Console running in each of the Applications tier instances while you perform this procedure.

Task 2: Prepare the Infrastructure Instances

1. Make sure that Identity Management and its associated OracleAS Metadata Repository are up and running on the Infrastructure whose port number you are changing.
2. If any Applications tier instances use different Metadata Repositories for their product metadata and DCM repositories, make sure those are up. In short, make sure all Metadata Repositories in your environment are up.

Task 3: Modify the Oracle HTTP Server Listen and Port Directives

If you are changing the HTTP port, change both the `Listen` and `Port` directives to the new port number in the Oracle HTTP Server `httpd.conf` file. You can perform this task using the Oracle Collaboration Suite Control Console or manual steps.

- Using the Oracle Collaboration Suite Control Console:
 1. Navigate to the Oracle Collaboration Suite home page and click **Ports**.
 2. On the Ports page, locate the Oracle HTTP Server Listen port and click the icon in the **Configure** column.
 3. On the Server Properties page:
 - Enter the new port number in the **Default Port** field. This is for the `Port` directive.
 - Enter the new port number in the **Listening Port** column. This is for the `Listen` directive. There may be more than one listening port listed. The only way to tell which is the non-SSL listen port is to choose the one with the old non-SSL listen port value.

The values for **Listening Port** and **Default Port** must be the same port number.
 4. At the bottom of the page, click **Apply**.
 5. On the Confirmation page, click **No**, you would not like to restart now.
- Using manual steps:

1. Open the `httpd.conf` file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/httpd.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\httpd.conf
```

2. Update the non-SSL `Listen` and `Port` directives with the new port number, and then save the file.

The value for `Listen` and `Port` must be the same port number, for example, to change the listener port to 7779:

```
Listen 7779
Port 7779
```

There may be multiple `Listen` and `Port` directives in this file. Modify the `Listen` and `Port` directives that are not enclosed in an SSL virtual host container. The easiest way to locate the proper `Listen` and `Port` directives is to search the file for the old port number.

3. Run the following command:

```
dcmctl updateConfig -ct ohs
```

If you are changing the HTTPS port, change both the SSL `Listen` and `Port` directives to the new port number in the Oracle HTTP Server `ssl.conf` file. You must do this using the following manual steps:

1. Open the `ssl.conf` file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/ssl.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\ssl.conf
```

2. Update the SSL `Listen` and SSL `Port` directives with the new port number:

The value for `Listen` and `Port` must be the same port number, for example, to change the listener port to 4445:

```
Listen 4445
Port 4445
```

3. Edit the `<VirtualHost _default_:4443></Virtual>` directive. For example, if you were changing the port number to 4445, you would set the following:

```
<VirtualHost _default_:4445></Virtual>
```

All three directives must be set to use the same port number.

4. Save the `ssl.conf` file.
5. Run the following command:

```
dcmctl updateConfig -ct ohs
```

Task 4: Enable Oracle HTTP Server to Run as Root for Ports Less Than 1024 on UNIX

Perform this task if you are changing the port to a value less than 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Collaboration Suite). On UNIX systems, if you change the Oracle Collaboration Suite non-SSL listen port number to a privileged port (with a value less than 1024), you must enable Oracle HTTP Server to run as root, as follows:

1. Log in as root.
2. Run the following commands in the Infrastructure Oracle home:

```
cd ORACLE_HOME/Apache/Apache/bin
chown root .apachectl
chmod 6750 .apachectl
```

Task 5: Update the Oracle Collaboration Suite Control Console

Update the Oracle Collaboration Suite Control Console with the new port number:

1. Open the `targets.xml` file:

```
(UNIX) ORACLE_HOME/sysman/emd/targets.xml
(Windows) ORACLE_HOME\sysman\emd\targets.xml
```

2. Update each occurrence of the old Oracle HTTP Server listen port number with the new port number, and then save the file.

Depending on your configuration, this file may not contain any occurrences of the Oracle HTTP Server listen port, or it may contain many occurrences. The listen

port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Oracle HTTP Server listen port number, and replace them with the new port number.

3. Reload the Oracle Collaboration Suite Control Console:

```
emctl reload
```

Task 6: Update OracleAS Single Sign-On

Perform this task if OracleAS Single Sign-On is configured to use the Oracle HTTP Server HTTP listen port in the installation where you are changing the port.

1. On UNIX systems, set the LD_LIBRARY_PATH, LD_LIBRARY_PATH_64, or SHLIB_PATH environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
2. Run the following command in the OracleAS Single Sign-On Oracle home:

To change the non-SSL port:

```
(UNIX) ORACLE_HOME/sso/bin/ssocfg.sh http hostname new_non_ssl_port_number
(Windows) ORACLE_HOME\sso\bin\ssocfg.bat http hostname new_non_ssl_port_number
```

To change the SSL port:

```
(UNIX) ORACLE_HOME/sso/bin/ssocfg.sh https hostname new_ssl_port_number
(Windows) ORACLE_HOME\sso\bin\ssocfg.bat https hostname new_ssl_port_number
```

In the example:

- *hostname* is the host on which OracleAS Single Sign-On is running
- *new_port_number* is the new non-SSL Oracle HTTP Server listen port number

Task 7: Re-register mod_osso

Re-register mod_osso as follows:

1. On UNIX systems, set the LD_LIBRARY_PATH, LD_LIBRARY_PATH_64, or SHLIB_PATH environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
2. On Windows systems, set PATH=%PATH%;\$ORACLE_HOME%\bin;%ORACLE_HOME%\lib.
3. Re-register mod_osso to take care of the default partner applications by running the following command in the Identity Management Oracle home:

UNIX:

```
ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path identity_management_oracle_home
-site_name identity_management_hostname:new_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
```

Windows:

```
ORACLE_HOME\sso\bin\ssoreg.bat
-oracle_home_path applications_tier_oracle_home
-site_name identity_management_hostname:new_port_number
```

```
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
```

For example, if you want to change the Oracle HTTP Server listen port to 7779 on host myhost:

```
$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path /disk1/oracleas
-site_name myhost:7779
-config_mod_osso TRUE
-mod_osso_url http://myhost.mydomain:7779
```

4. If you have configured or modified any additional partner applications, you must also re-register those.

See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering mod_osso

Task 8: Update Oracle Delegated Administration Services

If you have Oracle Delegated Administration Services configured, and Oracle Delegated Administration Services uses the new port number, follow these steps to update the Oracle Delegated Administration Services URL entry in Oracle Internet Directory.

You can find out what port Oracle Delegated Administration Services uses with the following command:

```
ldapsearch -h oid_host -p oid_port -D "cn=orcladmin"
-w "password" -b "cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext"
-s base "objectclass=*" orcldasurlbase
```

1. Create a file named mod.ldif with the following contents (you can create the file in any directory):

```
dn:cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
changetype:modify
replace:orcldasurlbase
orcldasurlbase:http://hostname:new_http_port_number/
```

Note the slash at the end of the orcldasurlbase URL.

2. Run the following command:

```
ldapmodify -D cn=orcladmin -w password -p oid_port -f mod.ldif
```

Task 9: Update OracleAS Certificate Authority

If you are using OracleAS Certificate Authority:

1. Re-register OracleAS Certificate Authority with the OracleAS Single Sign-On server by running the following command in the OracleAS Certificate Authority Oracle home:

```
ocactl changesecurity -server_auth_port port_number
```

In the example, *port_number* is the OracleAS Certificate Authority Server Authentication Virtual Host (SSL) port; the default is 4400.

See Also: *Oracle Application Server Certificate Authority Administrator's Guide*

2. If OracleAS Certificate Authority is located in a different Oracle home than the OracleAS Single Sign-On server, restart Oracle HTTP Server and the oca instance in the OracleAS Certificate Authority Oracle home:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl stopproc process-type=oca
opmnctl startproc ias-component=HTTP_Server
opmnctl startproc process-type=oca
```

Task 10: Restart the Identity Management Instance

Restart the Identity Management instance:

```
emctl stop iasconsole
opmnctl stopall
opmnctl startall
emctl start iasconsole
```

Task 11: Restart OracleAS Certificate Authority

If OracleAS Certificate Authority is configured in this instance, restart it:

```
ocactl start
```

Task 12: Update the Applications Tier Instances to Use the New Port Number

Now that you have changed the Oracle HTTP Server port on the Identity Management installation, you must update all Applications tier instances to use the new port number.

1. Update each Applications tier instance using the Change Identity Management wizard in the Oracle Collaboration Suite Control Console. Note that the wizard will not prompt you for the new port number; it retrieves the port number internally.

On each Applications tier instance that uses Identity Management:

- a. Using the Oracle Collaboration Suite Control Console, navigate to the Oracle Collaboration Suite home page for the Applications tier instance.
- b. Click the **Infrastructure** link.
- c. On the Infrastructure page, in the **Identity Management** section, click **Change**.
- d. Follow the steps in the wizard.
- e. When the wizard is finished, you must perform an opmnctl reload. Enter the following command from the Applications tier (after setting ORACLE_HOME to the Applications tier home):

```
ORACLE_HOME/opmn/bin/opmnctl reload
```

- f. Navigate to the Oracle Collaboration Suite home page and start the Applications tier instance by clicking **Start All**.
2. Run the following command on every Applications tier which is hosting an instance of OracleAS Portal:

```
ORACLE_HOME/portal/conf/ptlconfig -dad <dad> -pw <Portal schema password or  
OID Admin Password> -sso [-host <portal_site_name> -port <portal_site_port>  
[-ssl]
```

In the above example, the <dad> should be portal. Use the new Applications tier SSL port number when you specify -port, and be sure to use the -ssl flag if you have enabled SSL.

3. Refresh the Oracle Internet Directory cache in your applications:
 - a. Log in to the Portal.
 - b. Click the Administer tab.
 - c. Click the global settings link.
 - d. Click the SSO/OID tab.
 - e. Check the refresh Oracle Internet Directory cache settings and click **Apply**.

Changing a Hostname, Domain Name, or IP Address

After you have installed Oracle Collaboration Suite, there may come a time when you want to change the hostname, domain name, or IP address of a host. Depending on your installation type, you may perform some or all of these operations.

[Table 14–3](#) summarizes the installation types that support hostname, domain name, and IP address changes, and provides pointers to the appropriate procedures.

Table 14–3 Supported Procedures for Hostname, Domain Name, and IP Address Changes

Installation Type	Changing the Hostname or Domain Name	Changing the IP Address
Applications tier	Supported Refer to "Changing the Hostname or Domain Name of an Applications Tier Installation" on page 14-36	Supported Change the address in your operating system. No updates to Oracle Collaboration Suite are required
Infrastructure tiers hosting both Oracle Internet Directory and OracleAS Metadata Repository	Not supported	Supported Refer to "Changing the IP Address of an Infrastructure Tier" on page 14-46
Infrastructure tiers hosting Oracle Internet Directory only (OracleAS Metadata Repository is not hosted on this Infrastructure tier)	Supported Refer to "Changing the Hostname, Domain Name, or IP Address of an Infrastructure Installation" on page 14-40	Supported Refer to "Changing the IP Address of an Infrastructure Tier" on page 14-46

Changing the Hostname or Domain Name of an Applications Tier Installation

This section describes how to change the hostname, domain name, or both, of an Applications tier host.

The procedure contains the following:

- [Things to Know Before You Start](#)
- [Task 1: Prepare Your Host](#)
- [Task 2: Change the Hostname](#)
- [Task 3: Run the chgiphost Command](#)
- [Task 4: Restart Your Environment](#)
- [Task 5: Update OracleAS Portal and Oracle Mobile Collaboration](#)
- [Task 6: Manually Update the Hostname in Files](#)

Things to Know Before You Start

Review the following items before you start:

- Because the Applications tier instance is registered with Oracle Internet Directory, you must supply the `cn=orcladmin` password during the procedure.
- Consider changing the log level before running the `chgiphost` command so you can view more detailed information.

See Also: ["Setting the Log Level for chgiphost"](#) on page 14-48

- If your old hostname is a string that is likely to appear in a configuration file, the `chgiphost` script may encounter problems when trying to update the configuration files. Refer to ["Customizing the chgiphost Script"](#) on page 14-49 for information on how to avoid this problem.
- Write down the old hostname and IP address before you begin. You will be prompted for these values.
- Oracle recommends that you perform a backup of your environment before you start this procedure. Refer to [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#).

Task 1: Prepare Your Host

Prepare your host for the change by removing instances from OracleAS Clusters and stopping all processes.

1. If the host contains a Applications tier instance that is part of an OracleAS Web Cache cluster, remove the instance from the cache cluster. You can add the instance back into the cluster at the end of the procedure.

See Also: *Oracle Application Server Web Cache Administrator's Guide* for instructions on removing caches from a cache cluster

2. Shut down each instance on the host by running the following commands in each Oracle home:

- On UNIX systems:

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
```

- On Windows systems:

```
ORACLE_HOME\bin\emctl stop iasconsole
ORACLE_HOME\opmn\bin\opmnctl stopall
```

3. Make sure Oracle Collaboration Suite processes will not start automatically after restarting the host by disabling any automated startup scripts you may have set up, such as `/etc/init.d` scripts.
4. Make sure the Oracle Internet Directory that the Applications tier is using is running.

Task 2: Change the Hostname

Update your operating system with the new hostname, domain name, or both. Consult your operating system documentation for more information on how to perform the following steps. You can also change the IP address, if desired.

1. Make the updates to your operating system to properly change the hostname, domain name, or both.
2. Restart the host, if necessary for your operating system.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new hostname to make sure everything is resolving properly.

Task 3: Run the chgiphost Command

Follow these steps for each Applications tier instance on your host. Be sure to complete the steps entirely for one Applications tier instance before you move on to the next.

1. Log in to the host as the user that installed the Applications tier instance.
2. Make sure your ORACLE_HOME environment variable is set to the Applications tier Oracle home.
3. On UNIX systems, set the LD_LIBRARY_PATH, LD_LIBRARY_PATH_64, or SHLIB_PATH environment variables to the proper values, as shown in [Table 1-1](#), "Oracle Collaboration Suite Environment Variables for UNIX" on page 1-2. The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
4. Run the following commands in the Applications tier Oracle home:

- On UNIX systems:

```
cd ORACLE_HOME/chgip/scripts
./chgiphost.sh -mid
```

- On Windows systems:

```
cd ORACLE_HOME\chgip\scripts
chgiphost.bat -mid
```

The chgiphost command prompts for information, as shown in [Table 14-4](#). Note that the prompts may provide values in parentheses. You can enter a different value, or press the return key to accept the suggested value.

Table 14-4 Prompts and Actions for chgiphost -mid

Prompt	Action
Enter fully qualified hostname (hostname.domainname) of destination	Enter the new fully-qualified hostname. This may be a new hostname, domain name, or both.
Enter valid IP Address of destination	If you changed the IP address of the host, enter the new IP address. Otherwise, enter the current IP address.
Enter valid IP Address of source	If you changed the IP address of the host, enter the old IP address. Otherwise, enter the current IP address.
OIDAdmin Password:	Enter the cn=orcladmin password for the Oracle Internet Directory in which this Applications tier instance is registered.

5. Verify that the tool ran successfully by checking for errors in the files in the following directory:

- On UNIX systems:

```
ORACLE_HOME/chgip/log
```

- On Windows systems:

```
ORACLE_HOME\chgif\log
```

Task 4: Restart Your Environment

Restart the Applications tier instances and restore your configuration back to the way it was before you started the procedure.

1. Start each Applications tier instance on your host by running the following commands in each Oracle home:

- On UNIX systems:

```
ORACLE_HOME/opmn/bin/opmnctl startall
ORACLE_HOME/bin/emctl start iasconsole
```

- On Windows systems:

```
ORACLE_HOME\opmn\bin\opmnctl startall
ORACLE_HOME\bin\emctl start iasconsole
```

2. If you removed any instances from an OracleAS Web Cache cluster at the beginning of this procedure, add them back to the cache cluster.

See Also: *Oracle Application Server Web Cache Administrator's Guide* for instructions on adding caches to a cluster

3. If you disabled any processes for automatically starting Oracle Collaboration Suite at the beginning of this procedure, enable them.

Task 5: Update OracleAS Portal and Oracle Mobile Collaboration

This is a special step required for updating OracleAS Portal and Oracle Mobile Collaboration when you change the hostname.

When you change the hostname, the Oracle Mobile Collaboration server URL changes to use the new hostname. You must update the Oracle Internet Directory Service Registry with the new Oracle Mobile Collaboration service URL in order for other applications, such as OracleAS Portal, to access Oracle Mobile Collaboration.

Refer to ["Managing the Oracle Internet Directory Service Registry"](#) on page 7-7 for instructions on updating the Oracle Internet Directory Service Registry.

After making this change, if you are using Oracle Collaborative Portlets, you must re-run the Collaborative Portlets Configuration Assistant. This will rebuild the portlets with the new hostname connection information.

Refer to ["Changing the Host or Port on an Applications Tier hosting Oracle Collaborative Portlets"](#) on page 5-43 for instructions on running the Collaborative Portlets Configuration Assistant.

Task 6: Manually Update the Hostname in Files

If you edited a file and entered the hostname as part of a user-defined parameter such as the Oracle home path, the hostname is not automatically updated by running the `chgifhost.sh` script. To update the hostname in such cases, you need to edit the files manually. For example, the `plsql.conf` file may contain an NFS path including the hostname, such as: `/net/dsun1/private/...`

The `chgifhost.sh` script also does not edit the hostname references in the documentation files. You will need to manually edit these files to update the

hostname. Examples of such files are the following files in the *ORACLE_HOME*/Apache/Apache/htdocs directory.

- index.html.de
- index.html.es_ES
- index.html.fr
- index.html.it
- index.html.ja
- index.html.ko
- index.html.pt_BR
- index.html.zh_CN
- index.html.zh_TW

Changing the Hostname, Domain Name, or IP Address of an Infrastructure Installation

This section describes how to change the hostname, domain name, or IP address on an Infrastructure host that contains an Identity Management installation. This procedure applies to any Identity Management-only installation.

The procedure contains the following:

- [Things to Know Before You Start](#)
- [Task 1: Shut Down Applications Tier Instances](#)
- [Task 2: Prepare Your Infrastructure Host](#)
- [Task 3: Change the Hostname or IP Address](#)
- [Task 4: Start Oracle Internet Directory](#)
- [Task 5: Run the chgiphost Command](#)
- [Task 6: Update Your Environment](#)
- [Task 7: Restart Your Environment](#)

Things to Know Before You Start

Review the following items before you start the procedure:

- Consider changing the log level before running the chgiphost command so you can view more detailed information.

See Also: ["Setting the Log Level for chgiphost"](#) on page 14-48

- If your old hostname is a string that is likely to appear in a configuration file, the chgiphost script may encounter problems when trying to update the configuration files. Refer to ["Customizing the chgiphost Script"](#) on page 14-49 for information on how to avoid this problem.
- Write down the old hostname and IP address before you begin. You will be prompted for these values.
- Oracle recommends that you perform a backup of your environment before you start this procedure. Refer to [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#).

Task 1: Shut Down Applications Tier Instances

For each Applications tier instance that uses Identity Management, stop the Applications tier instance as follows:

1. On the Oracle Collaboration Suite home page of the Oracle Collaboration Suite Control Console, select **Stop All**.
2. Leave the Oracle Collaboration Suite Control running.

It is important that you leave the Oracle Collaboration Suite Control running in each of the Applications tier instances while you perform this procedure.

Task 2: Prepare Your Infrastructure Host

Prepare your Infrastructure host for the hostname change by stopping all processes.

1. Set the `ORACLE_HOME` environment variable.
2. Shut down the Identity Management installation:
 - On UNIX systems:


```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
```
 - On Windows systems:


```
ORACLE_HOME\bin\emctl stop iasconsole
ORACLE_HOME\opmn\bin\opmnctl stopall
```
3. Make sure Oracle Collaboration Suite processes will not start automatically after a restart the host by disabling any automated startup scripts you may have set up, such as `/etc/init.d` scripts.

Task 3: Change the Hostname or IP Address

Update your operating system with the new hostname, domain name, or IP address. Consult your operating system documentation for more information on how to perform the following steps.

1. Make the updates to your operating system to properly change hostname, domain name, or both.
2. Restart the host, if necessary for your operating system.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new hostname to make sure everything is resolving properly.

Task 4: Start Oracle Internet Directory

Start the Oracle Internet Directory:

- On UNIX systems:


```
ORACLE_HOME/opmn/bin/opmnctl start
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OID
```
- On Windows systems:


```
ORACLE_HOME\opmn\bin\opmnctl start
ORACLE_HOME\opmn\bin\opmnctl startproc ias-component=OID
```

Task 5: Run the chgiphost Command

Perform these steps using the Infrastructure Oracle home:

1. Log in to the host as the user that installed the Infrastructure tier.
2. Set the `ORACLE_HOME` and `ORACLE_SID` environment variables.
3. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1-1, "Oracle Collaboration Suite Environment Variables for UNIX"](#) on page 1-2. The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
4. Run the following commands in the Infrastructure Oracle home:

- On UNIX systems:

```
cd ORACLE_HOME/chgip/scripts
./chgiphost.sh -idm
```

- On Windows systems:

```
cd ORACLE_HOME\chgip\scripts
chgiphost.bat -idm
```

The `chgiphost` command prompts for information, as shown in [Table 14-5](#). Note that the prompts may provide values in parentheses. You can enter a different value, or press the return key to accept the suggested value.

Table 14-5 Prompts and Actions for `chgiphost -idm`

Prompt	Action
Enter fully qualified hostname (hostname.domainname) of destination	If you changed the hostname or domain name on your system, enter the new fully-qualified hostname. Otherwise, enter the current fully-qualified hostname.
Enter fully qualified hostname (hostname.domainname) of source	If you changed the hostname or domain name on your system, enter the old fully-qualified hostname. Otherwise, enter the current fully-qualified hostname.
Enter valid IP Address of destination	If you changed the IP address of the system, enter the new IP address. Otherwise, enter the current IP address
Enter valid IP Address of source	If you changed the IP address of the system, enter the old IP address. Otherwise, enter the current IP address

5. Verify that the tool ran successfully by checking for errors in the files in the following directory:

- On UNIX systems:

```
ORACLE_HOME/chgip/log
```

- On Windows systems:

```
ORACLE_HOME\chgip\log
```

Task 6: Update Your Environment

This task contains the steps to update your environment for the new hostname, domain name, or IP address.

1. Update the `ldap.ora` file in each Applications tier instance (J2EE and Web Cache, Portal and Wireless, and Oracle Business Intelligence) that uses Oracle Internet Directory.

In each Oracle home:

- a. Edit the following file:

```
(UNIX) ORACLE_HOME/ldap/admin/ldap.ora
(Windows) ORACLE_HOME\ldap\admin\ldap.ora
```

- b. Update the `DIRECTORY_SERVERS` parameter with the new fully-qualified hostname.

2. Run the following command (*ORACLE_HOME* in the Infrastructure Oracle home):

- On UNIX systems:

```
ORACLE_HOME/jdk/bin/java -jar ORACLE_HOME/sso/lib/ossoca.jar reassoc -repos
ORACLE_HOME
```

```
ORACLE_HOME/jdk/bin/java -jar ORACLE_HOME/sso/lib/ossoca.jar reassoc
-midtier ORACLE_HOME old_hostname new_hostname
```

- On Windows systems:

```
ORACLE_HOME\jdk\bin\java -jar ORACLE_HOME\sso\lib\ossoca.jar reassoc -repos
ORACLE_HOME
```

```
ORACLE_HOME\jdk\bin\java -jar ORACLE_HOME\sso\lib\ossoca.jar reassoc
-midtier ORACLE_HOME old_hostname new_hostname
```

3. Run the following command to update Oracle Directory Integration and Provisioning:

- On UNIX systems:

```
ORACLE_HOME/bin/odisrvreg -h OID_hostname -p OID_port -D "cn=orcladmin" -w
orcladmin_password
```

- On Windows systems:

```
ORACLE_HOME\bin\odisrvreg -h OID_hostname -p OID_port -D "cn=orcladmin" -w
orcladmin_password
```

4. Follow these steps to update the Oracle Delegated Administration Services URL entry in Oracle Internet Directory.

- a. Create a file named `mod.ldif` with the following contents (you can create the file in any directory):

```
dn:cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
changetype:modify
replace:orcldasurlbase
orcldasurlbase:http://hostname:http_port_number/
```

Where *hostname* is the new hostname and *http_port_number* is the Oracle HTTP Server port for the Infrastructure installation. Note the slash at the end of the `orcldasurlbase` URL.

- b. Run the following command:

```
ldapmodify -D cn=orcladmin -w password -p OID_port -f mod.ldif
```

5. In each Applications tier installation, run the Change Identity Management Services wizard:

- a. Using the Oracle Collaboration Suite Control Console, navigate to the Oracle Collaboration Suite home page for the Applications tier instance.

- b. Select the **Infrastructure** link.
- c. On the Infrastructure page, in the Identity Management section, select **Change**.
- d. Follow the steps in the wizard for supplying the new Identity Management information.

Task 7: Restart Your Environment

Restart the Infrastructure installation and restore your configuration back to the way it was before you started the procedure.

1. Restart the Identity Management instance:

- On UNIX systems:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/opmn/bin/opmnctl startall
ORACLE_HOME/bin/emctl start iasconsole
```

- On Windows systems:

```
ORACLE_HOME\opmn\bin\opmnctl stopall
ORACLE_HOME\opmn\bin\opmnctl startall
ORACLE_HOME\bin\emctl start iasconsole
```

2. If you disabled any processes for automatically starting Oracle Collaboration Suite at the beginning of this procedure, enable them.
3. Start all Applications tier instances.

Configuration 1: Oracle Internet Directory only

1. Update the `ldap.ora` file in every instance that uses Oracle Internet Directory. This includes other Identity Management instances (OracleAS Single Sign-On, Oracle Delegated Administration Services, Oracle Directory Integration and Provisioning) and Applications tier instances (J2EE and Web Cache, Portal and Wireless, and Oracle Business Intelligence).

In each Oracle home:

- a. Edit the following file:

```
(UNIX) ORACLE_HOME/ldap/admin/ldap.ora
(Windows) ORACLE_HOME\ldap\admin\ldap.ora
```

- b. Update the `DIRECTORY_SERVERS` parameter with the new fully-qualified hostname.

2. In the OracleAS Single Sign-On installation, run the Change Identity Management Services wizard and supply the new Oracle Internet Directory information:
 - a. Using the Oracle Collaboration Suite Control Console, navigate to the Oracle Collaboration Suite home page for OracleAS Single Sign-On.
 - b. Click the **Infrastructure** link.
 - c. On the Infrastructure page, in the Identity Management section, click **Change**.
 - d. Follow the steps in the wizard for supplying the new Identity Management information (new hostname).

3. In each Applications tier installation, run the Change Identity Management Services wizard and supply the new Oracle Internet Directory information, as described in the preceding step.

Configuration 2: OracleAS Single Sign-On, Oracle Delegated Administration Services, and (optionally) Oracle Directory Integration and Provisioning

1. Run the following command (*ORACLE_HOME* is the OracleAS Single Sign-On Oracle home):

- On UNIX systems:

```
ORACLE_HOME/jdk/bin/java -jar ORACLE_HOME/sso/lib/ossoca.jar reassoc
-midtier ORACLE_HOME old_hostname new_hostname
```

- On Windows systems:

```
ORACLE_HOME\jdk\bin\java -jar ORACLE_HOME\sso\lib\ossoca.jar reassoc
-midtier ORACLE_HOME old_hostname new_hostname
```

2. Re-register OracleAS Single Sign-On (*ORACLE_HOME* is the OracleAS Single Sign-On Oracle home):

- On UNIX systems:

```
ORACLE_HOME/jdk/bin/java -jar ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path applications_tier_oracle_home
-site_name applications_tier_hostname:http_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-u user
```

- On Windows systems:

```
ORACLE_HOME\jdk\bin\java -jar ORACLE_HOME\sso\lib\ossoreg.jar
-oracle_home_path applications_tier_oracle_home
-site_name applications_tier_hostname:http_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-u user
```

See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on running the preceding command

3. If Oracle Directory Integration and Provisioning is configured, run the following command:

- On UNIX systems:

```
ORACLE_HOME/bin/odisrvreg -h OID_hostname -p OID_port -D "cn=orcladmin" -w
orcladmin_password
```

- On Windows systems:

```
ORACLE_HOME\bin\odisrvreg -h OID_hostname -p OID_port -D "cn=orcladmin" -w
orcladmin_password
```

4. If you have Oracle Delegated Administration Services configured, follow these steps to update the Oracle Delegated Administration Services URL entry in Oracle Internet Directory.
 - a. Create a file named *mod.ldif* with the following contents (you can create the file in any directory):

```
dn:cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
changetype:modify
replace:orcldasurlbase
orcldasurlbase:http://hostname:http_port_number/
```

Where *hostname* is the new hostname and *http_port_number* is the Oracle HTTP Server port for the Identity Management installation. Note the slash at the end of the `orcldasurlbase` URL.

- b. Run the following command:

```
ldapmodify -D cn=orcladmin -w password -p OID_port -f mod.ldif
```

5. In each Applications tier installation (J2EE and Web Cache, Portal and Wireless, or Oracle Business Intelligence), run the Change Identity Management Services wizard:
- Using the Oracle Collaboration Suite Control Console, navigate to the Oracle Collaboration Suite home page for the Applications tier instance.
 - Click the **Infrastructure** link.
 - On the Infrastructure page, in the Identity Management section, click **Change**.
 - Follow the steps in the wizard for supplying the new Identity Management information.

Changing the IP Address of an Infrastructure Tier

This section describes how to change the IP address of a Infrastructure tier. The procedure contains the following:

- [Things to Know Before You Start](#)
- [Task 1: Shut Down Applications Tier Instances](#)
- [Task 2: Prepare Your Infrastructure Host](#)
- [Task 3: Change the IP Address](#)
- [Task 4: Update the Infrastructure](#)
- [Task 5: Restart Your Environment](#)

Things to Know Before You Start

Review the following items before you start the procedure:

- Write down the old IP address before you begin. You will be prompted for this during the procedure.
- Oracle recommends that you perform a backup of your environment before you start this procedure. Refer to [Chapter 11, "Backing Up and Recovering Oracle Collaboration Suite"](#).

Task 1: Shut Down Applications Tier Instances

Shut down all Applications tier instances that use the Infrastructure installation, even if they are on other hosts.

Task 2: Prepare Your Infrastructure Host

Prepare your Infrastructure host for the change by stopping all processes.

1. Set the `ORACLE_HOME` and `ORACLE_SID` environment variables.

2. Shut down the Infrastructure:

```
emctl stop iasconsole
opmnctl stopall
lsnrctl stop

sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
SQL> quit
```

3. Verify that all Oracle Collaboration Suite processes have stopped.**4. Make sure Oracle Collaboration Suite processes will not start automatically after a restarting the host by disabling any automated startup scripts you may have set up, such as `/etc/init.d` scripts.****Task 3: Change the IP Address**

Update your operating system with the new IP address, restart the host, and verify that the host is functioning properly on your network. Consult your operating system documentation for more information on how to do this.

1. Make the updates to your operating system to properly change the IP address.
2. Restart the host, if required by your operating system.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new IP address to make sure everything is resolving properly.

Task 4: Update the Infrastructure

Update the Infrastructure on your host with the new IP address.

1. Log in to the host as the user that installed the Infrastructure.
2. Set the `ORACLE_HOME` and `ORACLE_SID` environment variables.
3. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1-1, "Oracle Collaboration Suite Environment Variables for UNIX"](#) on page 1-2. The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
4. Start the database:

```
sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> startup
SQL> quit
```

```
lsnrctl start
```

5. Start OPMN:

```
opmnctl start
```

6. Start Oracle Internet Directory:

```
opmnctl startproc ias-component=OID process-type=OID
```

7. Run the following commands in the Infrastructure Oracle home:

```
(UNIX)
cd $ORACLE_HOME/chgip/scripts
```

```
./chgiphost.sh -infra
```

(Windows)

```
cd ORACLE_HOME\chgif\scripts
chgiphost.bat -infra
```

The `chgiphost` command prompts for the old and new IP address.

8. Verify that the tool ran successfully by checking for errors in the files in the following directory:

```
ORACLE_HOME/chgif/log
```

Task 5: Restart Your Environment

Finish starting the Infrastructure and start any Applications tier instances that use it.

1. Finish starting the Infrastructure:

```
opmnctl startall
emctl start iasconsole
```

2. If a Applications tier instance is on the same host as the infrastructure, then you need to run the `chgiphost` script on the Applications tier instance before restarting the Applications tier processes. See ["Changing Applications Tier Ports"](#) on page 14-2 for details.
3. If you disabled any processes for automatically starting Oracle Collaboration Suite at the beginning of this procedure, enable them.

Special Topics for Changing Your Hostname or Domain Name

This section contains the following special topics that apply to changing the hostname or domain name of an Oracle Collaboration Suite host:

- [Setting the Log Level for chgifhost](#)
- [Customizing the chgifhost Script](#)
- [Changing your Hostname after Upgrading from Windows 2000 to Windows 2003](#)
- [Recovering from Errors When Changing Your Hostname](#)

Setting the Log Level for chgifhost

By default, the console log level for the `chgiphost` command is `SEVERE`. This causes only critical information to be printed while running `chgiphost`. If you would like to view additional progress information, set the console log level to `CONFIG` as follows:

Note: See [Table 14-6](#) for a complete listing of standard Java log levels, which you can use for configuring the log level.

1. Edit the following file:

```
(UNIX) ORACLE_HOME/chgif/config/chgif.log.properties
(Windows) ORACLE_HOME\chgif\config\chgif.log.properties
```

2. Change the `java.util.logging.ConsoleHandler.level` parameter to `CONFIG`:

```
java.util.logging.ConsoleHandler.level = CONFIG
```

Table 14–6 Log Levels Supported for chgiphost

Log Level	Description
ALL	Special level that indicates all messages should be logged
SEVERE	Serious failure notices will be logged
WARNING	Potential errors will be logged
INFO	Informational messages will be logged
CONFIG	Static configuration messages will be logged
FINE	Tracing information will be logged
FINER	Detailed tracing information will be logged
FINEST	Highly detailed tracing information will be logged
OFF	Special level used to turn off all logging

Note: The log-levels are different for the log-file and the console (stdout). Since the log level for the console is SEVERE by default, only SEVERE-level messages and above will be passed. However, in the log file (where the default FileHandler level is CONFIG), all messages with level CONFIG and above are logged. chgiphost does not use levels FINE and below, so for chgiphost purposes, all messages will be logged in the log file.

Customizing the chgiphost Script

By default, the chgiphost script updates key configuration files in the Oracle home with the new hostname. If either of the following cases apply to your installation, you may want to consider customizing the behavior of the chgiphost script:

- You have created additional configuration files that contain the hostname and would like the chgiphost script to update those files.

In order to update these files, add their full path name to the following file before running chgiphost:

- On UNIX systems:

`ORACLE_HOME/chgip/config/hostname.lst`

- On Windows systems:

`ORACLE_HOME\chgip\config\hostname.lst`

- Your old hostname is very short (one or two letters) or is a string that is likely to appear in a configuration file

Before running chgiphost, examine each of the files listed in `hostname.lst` to determine if the old hostname exists in any settings in those files. If you find a match, you can correct those settings after you run chgiphost.

- Your Oracle home contains the hostname in its full path.

In this case, the chgiphost script may not update your configuration files properly. You can avoid this problem by using a Java utility called FileFixer, which searches for specific text strings in a file by matching regular expressions, and updates them to their new values. Note that FileFixer searches for patterns one line at a time. It cannot match patterns across lines.

To use FileFixer:

1. Make a copy of the following file:

- On UNIX systems:

```
ORACLE_HOME/chgip/config/hostname_short_sample.lst.xml
```

- On Windows systems:

```
ORACLE_HOME\chgip\config\hostname_short_sample.lst.xml
```

2. Edit your copy of the file to specify the regular expression matching required for your old and new hostnames. The file contains an example of how to do this.

3. Specify the file when running the `chgiphost` script:

```
chgiphost option -hostnameShortXml full_path_to_your_xml_file
```

For example, if you named your file `/mydir/my_sample.lst.xml`, and you are updating a Applications tier installation, run `chgiphost` as follows:

```
chgiphost -mid -hostnameShortXml /mydir/my_sample.lst.xml
```

Changing your Hostname after Upgrading from Windows 2000 to Windows 2003

When you upgrade from Windows 2000 to Windows 2003, lower-case letters in your hostname may be changed to upper-case letters. For example, if your hostname is "myhost" before the upgrade, it may be changed to "MYHOST". If this occurs, some Oracle Collaboration Suite processes may not function properly.

To resolve this problem, you do not need to run the `chgiphost` command to update Oracle Collaboration Suite. Add an entry with the lower-case hostname to the hosts file:

```
OS_path\system32\drivers\etc\hosts
```

For example, if your fully-qualified hostname was `myhost.mydomain` before the upgrade, and your IP address is 1.2.3.4, add the following line:

```
1.2.3.4 myhost.mydomain myhost
```

Recovering from Errors When Changing Your Hostname

This section describes how to recover from typical errors you might encounter when using the `chgiphost.sh` script. It contains the following scenarios:

- [Scenario 1: You Specified the Wrong Destination Name](#)
- [Scenario 2: You Encountered an Error when Running `chgiphost.sh`](#)

Scenario 1: You Specified the Wrong Destination Name

Suppose you ran the `chgiphost.sh` script but specified the wrong destination name. In this case, you can remedy the error by running `chgiphost.sh` again. Here are the details.

Suppose the current source hostname is `loire985`, the incorrect destination hostname you specified is `mqa985`, and the correct destination hostname is `sqb985`. Initially, you ran `chgiphost.sh` with `source = loire985` and `destination = mqa985`.

To recover from this error:

1. Run `chgiphost.sh` with `source = mqa985` and `destination = sqb985`.
2. Run `chgiphost.sh` again with `source = loire985` and `destination = sqb985`.

Scenario 2: You Encountered an Error when Running `chgiphost.sh`

For example, you will get an error message if you enter the wrong password for Oracle Internet Directory. In this case, you should run `chgiphost.sh` again, with the same source and destination hostnames as before, and make sure to supply the correct password when prompted.

If you encounter an error when running `chgiphost.sh`, you should fix the error and run `chgiphost.sh` again.

Customizing Oracle Collaboration Suite

You can make various customizations to the logos, colors, and fonts used in various Oracle Collaboration Suite interfaces.

- [Customizing Default Logos](#)
- [Customizing Colors and Fonts](#)
- [Customizing Oracle Content Services](#)
- [Customizing Oracle Real-Time Collaboration](#)
- [Customizing and Extending Oracle Web Access Client](#)

Customizing Default Logos

This section tells you how to customize the default logos for various components of Oracle Collaboration Suite. It contains the following topics:

- [Replacing the Default Logo on the Oracle Collaboration Suite Portal Home Page](#)
- [Customizing the Oracle WebMail Logo](#)
- [Customizing the Oracle Web Conferencing Logo](#)
- [Customizing the Oracle Mobile Collaboration & Voice Logo](#)

Replacing the Default Logo on the Oracle Collaboration Suite Portal Home Page

You can replace the default logo on the Oracle Collaboration Suite Portal home page with a custom image of your choosing.

To replace the default logo on the Oracle Collaboration Suite Portal home page:

1. Log in to Portal as an administrator (such as `orcladmin`)
2. Select the **Navigator** global button
3. Select the **Page Groups** tab
4. Click the **Oracle Collaboration Suite** link
5. Click the **Navigation Pages** link
6. Locate "Oracle Collaboration Suite:Banner" and click the **edit** link next to it
7. Locate the region containing the default Oracle Collaboration Suite logo, and select the **Edit** icon immediately to the left of the logo image
8. On the **Item Attributes** screen, select **Browse** to upload a custom logo image
9. When you have finished, select **OK** to save your settings.

Customizing the Oracle WebMail Logo

Follow the steps outlined below to replace the default corporate and product branding logos in Oracle WebMail with custom images. Note that these steps must be performed on all Applications tiers where Oracle WebMail is configured.

1. Locate the directory where the Oracle WebMail logo images are stored:

On UNIX systems:

```
ORACLE_HOME/j2ee/OC4J_OCSCClient/images
```

On Windows systems:

```
ORACLE_HOME\j2ee\OC4J_OCSCClient\images
```

2. Back up the default corporate and product branding logos:

On UNIX systems:

```
cp ocs_brand_header.gif ocs_brand_header.gif.backup
cp mail_subbrand.gif mail_subbrand.gif.backup
```

On Windows systems:

```
copy ocs_brand_header.gif ocs_brand_header.gif.backup
copy mail_subbrand.gif mail_subbrand.gif.backup
```

3. Replace the default corporate and product branding logos with custom images (substitute actual image file names for custom_corporate_logo.gif and custom_product_logo.gif):

On UNIX systems:

```
cp custom_corporate_logo.gif ocs_brand_header.gif
cp custom_product_logo.gif mail_subbrand.gif
```

On Windows systems:

```
copy custom_corporate_logo.gif ocs_brand_header.gif
copy custom_product_logo.gif mail_subbrand.gif
```

4. Another copy of the image is stored in `/um/admin/pages`. You should replace this image with your custom image as well.
5. After placing a new image, you must restart OracleAS WebCache in order for the new image to be loaded into the cache. Until you restart OracleAS WebCache, clients accessing the image will continue to load the cached, older version of the image.

Customizing the Oracle Calendar Logo

Follow the steps outlined below to replace the default corporate and product branding logos in the Oracle Calendar Web client with custom images. Note that these steps must be performed on all Applications tiers where Oracle Calendar is configured.

1. Locate all directories where Oracle Calendar logo images are stored:

On UNIX systems:

```
ORACLE_HOME/ocas/htdocs/ocas/american/banners
ORACLE_HOME/ocas/htdocs/ocas/brazilian_portuguese/banners
ORACLE_HOME/ocas/htdocs/ocas/danish/banners
...
```

```
ORACLE_HOME/ocas/htdocs/ocwc/american/banners
ORACLE_HOME/ocas/htdocs/ocwc/brazilian_portugese/banners
ORACLE_HOME/ocas/htdocs/ocwc/danish/banners
...
```

On Windows systems:

```
ORACLE_HOME\ocas\htdocs\ocas\american\banners
ORACLE_HOME\ocas\htdocs\ocas\brazilian_portugese\banners
ORACLE_HOME\ocas\htdocs\ocas\danish\banners
...
ORACLE_HOME\ocas\htdocs\ocwc\american\banners
ORACLE_HOME\ocas\htdocs\ocwc\brazilian_portugese\banners
ORACLE_HOME\ocas\htdocs\ocwc\danish\banners
...
```

2. In each directory corresponding to the language(s) for which the logo is to be customized, back up the default branding logo:

On UNIX systems:

```
cp calendar_subbrand.gif calendar_subbrand.gif.backup
```

On Windows systems:

```
copy calendar_subbrand.gif calendar_subbrand.gif.backup
```

3. Replace the default logo with a custom image (substitute actual image file name for `custom_product_logo.gif`):

On UNIX systems:

```
cp custom_product_logo.gif calendar_subbrand.gif
```

On Windows systems:

```
copy custom_product_logo.gif calendar_subbrand.gif
```

Customizing the Oracle Web Conferencing Logo

Follow the steps outlined below to replace the default corporate and product branding logos in Oracle Web Conferencing with custom images. Note that these steps must be performed on all Applications tiers where Oracle Web Conferencing is configured.

1. Locate the directory where Oracle Web Conferencing logo images are stored:

On UNIX systems:

```
ORACLE_HOME/j2ee/OC4J_imeeting/applications/imeeting/imtapp/res/media
```

On Windows systems:

```
ORACLE_HOME\j2ee\OC4J_imeeting\applications\imeeting\imtapp\res\media
```

2. Back up the default corporate and product branding logos:

On UNIX systems:

```
cp oracle_ocs_corp.gif oracle_ocs_corp.gif.backup
cp imt_ocs_prod.gif imt_ocs_prod.gif.backup
```

On Windows systems:

```
copy oracle_ocs_corp.gif oracle_ocs_corp.gif.backup
```

```
copy imt_ocs_prod.gif imt_ocs_prod.gif.backup
```

3. Replace the default corporate and product branding logos with custom images (substitute actual image file names for `custom_corporate_logo.gif` and `custom_product_logo.gif`):

On UNIX systems:

```
cp custom_corporate_logo.gif oracle_ocs_corp.gif
cp custom_product_logo.gif imt_ocs_prod.gif
```

On Windows systems:

```
copy custom_corporate_logo.gif oracle_ocs_corp.gif
copy custom_product_logo.gif imt_ocs_prod.gif
```

Customizing the Oracle Mobile Collaboration & Voice Logo

Follow the steps outlined below to replace the default corporate and product branding logos in the Oracle Mobile Collaboration & Voice setup pages with custom images. Note that these steps must be performed on all Applications tiers where Oracle Mobile Collaboration & Voice is configured.

1. Locate the directory where the Oracle Mobile Collaboration & Voice setup images are stored:

On UNIX systems:

```
ORACLE_HOME/j2ee/OC4J_Portal/applications/marconi/marconi-web/images
```

On Windows systems:

```
ORACLE_HOME\j2ee\OC4J_Portal\applications\marconi\marconi-web\images
```

2. Back up the default logo:

On UNIX systems:

```
cp ocs_brand_header.gif ocs_brand_header.gif.backup
```

On Windows systems:

```
copy ocs_brand_header.gif ocs_brand_header.gif.backup
```

3. Replace the default logo with a custom image (substitute the actual image file name for `custom_corporate_logo.gif`):

On UNIX systems:

```
cp custom_corporate_logo.gif ocs_brand_header.gif
```

On Windows systems:

```
copy custom_corporate_logo.gif ocs_brand_header.gif
```

Customizing Colors and Fonts

This section tells you how to customize the colors and fonts of various Oracle Collaboration Suite components. It contains the following topics:

- [Changing the Default Colors and Fonts on the Oracle Collaboration Suite Portal Home Page](#)

- [Customizing Oracle WebMail Colors and Fonts](#)
- [Customizing Oracle Web Conferencing Colors and Fonts](#)
- [Customizing Oracle Mobile Collaboration & Voice Colors and Fonts](#)

Changing the Default Colors and Fonts on the Oracle Collaboration Suite Portal Home Page

To change default colors and fonts on the Portal home page, follow these instructions:

1. Log in to Portal as an administrator (e.g. orcladmin)
2. Click the **Builder** global button
3. Click the **Navigator** global button
4. Locate the **Oracle Collaboration Suite** page group, and click the **Contents** link.
5. Click the **Styles** link
6. Locate the `OCSHomePageStyle` style, and click the **Edit** link
7. Use the Portal style editor tool to customize the appearance of the Portal home page:
 - a. Use the **Style Element Type** drop-down list to view style settings for various style elements (Common, Portlets, Tabs, and Items)
 - b. Within each style element type, use the Style Element Properties tool to customize style properties
 - c. Click the **Apply** button to apply your changes and preview the result in the Preview section

Customizing Oracle WebMail Colors and Fonts

To change the default colors and fonts in Oracle WebMail, change the style properties in the appropriate `.xss` XML stylesheet files.

To change the administration UI, edit the following file:

```
ORACLE_HOME/j2ee/OC4J_OCSCClient/applications/VMAdminApp/vmadmin_
client/cabo/styles/blaf.xss
```

To change the end-user UI, edit the following file:

```
ORACLE_HOME/j2ee/OC4J_OCSCClient/applications/UMClientApp/um_
client/cabo/styles/blaf.xss
```

Customizing Oracle Calendar Colors and Fonts

To change the default colors and fonts in Oracle Calendar, change the style properties in the OCAS and OCWC `.css` Cascading Style Sheet files. Make your changes to all of the files corresponding to the languages which your users will use.

For OCAS, change the style properties in the following files:

```
ORACLE_HOME/ocas/htdocs/ocas/american/stylesheet/swcdefault.css
ORACLE_HOME/ocas/htdocs/ocas/french/stylesheet/swcdefault.css
ORACLE_HOME/ocas/htdocs/ocas/german/stylesheet/swcdefault.css
...
```

For OCWC, change the style properties in the following files:

```
ORACLE_HOME/ocwc/htdocs/ocas/american/stylessheet/swcdefault.css
ORACLE_HOME/ocwc/htdocs/ocas/french/stylessheet/swcdefault.css
ORACLE_HOME/ocwc/htdocs/ocas/german/stylessheet/swcdefault.css
...
```

Customizing Oracle Web Conferencing Colors and Fonts

To change the default colors and fonts in Oracle Web Conferencing, change the style properties in the following .xss XML stylesheet files.

For the Oracle Web Conferencing end-user UI:

```
ORACLE_HOME/j2ee/OC4J_immeeting/applications/immeeting/imtapp/cabo/styles/blaf.xss
```

For the Oracle Web Conferencing help system:

```
ORACLE_HOME/j2ee/OC4J_immeeting/applications/immeeting/imthelp/cabo/styles/blaf.xss
```

Customizing Oracle Mobile Collaboration & Voice Colors and Fonts

To change the default colors and fonts in the Oracle Mobile Collaboration & Voice Web UI, change the style properties in the following .xss XML stylesheet files.

For the multi-channel application setup pages:

```
ORACLE_HOME/j2ee/OC4J_
Wireless/applications/modules/modules-web/cabo/styles/blaf.xss
```

For the Web client common pages:

```
ORACLE_HOME/j2ee/OC4J_
Portal/applications/webclient-common/webclient-common-web/cabo/styles/blaf.xss
```

For the Oracle Mobile Collaboration & Voice setup wizard pages:

```
ORACLE_HOME/j2ee/OC4J_Portal/applications/marconi/marconi-web/cabo/styles/blaf.xss
```

For the Oracle Mobile Collaboration & Voice administrative UI:

```
ORACLE_HOME/j2ee/OC4J_Portal/applications/webtool/webtool-web/cabo/styles/blaf.xss
```

Changing the Look and Feel of the Provisioning Console

By default, the Oracle Internet Directory Provisioning Console and its user version, the Self-Service Console, do not have the same look and feel as other Oracle Collaboration Suite components.

In order for the Provisioning Console to have same look and feel as that of other Oracle Collaboration Suite components, you need to change the stylesheet that it is using by performing the following procedure:

1. On the Infrastructure hosting Oracle Internet Directory, cd to:

```
ORACLE_HOME/j2ee/OC4J_SECURITY/applications/oiddas/ui/WEB-INF
```

2. Copy the `uix-config.xml` file to `uix-config.xml.ocs`:

```
mv uix-config.xml uix-config.xml.ocs
```


3. Restart Oracle Delegated Administration Services:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

Customizing Oracle Content Services

Although you can not customize the Oracle Content Services Web interface, you can build your own custom interface and integrate it using the Oracle Content Services Web services. See *Oracle Content Services Application Developer's Guide* for more information about using the Oracle Content Services Web services.

Customizing Oracle Real-Time Collaboration

Oracle Real-Time Collaboration offers a number of different tools that administrators can use to customize the appearance and behavior of Oracle Real-Time Collaboration suite components and user interfaces.

You can customize the Oracle Real-Time Collaboration Web Client used to download the Oracle Web Conferencing or Oracle Messenger consoles, schedule conferences, view archives of conferences or messages, and perform administrative tasks. You can change the appearance of the home page, or modify what features are available to users. Users can also change their own preferences for these web pages.

You can also customize the Oracle Web Conferencing console used to participate in conferences. You can control what features are available to users, such as whether users can share documents or use an electronic white board during a conference. Users can also change their preferences for the console behavior.

You can do any of the following to customize the Oracle Real-Time Collaboration system:

- Set Oracle Real-Time Collaboration properties using the `rtcctl` utility. See Chapter 3, "Configuring Oracle Real-Time Collaboration" in *Oracle Real-Time Collaboration Administrator's Guide* for details about the properties you can set.
- Create a special site for a division or functional group at your company, such as the sales team or support organization, with customized feature. See Chapter 8, "Oracle Real-Time Collaboration Sites" in *Oracle Real-Time Collaboration Administrator's Guide* for details.
- Use the **Conference Properties** tab under the **Sites** tab to set conference defaults for a site. See "Customizing Site Properties" in Chapter 8 of *Oracle Real-Time Collaboration Administrator's Guide* for details.
- Let users set their own defaults for the Oracle Real-Time Collaboration Web Client and the Oracle Web Conferencing console using the **Preferences** link from the Web client home pages.
- Let users set their preferences for the Oracle Web Conferencing console during the current conference using the console **Preferences** button.

Customizing and Extending Oracle Web Access Client

Oracle Web Access Client is highly customizable and extendable. The following topics provide a broad outline of the options available for customizing Oracle Web Access Client. This section contains the following topics:

- [General Notes on Customizing Oracle Web Access Client](#)
- [Customizing Oracle Web Access Client Skins](#)
- [Customizing Oracle Web Access Client Menu Sets](#)
- [Customizing Oracle Web Access Client Resource Bundles](#)
- [Popping Up Oracle Web Access Client Windows](#)
- [Populating a Compose Window Opened from the Main Window](#)
- [Receiving Data using Custom Items in Context Menus](#)

General Notes on Customizing Oracle Web Access Client

To improve client side performance, Oracle Web Access Client allows users' browsers to cache most of the required files, including ones that you might want to customize. If you make any customizations as described in this document, it is likely that any users who accessed Oracle Web Access Client before you made customizations will have cached un-customized versions of files in their browser. Thus they will not see any of the new customizations until they clear their browser cache.

To partially avoid this, Oracle recommends that you complete creating your new skins or menu sets before you deploy them, so that users can never access anything but the final versions.

Customizing Oracle Web Access Client Skins

Oracle Web Access Client comes with default skins. A skin is a set of customizations that go together, under a single name, and apply look-and-feel changes such as font, color, and position of buttons, all at once to the Oracle Web Access Client interface. In a sense, a skin changes the surface of Oracle Web Access Client, without affecting the inner workings.

Setup

To begin creating a custom skin, you should start by copying an existing skin that you will then edit. You can copy the sample custom skin that comes in the installation from `ORACLE_HOME/ocscclient/skins/Modern/`, or you can use any other custom skin that is already in `ORACLE_HOME/ocscclient/skins/`. For example, if you were creating a new skin called MySkin, you should create a directory `ORACLE_HOME/ocscclient/skins/MySkin/`, which should contain the file `styles.css` and the directory `images/` (which in turn will contain several image files).

Note: you should not name your custom skins "Traditional", as this is the name of the pre-installed skin that comes with Oracle Web Access Client (and cannot be deleted or modified).

Customizing

styles.css You can change the style sheet used to render the Oracle Web Access Client. Use your favorite text editor. The class names used in the `styles.css` file are all in English and descriptive of the situation in which they are used. If you're not sure in what situation a class is used, edit it, and try out the client to see what was affected by your change.

The easiest changes to make will be in the colors used throughout the style sheet. (It is helpful to use your editor's "find/replace" feature to replace all occurrences of a color

with another.) Be careful when changing size quantities such as font size, margin, border, or padding, because in some cases you might not leave enough space for the UI components or text labels to be fully displayed.

Icon Images You can modify any of the icons in the `images/` directory. Use any graphics editor, as long as it can output the same formats that the original images are in (GIF or PNG). Oracle recommends that you keep the dimensions of each icon the same as the original images. In most cases images will be resized when rendered in the browser window.

One exception is the file `branding.gif`. This image will be displayed on the bottom left of the window, and is an opportunity for you to display a company logo. The image should be tall and narrow so that it fits that area well. In the Traditional skin this image is transparent, so you will not see a logo at all in the default client.

Deployment

In order to make your new custom skin available to users, start Oracle Web Access Client using Oracle Collaboration Suite Control. Remember, if you made modifications to an existing skin, users might have to clear their browser cache in order to download the latest version.

User Configuration

You can set your new skin as the default skin using Oracle Collaboration Suite Control, from the Web Access component Home page, on the Default Settings tab. The skin you set will be the skin seen by each user who logs into Oracle Web Access Client for the first time.

Users who have logged in at least once before you changed the default skin will not automatically be assigned the new skin. However, they will be able to switch to the new skin using the Preferences window under the Appearance section.

Customizing Oracle Web Access Client Menu Sets

A menu set is the set of commands that can be invoked by a user from the various dropdown menus on the Oracle Web Access Client menu bar. There is a default menu set, and you can create your own customized menu sets.

Setup

To begin creating a custom menu set, you should start by copying an existing menu set that you will then edit. You can copy the sample custom menu set from `ORACLE_HOME/ocscclient/menus/Simplified.xml`, or you can use any other custom menu set that is already in `ORACLE_HOME/ocscclient/menus/`. For example, if you were creating a new menu set called `MyMenus`, you should end up with a file `ORACLE_HOME/ocscclient/menus/MyMenus.xml`.

Note: You should not name your custom menu sets "Default", as this is the name of the preinstalled menu set that comes with Oracle Web Access Client (and cannot be deleted or modified).

Customizing

You can change which items are displayed in a menu or toolbar by editing the menu set's XML file. Use any text editor or an XML editing utility.

The XML file will be validated using this DTD: `ORACLE_HOME/j2ee/OC4J_OCSClient/applications/ocscclient/ocscclient-web/10.1.1.0.2/menus/menu.dtd`.

Exiting Menu Items If you copy `Simplified.xml` and look at it, you will see all the preinstalled existing menus. Each menu or toolbar consists of a list of menu items or toolbar items and separators. Note that menu items can be placed in toolbars but toolbar items can't be placed in menus. You can reorder the items within a menu or toolbar, but you cannot move an item out of one menu or toolbar and into another, nor make duplicates of an item. You can add separators wherever you like. You can remove a menu item or toolbar item by deleting it, commenting it out, or adding the attribute `hidden="true"` to the item. Caution: Do not change the items' `id` attributes or the menu set will not work.

Custom Menu Items You can add custom items to any menu or toolbar. The Simplified menu set contains a sample custom menu item linking to the Oracle homepage.

The following is a sample custom item:

```
<CUSTOMITEM id="myCustomItemID" url="http://www.mycompany.com/mycustompage"
icon="myicon.gif">
```

The `id` should be a unique alphanumeric string. This will determine what text label will be displayed on your custom item. You must create a corresponding entry in the `CustomMenuBundle` resource bundle (see ["Customizing Oracle Web Access Client Resource Bundles"](#) on page 15-11 for instructions) where the translation unit's `id` is the same as the custom item's `id`, and the source/target string is what the user will see as the item's label. You must create this entry in all languages that you expect to be used by the users of your application, or else the menu item will not have a proper text label in languages for which you don't provide an entry.

The URL should be the location of a Web page to which users will be taken when they click on that menu or toolbar item. For some context menus, data about the selected item will be passed to your custom page using the URL parameters in the query string (See ["Populating a Compose Window Opened from the Main Window"](#) on page 15-14).

The `icon` is optional. If present, it should be the name of an image file in the `images/` directory of a skin. It can be a preexisting icon, or it can be a brand new one that you create. Be sure to add any new icons to each custom skin, or else the icon will not be displayed.

Note: Since you can't add to the preinstalled skins, icons for custom menu items will never display unless the user chooses a custom skin, or you set a custom skin to be the default skin.

Custom Font List for the Rich Text Editor You can modify the list of fonts that are available for users to choose from when composing text using the Rich Text Editor. Fonts can be reordered, hidden, removed, modified or added in the `<FONTLIST>` tag at the end of the `menu.xml` file. Here is an example font entry:

```
<FONT name="Arial" value="arial,sans-serif" style="arialFontStyle"/>
```

All 3 attributes are required:

- **name** defines what will be displayed on the dropdown menu (the font name will be the same in all languages). If you want the menu option to be automatically

selected when the cursor is at a point using this font, then the name value must be exactly the same as the font's name in the Operating System.

- **value** is the HTML code that represents that font, as would be seen in a `<FONT>` HTML tag.
- **style** is the name of a CSS class in the skin definition's `styles.css` file that will be used to render the font name in the dropdown menu. If that class doesn't exist in a certain skin, the font name will be rendered in the default font.

Deployment

In order to make your new custom menu set available to users, restart Oracle Web Access Client using Oracle Collaboration Suite Control. Remember, if you made modifications to an existing menu set, users might have to clear their browser cache in order to download the latest version.

User Configuration

You can set your new menu set as the default menu set using Oracle Collaboration Suite Control, from the Web Access component Home page, in the Default Settings tab. The menu set you select will be seen by each user who logs into Oracle Web Access Client for the first time.

Users cannot choose which menu set they will see.

Customizing Oracle Web Access Client Resource Bundles

Resource bundles are the various collections of text labels used throughout the Oracle Web Access Client user interface. They are translated into several different languages.

Setup

To obtain a copy of a resource bundle that you can modify, you need to use a script found at `ORACLE_HOME/ocscclient/util/scripts/get_labels_xliff.pl`. Make sure that the environment variable `ORACLE_HOME` is properly set for this script to run successfully.

The first parameter is which resource bundle you want to obtain a copy of. You can get all of them by passing `-allbundles`, or you can get a single one by passing `-bundle BundleName`, where `BundleName` is one of the following: `SharedBundle`, `CalendarBundle`, `CharsetNameResourceBundle`, `FilesBundle`, `MailBundle`, `PeopleBundle`, `PreferencesBundle`, `SGTBundle`, `CustomMenuBundle`.

The second parameter is which language translations you want to obtain a copy of. You can get all of them by passing `-alllangs`, or you can get a single one by passing `-lang LangID`, where `LangID` is the language code (such as `en` for English, or optionally appended with a country code for a specific country's version of the language, such as `fr_CA` for Canadian French).

The files you request will be saved in the XLIFF format in `ORACLE_HOME/ocscclient/labels/`.

Customizing

The XLIFF format is an XML format used for holding translatable strings. You can edit the generated XLIFF files with a text editor, XML editing utility, or an XLIFF editor such as EvilTrans (<https://sourceforge.net/projects/eviltrans/>) or Heartsome (<http://www.heartsome.net/EN/xfedit.html>).

Each <trans-unit> element in an XLIFF file represents a text label in the user interface. The id must not be modified (it may appear encoded because it matches the compiled application). The actual text label being displayed is the content of the <target> element in all languages except English, where it is in the <source> tag instead.

If you created a custom menu item (See ["Customizing Oracle Web Access Client Menu Sets"](#) on page 15-9) you will need to add a new <trans-unit> inside the CustomMenuBundle. Make a copy of an existing one and edit its id, <source> and <target> accordingly.

Deployment

In order to make your new resource bundles available to users, restart Oracle Web Access Client using Oracle Collaboration Suite Control. Remember, users might have to clear their browser cache in order to download the latest version.

User Configuration

There is no configuration required for users to choose custom resources. If you modify any labels in a certain language, all users using Oracle Web Access Client in that language will automatically use your custom labels.

Popping Up Oracle Web Access Client Windows

Oracle Web Access Client is engineered to work in 'chromeless' browser windows. 'Chromeless' means a browser window with the normal menus, toolbar and other controls hidden. (This is mainly to discourage the user from using things like the back or refresh buttons, typing a URL directly in the address bar, or bookmarking.) In order to open up chromeless browser windows, Oracle Web Access Client provides JavaScript APIs.

To use the APIs to open an Oracle Web Access Client window directly from any Web page, include the following library:

```
<script src="http://hostname:port/ocsclient/popupLibrary">
```

This library provides the following entry points:

```
function ocsIcPopupMainWindow(baseUrl, isAccessible)
function ocsIcPopupComposeWindow(baseUrl, isAccessible)
function ocsIcPopupViewWindow(baseUrl, uid, isAccessible)
```

For all functions, baseUrl should be the root URL of the Oracle Web Access Client application, such as: http://hostname:port/ocsclient/.

isAccessible is an optional parameter; if you set it to true it will turn on Accessibility mode.

For ocsIcPopupViewWindow, uid should be the ID of the containing folder and message to be opened, such as INBOX/100. (This is the same ID you would find in the URL for opening a message in Oracle WebMail.)

You can call these functions from within a block of JavaScript in your page, or you can make them execute when the user clicks on a link with HTML code such as:

```
<a href="javascript:ocsIcPopupMainWindow('http://hostname:port/ocsclient/')">
Launch Web Access</a>
```

When the window pops up, if the user isn't yet authenticated (such as through OracleAS Single Sign-On) it will show the login page. Otherwise it will show the appropriate UI.

Extended Composer API

There is a fourth entry point provided by the above library. It is used to pop up a Compose window which already has some fields populated:

```
function ocsIcPopupAPI(baseUrl, params, isAccessible)
```

In this case, `params` is a "bag", an object whose fields represent the parameters to be passed with which to populate the compose window. It can be defined in the following ways:

```
var bag = {};
bag.api_To = "username@domain.com";
bag.api_Subject = "Hello";
```

or:

```
var bag = {};
bag["api_To"] = "username@domain.com";
bag["api_Subject"] = "Hello";
```

or declared inline:

```
ocsIcPopupViewWindow( http://hostname:port/ocscclient/
                      {api_To:"username@domain.com", api_Subject:"Hello"} );
```

Table 15–1 shows the valid parameters for the extended composer API.

Table 15–1 Extended Composer API Parameters

Parameter	Description
<code>api_Type (String)</code>	"NEW" for a blank composer (the default). "REPLY", "REPLY_ALL" or "FORWARD" will set up the composer as if the corresponding function had been applied to the messages passed in using <code>api_UIDArray</code> .
<code>api_UIDArray (Array of String)</code>	Array of message identifiers (formatted as in <code>ocsIcPopupViewWindow</code> , such as ["INBOX/100", "INBOX/101"]). Should contain only one item for "REPLY" or "REPLY_ALL", can contain more for "FORWARD".
<code>api_To (String)</code>	A string of e-mail addresses to be placed in the to: field of the composer. It is appended to any addresses that are already there in the case of this being a reply or forward.
<code>api_Cc (String)</code>	A string of e-mail addresses to be placed in the cc: field of the composer. It is appended to any addresses that are already there in the case of this being a reply or forward.
<code>api_Bcc (String)</code>	A string of e-mail addresses to be placed in the bcc: field of the composer. It is appended to any addresses that are already there in the case of this being a reply or forward.
<code>api_Subject (String)</code>	A string to be placed in the subject: field of the composer. It replaces the subject of the original message in the case of this being a reply or forward.

Populating a Compose Window Opened from the Main Window

You can create a custom menu item or toolbar button (See: "[Customizing Oracle Web Access Client Menu Sets](#)" on page 15-9) in the compose window to open up your custom Web page, which can in turn read values from and write values back into the compose window to populate some fields.

To access the composer window, your custom page needs to refer to the JavaScript object `window.opener`. For protection against cross-site scripting attacks, modern browsers will not allow a page to access this object unless both the pages in the opening and opened window are hosted in the same domain. Thus, you must make sure your page is hosted on the same domain as Oracle Web Access Client.

The compose window provides the following accessor functions:

```
function icCustomGetData(dataKey)
function icCustomSetData(dataKey, dataVal)
```

`dataKey` is a string identifying the value you want to get or set. The valid key names for `dataKey` are shown in [Table 15-2](#).

Table 15-2 *dataKey Key Names*

Key Name	Description
"composer.to" (2-D Array of String)	An array containing each recipient in the to: field. Each recipient is another array, containing 2 strings: display name and e-mail address. Display name can be null, but e-mail address should always be a non-empty string (even if it is not an e-mail address - it might be resolved into an e-mail address later by looking up in the address book).
"composer.cc" (2-D Array of String)	An array containing each recipient in the cc: field. Recipients are in the same format described above for the to: field.
"composer.bcc" (2-D Array of String)	An array containing each recipient in the bcc: field. Recipients are in the same format described above for the to: field.
"composer.subject" (String)	The string in the subject: field of the composer.

The following is an example of how the 2-D array format for recipient fields works:

If the user enters the following recipients in the **to:** field:

```
John Doe <jdoe@oracle.com>; jane.smith@oracle.com; Jill Smith
```

Then the value returned by the API for this field will be:

```
[["John Doe", "jdoe@oracle.com"], [null, "jane.smith@oracle.com"],
[null, "Jill Smith"]]
```

Even though the last item is not a well-formatted e-mail address, the text is treated as the address rather than the display name because a separate address is not present.

Note that the array returned by `icCustomGetData()` is a private copy generated for the extension. Altering the array will not affect the originating composer field; the field can only be modified using `icCustomSetData()`.

Warnings

Nothing prevents users from opening multiple copies of an extension simultaneously in separate windows. Additionally, the user can still interact with the composer window directly while an extension is open. Although there is no risk of a crash,

changes made in one window could overwrite changes concurrently made in another. If your organization uses extensions to modify composer fields, you should instruct users to avoid these situations.

Sample Extension Code

Example 15-1 is an example of a simple extension that lists all the current cc: recipients and offers to add `jsmith@oracle.com` to the list.

The extension is implemented using the following sample code:

Example 15-1 Sample Extension Code

[illegible]

Receiving Data using Custom Items in Context Menus

When you create a custom menu item (See "[Customizing Oracle Web Access Client Menu Sets](#)" on page 15-9) in a context menu, data about the object that was right-clicked to open that context menu can be passed to your custom page URL using the querystring. If the URL you provided in the custom menu set's XML file already contains a query string, the data will be appended as extra URL parameters. (Make sure the parameters you added don't have the same names as the ones Oracle Web Access Client will add on).

The parameters passed to the custom item's URL are:

For all context menus:

- **ocsUser**: The e-mail address of the currently logged on user.

For mail message list pane context menu:

- **ocsJmaMessageId**: The JMA ID of the selected message.
- **ocsJmaFolderId**: The JMA folder path of the folder the selected message is in.

For mail folder tree pane context menu:

- **ocsJmaFolderId**: The JMA folder path of the selected folder.

For message pane recipient context menu:

- **ocsEmailAddress**: The e-mail address of the clicked-on recipient.

For contacts list pane and folder tree context menus:

- **ocsObjectUid**: The internal ocsapi UID of the selected object.

For Example, The JMA folder path and message ID can be used when accessing the user's account using the IMAP protocol.

Part IV

Appendixes

The following Appendixes contain reference information that you may find helpful from time to time while you administer Oracle Collaboration Suite.

Part IV contains the following Appendixes:

- [Appendix A, "Default Port Numbers and Ranges"](#)
- [Appendix B, "Default Locations of Component Log Files"](#)
- [Appendix C, "User Provisioning Java API"](#)

Default Port Numbers and Ranges

This appendix provides the following information for each Oracle Collaboration Suite service that uses a port:

- **Allotted Port Range:** The set of port numbers Oracle Collaboration Suite attempts to use when assigning a port.
- **Default Port Number:** The first port number Oracle Collaboration Suite attempts to assign to a service. It is usually the lowest number in the allotted port range.
- **When Assigned?:**
 - **Installation:** Most port numbers are assigned by Oracle Collaboration Suite during installation. Oracle Collaboration Suite chooses a free port from the allotted port range.
 - **After Installation:** You can optionally configure some services after installation.
- **Override during installation in `staticports.ini`?:** Indicates whether you can override the default port assignment during installation by specifying a port number in `staticports.ini`. You create a template called `staticports.ini` with the port numbers you would like to use, and launch Oracle Universal Installer with special options.

See Also: Refer to "2.5.4 Using Custom Ports (The Static Ports Feature)" in *Oracle Collaboration Suite Installation Guide for Solaris Operating System* or *Oracle Collaboration Suite Installation Guide for Microsoft Windows* for directions on overriding port assignments during installation with `staticports.ini`.

Oracle Application Server Ports

Oracle Collaboration Suite is build on the Oracle Application Server 10g platform. This section lists the ports used by the various Oracle Application Server components.

The ports are sorted by the following components:

- [J2EE and OracleAS Web Cache Ports](#)
- [Portal and Oracle Mobile Collaboration Ports](#)
- [Infrastructure Ports](#)
- [OracleAS Integration InterConnect Ports](#)
- [Oracle Enterprise Manager Grid Control 10g Ports](#)

J2EE and OracleAS Web Cache Ports

Table A–1 lists the ports in a J2EE and Web Cache installation.

Table A–1 J2EE and Web Cache Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Oracle HTTP Server				
Listen	7777 - 7877	7778	Installation	Yes
Port	7777 - 7877	7777	Installation	Yes
Listen (SSL)	4443 - 4543	4444	Installation This port is not used unless you enable SSL after installation. Refer to <i>Oracle HTTP Server Administrator's Guide</i> .	Yes
Port (SSL)	4443 - 4543	4443	Installation This port is not used unless you enable SSL after installation. Refer to <i>Oracle HTTP Server Administrator's Guide</i> .	Yes
Diagnostic	7200 - 7299	7200	Installation	Yes
OracleAS Web Cache				
HTTP Listen	7777 - 7877	UNIX: 7777 Windows: 80	Installation	Yes
HTTP Listen (SSL)	4443 - 4543	4443	Installation This port is not used unless you enable SSL after installation. Refer to <i>Oracle Application Server Web Cache Administrator's Guide</i> .	Yes
Administration	4000 - 4300	4000	Installation	Yes
Invalidation	4001 - 4300	4001	Installation	Yes
Statistics	4002 - 4300	4002	Installation	Yes
OC4J				
AJP	3301 - 3400	3301	Installation	No
JMS	3701 - 3800	3701	Installation	No
RMI	3201 - 3300	3201	Installation	No
IIOP	3401 - 3500	3401	After installation, when you configure IIOP. Refer to <i>Oracle Application Server Containers for J2EE User's Guide</i> .	No
IIOPS1 (Server only)	3501 - 3600	3501	After installation, when you configured IIOPS1.	No
IIOPS2 (Server and client)	3601 - 3700	3601	After installation, when you configured IIOPS2.	No
OPMN				
ONS Local	6100 - 6199	6100	Installation	Yes
ONS Remote	6200 - 6299	6200	Installation	Yes

Table A–1 (Cont.) J2EE and Web Cache Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
ONS Request	6003 - 6099	6003	Installation	Yes
Oracle Enterprise Manager				
Application Server Control Console	1810 - 1829	1810	Installation	Yes
Application Server Control Console (SSL)	1810 - 1829	1810	After installation, when you configure the Application Server Control Console for SSL. Refer to Section A.4, "Configuring Security for Enterprise Manager Application Server Control Console" .	No
Application Server Control Console RMI	1850 - 1869	1850	Installation	Yes
Oracle Management Agent	1830 - 1849	1830	Installation	Yes
Miscellaneous Services				
DCM Discovery	7100 - 7199	7100	Installation	Yes
Java Object Cache	7000 - 7099	7000	Installation	Yes
Log Loader	44000 - 44099	44000	Installation	Yes
Port Tunneling	7501 - 7599	7501	After installation, when you configure Port Tunneling.	No

Portal and Oracle Mobile Collaboration Ports

A Portal and Oracle Mobile Collaboration installation uses the ports listed in:

- [Table A–1, "J2EE and Web Cache Ports"](#)
- [Table A–2, "Portal and Oracle Mobile Collaboration Ports"](#)

Table A–2 Portal and Oracle Mobile Collaboration Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Oracle Ultra Search				
RMI Daemon	1098	1098	Installation	No
RMI Registry	1099	1099	Installation	No
OracleAS Portal				
OracleAS Portal ¹	N/A	N/A	N/A	N/A
Oracle Mobile Collaboration				
Oracle Mobile Collaboration	N/A	N/A	N/A	N/A
Wireless Notification Dispatcher Calendar	9100 - 9199	9100	Installation	No

¹ This service does not have its own port. You can access it through the HTTP listener port.

Infrastructure Ports

An Infrastructure installation uses the ports listed in:

- [Table A-1, "J2EE and Web Cache Ports"](#)
- [Table A-3, "Infrastructure Ports"](#)

Table A-3 Infrastructure Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in statports.ini?
Oracle Enterprise Manager				
Oracle Management Agent	1830 - 1849	1830	Installation	Yes
Console HTTP	5500 - 5559	5500	Installation	Yes
Oracle Internet Directory				
Oracle Internet Directory	389, 3060 - 3129	389 ¹	Installation	Yes
Oracle Internet Directory (SSL)	636, 3130 - 3199	636 ²	Installation	Yes
OracleAS Certificate Authority				
Server Authentication Virtual Host (SSL)	4400 - 4419	4400	Installation	Yes
Mutual Authentication Virtual Host (SSL)	4400 - 4419	4401	Installation	Yes
OracleAS Metadata Repository				
Oracle Net Listener	1521	1521	Installation	No
OracleAS Single Sign-On				
OracleAS Single Sign-On ³	N/A	N/A	N/A	N/A

¹ Some versions of UNIX use port 389 in /etc/services. On these systems, the default Oracle Internet Directory non-SSL port number is 3060.

² Some versions of UNIX use port 636 in /etc/services. On these systems, the default Oracle Internet Directory SSL port number is 3130.

³ This service does not have its own port. You can access it through the HTTP listener port.

OracleAS Integration InterConnect Ports

[Table A-4](#) lists the ports used in an OracleAS Integration InterConnect installation.

Table A–4 OracleAS Integration InterConnect Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
OracleAS Integration InterConnect Adapters	Configurable	Configurable	After Installation <i>Refer to Oracle Application Server Integration InterConnect User's Guide</i>	No ¹
OracleAS Integration InterConnect Repository	Configurable	Configurable	After Installation <i>Refer to Oracle Application Server Integration InterConnect User's Guide</i>	No
RMI port for HTTP	9901	9901	Installation	No

¹ The feature of overriding port numbers with staticports.ini during installation is not available with the OracleAS Integration InterConnect installation.

Oracle Enterprise Manager Grid Control 10g Ports

[Table A–5](#) lists the ports used in an Oracle Enterprise Manager Grid Control 10g installation.

Table A–5 Oracle Enterprise Manager Grid Control 10g Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Grid Control Console	Uses the HTTP listener port ¹	Uses the HTTP listener port ¹		
Oracle Management Agent	1830 - 1849	1830	Installation	No ²
Oracle Management Service (SSL and non-SSL)	4889 - 4899	4889	Installation	No

¹ This service does not have its own port. You can access it through the HTTP listener port. Refer to setupinfo.txt in the install directory within the Grid Control Oracle home for the exact URL.

² The feature of overriding port numbers with staticports.ini is not available with the Oracle Enterprise Manager Grid Control 10g installation.

Oracle Calendar Ports

[Table A–6](#) lists ports used by Oracle Calendar server

Table A–6 Oracle Calendar Server Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini
Oracle Calendar Engine	5730-5880	5730	Installation	Yes
Oracle Calendar Synchronous Network Connection	5730-5880	5731	Installation	Yes
Oracle Calendar Directory Access Server	5730-5880	5732	Installation	Yes

Table A–6 (Cont.) Oracle Calendar Server Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini
Oracle Calendar Server Manager	5730-5880	5734	Installation	Yes
Oracle Calendar Application System	8010-8020	8010	Installation	Yes
Oracle Calendar ochecklet	8010-8020	8020	Installation	Yes

Note: Oracle Calendar server ports are assigned on a first-available, first-used basis within the allotted range at the time of installation. In an environment where Calendar has never been installed, the default ports will correspond to the ports listed in [Table A–6](#), otherwise, the next available port within the range will be assigned.

Oracle Content Services Ports

[Table A–7](#) lists ports used in Oracle Content Services.

Table A–7 Oracle Content Services Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Oracle Content Services Application (SSL and non-SSL)	Same as OracleAS Web Cache. If you are not using OracleAS Web Cache, same as Oracle HTTP Server.	Same as OracleAS Web Cache. If you are not using OracleAS Web Cache, same as Oracle HTTP Server.	Installation	Yes
Oracle Records Management Application (SSL and non-SSL)	Same as OracleAS Web Cache. If you are not using OracleAS Web Cache, same as Oracle HTTP Server.	Same as OracleAS Web Cache. If you are not using OracleAS Web Cache, same as Oracle HTTP Server.	Installation	Yes
FTP (Regular Node)	21	21	Installation	Yes
FTPS (Regular Node)	990	990	Installation	Yes
Node Manager (Regular Node)	53140 - 53899	dynamically assigned	Installation	No
Node Manager (HTTP Node - OC4J_Content and OC4J_RM)	53140 - 53899	dynamically assigned	Installation	No
Node DMS HTTP (Regular Node)	53900 - 53999	dynamically assigned	Installation	No

Oracle Real-Time Collaboration Ports

Table A–8, "Oracle Real-Time Collaboration Ports" lists ports used by Oracle Real-Time Collaboration.

In addition to the ports shown, Oracle Real-Time Collaboration requires the Oracle HTTP Server ports to be set to 80 for HTTP and 443 for HTTPS communications. If users need to access conference or participate in messages over the Internet, ports 80 and 443 must be open to the Internet. The mod_imeeting service shown in the table is a plug-in to the Oracle HTTP server, and uses its ports. See "Oracle Real-Time Collaboration Ports and Network Connectivity" in Chapter 1 of *Oracle Real-Time Collaboration Administrator's Guide* for more details about ports used by the system.

Table A–8 Oracle Real-Time Collaboration Ports

Component/Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
mod_imeeting HTTP connection	80	80	Installation	No
mod_imeeting HTTPS connection	443	443	Installation	No
mod_imeetingHTTPS tunnel connection	443	443	Installation	No
Process Manager	Any (only 1 allowed)	1027	Installation	No
Redirector server listening point	Any	NA	Installation	No
Redirector to Multiplexer	Any	1025	Installation	No
Redirector to Oracle Presence Server	5222	5222	Installation	No
Redirector to Oracle Presence Server using SSL	5223	5223	Installation	No
Voice Conversion Server	Any (only 1 allowed)	2455	Installation	No
Voice Proxy Server	Any (only 1 allowed)	3478	Installation	No

Oracle Voicemail & Fax Ports

Table A–9 Oracle Voicemail & Fax Ports

Component/Service	Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
NetMerge CCS	2019-2020	2019	NetMerge CCS Installation	No
Voicemail & Fax Services	7001-8000	None	Oracle Voicemail & Fax Installation	No
SMDI Monitor Service	7001-8000	7000	Oracle Voicemail & Fax Installation	No
DMS-Monitored Services	—	46080	Process start up	No

By default, a port range is not specified for the Oracle Voicemail & Fax services that are monitored by DMS. Oracle Voicemail & Fax assigns the default port to the first process and continues assigning consecutive ports to each new process. If you need to manage what ports are used for the DMS-monitored services, see [Specifying Ports for DMS-Monitored Services](#) on page 14-21 for information on how to specify port ranges.

Port Numbers (Sorted by Port Number)

[Table A-10](#) lists Oracle Collaboration Suite port numbers and services, sorted in ascending order by port number.

Table A-10 Port Numbers (Sorted by Port Number)

Port Number	Service
21	Oracle Content Services FTP
80	Oracle Real-Time Collaboration mod_immeeting HTTP connection (non-SSL)
389	Oracle Internet Directory (non-SSL)
443	Oracle Real-Time Collaboration mod_immeeting HTTPS connection (SSL) Oracle Real-Time Collaboration mod_immeeting HTTPS tunnel connection (SSL)
636	Oracle Internet Directory Server (SSL)
990	Oracle Content Services FIPS
1027	Oracle Real-Time Collaboration Process Manager
1098	Oracle Ultra Search RMI Daemon
1099	Oracle Ultra Search RMI Registry
1521	OracleAS Metadata Repository Oracle Net Listener
1810 - 1829	Oracle Enterprise Manager 10g Application Server Control Console (non-SSL and SSL)
1830 - 1849	Oracle Management Agent
1850 - 1869	Oracle Enterprise Manager 10g Application Server Control Console RMI
2019-2020	Oracle Voicemail & Fax NetMerge CCS
2049	Oracle Content Management Software Development Kit NFS
2455	Oracle Real-Time Collaboration Voice Conversion Server
3060 - 3129	Oracle Internet Directory (non-SSL)
3130 - 3199	Oracle Internet Directory (SSL)
3201 - 3300	OC4J RMI
3301 - 3400	OC4J AJP
3401 - 3500	OC4J IIOP
3478	Oracle Real-Time Collaboration Voice Proxy Server
3501 - 3600	OC4J IIOPS1 (Server only)
3601 - 3700	OC4J IIOPS2 (Server and client)
3701 - 3800	OC4J JMS
4000 - 4300	OracleAS Web Cache Administration OracleAS Web Cache Invalidation OracleAS Web Cache Statistics

Table A-10 (Cont.) Port Numbers (Sorted by Port Number)

Port Number	Service
4400 - 4419	OracleAS Certificate Authority Server Authentication Virtual Host (SSL) OracleAS Certificate Authority Mutual Authentication Virtual Host (SSL)
4443 - 4543	Oracle HTTP Server Listen (SSL) and Oracle HTTP Server Port (SSL) OracleAS Web Cache HTTP Listen (SSL)
4889 - 4899	Oracle Management Service (SSL and non-SSL)
5222	Oracle Real-Time Collaboration Redirector to Oracle Presence Server (non-SSL)
5223	Oracle Real-Time Collaboration Redirector to Oracle Presence Server (SSL)
5500 - 5559	Oracle Enterprise Manager Console HTTP
5730-5880	Oracle Calendar Engine Oracle Calendar Synchronous Network Connection Oracle Calendar Directory Access Server Oracle Calendar Server Manager
6003 - 6099	OPMN ONS Request
6100 - 6199	OPMN ONS Local
6200 - 6299	OPMN ONS Remote
7000 - 7099	Java Object Cache
7001-8000	Oracle Voicemail & Fax Services Oracle Voicemail & Fax SMDI Monitor Service
7100 - 7199	DCM Discovery
7200 - 7299	Oracle HTTP Server Diagnostic
7501 - 7599	Port Tunneling
7777 - 7877	Oracle HTTP Server Listen and Oracle HTTP Server Port OracleAS Web Cache HTTP Listen
9100 - 9199	Wireless Notification Dispatcher Calendar
9901	OracleAS Integration InterConnect RMI port for HTTP
16001 - 16020	OracleBI Discoverer OSAgent
44000 - 44099	Log Loader
46080	Oracle Voicemail & Fax DMS Service
53140 - 53899	Oracle Content Services Node Manager
53900 - 53999	Oracle Content Services Node DMS HTTP

Default Locations of Component Log Files

This appendix lists Oracle Collaboration Suite component log files, along with each file's purpose and default location.

Oracle Calendar Logs

[Table B-1](#) lists Oracle Calendar logs.

Table B-1 Oracle Calendar Log Files

Oracle Calendar Service	Log File Location and Name
Engine	<code>ORACLE_HOME/ocal/log/eng.log</code>
Lock Manager	<code>ORACLE_HOME/ocal/log/lck.log</code>
Synchronous Network Connection	<code>ORACLE_HOME/ocal/log/snc.log</code>
Directory Access Server	<code>ORACLE_HOME/ocal/log/das.log</code>
Corporate-Wide Services	<code>ORACLE_HOME/ocal/log/cws.log</code>
Calendar Server Manager	<code>ORACLE_HOME/ocal/log/csm.log</code>
Calendar Administrator	<code>ORACLE_HOME/ocad/bin/ocad.log</code>
Application System	<code>ORACLE_HOME/ocas/logs/ocas_log</code>

Oracle Content Services Logs

[Table B-2](#) lists Oracle Content Services logs.

Table B-2 Oracle Content Services Log Files

Oracle Content Services Service	Log File Location and Name
Regular Node	■ <code>ORACLE_HOME/content/log/content_services_domain_name/node_name.log</code> ■ <code>ORACLE_HOME/opmn/logs/Content~Node~1</code>
HTTP Node (Oracle Content Services)	■ <code>ORACLE_HOME/j2ee/OC4J_Content/application-deployments/Content/OC4J_Content_default_island_1/application.log</code> ■ <code>ORACLE_HOME/opmn/logs/Content~OC4J_Content~default_island~1</code>

Table B–2 (Cont.) Oracle Content Services Log Files

Oracle Content Services Service	Log File Location and Name
HTTP Node (Oracle Records Management)	▪ <code>ORACLE_HOME/j2ee/OC4J_RM/application-deployments/rm/OC4J_RM_default_island_1/application.log</code> ▪ <code>ORACLE_HOME/opmn/logs/Content~OC4J_RM~default_island~1</code>

Oracle Mail Logs

Oracle Mail provides the log files shown in [Table B–3](#). The names below are directory names; individual log files in the directories store data for specific dates or processes, and are named by date or process.

Oracle Mail server logs files are located in the `ORACLE_HOME/oes/log/server_type` directory. For example, List Server logs are found in the `$ORACLE_HOME/oes/log/list` directory. Each running server instance creates a log directory for itself when it starts and then writes to a log file in that directory.

For example, if there is a List Server instance running on a UNIX platform, and the operating system process ID for the process is 12345, the log file for the process will be `$ORACLE_HOME/oes/log/list/12345/12345.log`.

The maximum size to which a log file can grow is configured by the **Maximum Log Size** parameter for a particular server. If a log file reaches the maximum size, it is renamed and a new log file is created. The old file is renamed by appending a number to the file name, such as `12345.log.000`.

The renaming process cascades to older files. The names of older files are changed by increasing the value of the appended number.

Log files for Oracle Mail servers are also found in the `ORACLE_HOME/opmn/logs` directory. These log files contain debug and error output from the servers. Usually, it is not necessary to look at these files but they can be useful when investigating problems with servers.

For more information about Oracle Mail logs, see "Log Files" in Chapter 3 of *Oracle Mail Administrator's Guide*.

Table B–3 Oracle Mail Log File Directories

Oracle Real-Time Collaboration Service	Log File Location and Name
Oracle Mail server logs	<code>ORACLE_HOME/oes/log/server_type</code>
Oracle Mail server logs	<code>ORACLE_HOME/opmn/logs</code>

Oracle Mobile Collaboration Logs

[Table B–4](#) lists the Oracle Mobile Collaboration and Oracle Wireless log files and their location.

Table B–4 Oracle Mobile Collaboration and Oracle Wireless Log Files

Oracle Mobile Collaboration Service	Log File Location and Name
Oracle Mobile Push Mail	<code>ORACLE_HOME/wireless/pimap/logs/logs.xml</code>

Table B–4 (Cont.) Oracle Mobile Collaboration and Oracle Wireless Log Files

Oracle Mobile Collaboration Service	Log File Location and Name
Wireless Error Log	<i>ORACLE_HOME</i> /wireless/logs/log.xml

Oracle Real-Time Collaboration Logs

Oracle Real-Time Collaboration provides the log files shown in [Table B–5](#). Most of the names below are directory names; individual log files in the directories store data for specific dates or processes, and are named by date or process.

To view the log files interactively, log in to Oracle Real-Time Collaboration as a business administrator and choose **Logs** under the **System** tab.

Table B–5 Oracle Real-Time Collaboration Log File Directories

Oracle Real-Time Collaboration Service	Log File Location and Name
Oracle Real-Time Collaboration Web Client events not belonging to any user sessions	<i>ORACLE_HOME</i> /imeeting/logs/application
User sessions running the Oracle Real-Time Collaboration Web Client application, grouped by date (MM.DD.YYYY)	<i>ORACLE_HOME</i> /imeeting/logs/application/app_sessions
User sessions for the Oracle Real-Time Collaboration Web Client application on a particular site, grouped by date (MM.DD.YYYY)	<i>ORACLE_HOME</i> /imeeting/logs/application/site_logs/
Oracle Messenger Connection Manager	<i>ORACLE_HOME</i> /imeeting/logs/connmgr
High Availability process management for the Oracle Presence Server	<i>ORACLE_HOME</i> /imeeting/logs/imHaProcess
Oracle Presence Server	<i>ORACLE_HOME</i> /imeeting/logs/imrtr
Oracle Presence Server errors	<i>ORACLE_HOME</i> /imeeting/logs/imrtr/imrtr*.log
Oracle Presence Server statistics	<i>ORACLE_HOME</i> /imeeting/logs/imrtr/stats*.log
Oracle Presence Server chat conferences	<i>ORACLE_HOME</i> /imeeting/logs/imrtr/tc*.log
JDS Directory Service calls	<i>ORACLE_HOME</i> /imeeting/logs/imrtr/ds*.log
Multiplexer	<i>ORACLE_HOME</i> /imeeting/logs/mx
Redirector	<i>ORACLE_HOME</i> /imeeting/logs/rdtr
rtcctl commands	<i>ORACLE_HOME</i> /imeeting/logs/rtcctl
Process Manager	<i>ORACLE_HOME</i> /imeeting/logs/rtcpm
Process Manager logs for the Web Conferencing Server	<i>ORACLE_HOME</i> /imeeting/logs/rtcpm/confsvr
Process Manager logs for the Connection Manager	<i>ORACLE_HOME</i> /imeeting/logs/rtcpm/connmgr
Process Manager logs for the Oracle Presence Server	<i>ORACLE_HOME</i> /imeeting/logs/rtcpm/imrtr

Table B–5 (Cont.) Oracle Real-Time Collaboration Log File Directories

Oracle Real-Time Collaboration Service	Log File Location and Name
Process Manager logs for the Multiplexer	<code>ORACLE_HOME/imeeting/logs/rtcpm/mx</code>
Process Manager logs for the Voice Proxy Server	<code>ORACLE_HOME/imeeting/logs/rtcpm/voiceproxy</code>
Oracle Real-Time Collaboration Server process events that do not belong to any meeting, grouped by date (MM.DD.YYYY)	<code>ORACLE_HOME/imeeting/logs/servers</code>
Web Conference sessions, grouped by date (MM.DD.YYYY)	<code>ORACLE_HOME/imeeting/logs/sessions</code>
Voice Proxy Server	<code>ORACLE_HOME/imeeting/logs/voiceproxy</code>

Oracle Voicemail & Fax Logs

Table B–6 lists the Oracle Voicemail & Fax log files and their location.

Table B–6 Oracle Voicemail & Fax Log Files

Oracle Voicemail & Fax Service	Log File Location and Name
Call Transfer	<code>%ORACLE_HOME%\um\log\TransferProcess</code>
Fax Receiving	<code>%ORACLE_HOME%\um\log\FaxInProcess</code>
IVR (Interactive Voice Response)	<code>%ORACLE_HOME%\um\log\IVRProcess</code>
Message Delivery Monitor	<code>%ORACLE_HOME%\um\log\MsgDeliveryMonProcess</code>
Message Recovery	<code>%ORACLE_HOME%\um\log\MsgRecoveryProcess</code>
Message Waiting Indicator	<code>%ORACLE_HOME%\um\log\MWIProcess</code>
Recording	<code>%ORACLE_HOME%\um\log\RecordingProcess</code>
Retrieval	<code>%ORACLE_HOME%\um\log\RetrievalProcess</code>
Routing	<code>%ORACLE_HOME%\um\log\RoutingProcess</code>
SMDI (Simple Message Desk Interface) Monitor	<code>%ORACLE_HOME%\um\log\SMDIMonProcess</code>
Telephony Monitor	<code>%ORACLE_HOME%\um\log\TelephonyMonitorProcess</code>

Each log file writes status or trace information as it processes transactions for a particular service.

See Also: See Appendix A, "Troubleshooting" in *Oracle Voicemail & Fax Administrator's Guide* for more information on the Oracle Voicemail & Fax log files, including how to view the log files.

User Provisioning Java API

As of Oracle Application Server 10g Release 2 (10.1.2.0.2), the Oracle Internet Directory SDK includes a centralized user provisioning API, which enables you to manage users and their application properties in the Oracle Identity Management infrastructure. This chapter describes the main features of the API and explains how to use them.

This chapter contains the following sections:

- [Application Configuration](#)
- [User Management](#)
- [Debugging](#)
- [Sample Code](#)
- [Java Plug-ins for User Provisioning](#)

Application Configuration

Applications must register with the provisioning system in order to be recognized as provisionable. They must also create their own configuration in Oracle Internet Directory using the command-line interface. Java classes exist for viewing application configurations.

This section contains the following topics:

- [Application Registration and Provisioning Configuration](#)
- [Application Configuration Classes](#)

Application Registration and Provisioning Configuration

In order to register with the provisioning system, an application must create a provisioning configuration. Once the provisioning configuration exists, the provisioning system identifies the application as directory-enabled and provisionable.

The application must perform the following steps to create a provisioning configuration:

1. [Application Registration](#)
2. [Provisioning Configuration](#)

Application Registration

Oracle applications typically register themselves by using the repository APIs in the `repository.jar` file under `ORACLE_HOME/jlib`. This file is provided during installation specifically for application registration. In addition to creating an

application entry in Oracle Internet Directory, repository APIs can be used to add the application to privileged groups.

Applications written by customers, however, cannot use the `repository.jar` APIs to perform application registration. So application developers must use LDIF templates and create application entries in Oracle Internet Directory using LDAP commands.

An application must create a container for itself under one of these containers:

- `"cn=Products,cn=OracleContext"`—for applications that service users in multiple realms
- `"cn=Products,cn=OracleContext,RealmDN"`—for applications that service users in a specific realm

If an application is configured for a specific realm, then that application cannot manage users in other realms. In most cases, you should create the application outside any identity management realm so that the application is not tied to a specific realm in Oracle Internet Directory.

Whenever a new instance of the application installs, a separate entry for the application instance is created under the application's container. Some of the provisioning configuration is common to all the instances of a particular type and some is specific to the instance. When multiple instances of an application are deployed in an enterprise, each instance is independent of the others. Each instance is defined as a separate provisionable application. Users can be provisioned for one or more instances of this application, so that the user can get access to one or more instances of this application.

The examples in this section are for a sample application similar to Oracle Content Services. When the first instance of this application installs, specific entries must be created in Oracle Internet Directory. In the following example, the name of this application, chosen at run time, is `Content-App1` and the type of the application is `CONTENT`. The application can have LDIF templates that can be instantiated if required and then uploaded to Oracle Internet Directory. In this example, the application identity is outside any realm. That is, it is under the `"cn=Products,cn=OracleContext"` container.

```
dn: cn=IFS,cn=Products,cn=OracleContext
changetype: add
objectclass: orclContainer

dn: orclApplicationCommonName=Content-App1,cn=CONTENT,cn=Products,cn=OracleContext
changetype: add
orclappfullname: Content Application Instance 1
userpassword: welcome123
description: This is a test Application instance.
protocolInformation: xxxxx
orclVersion: 1.0
orclaci: access to entry by group="cn=odisgroup,cn=DIPAdmins,
cn=Directory Integration Platform,cn=Products,
cn=OracleContext" (browse,proxy) by group="cn=User Provisioning Admins,
cn=Groups,cn=OracleContext" (browse,proxy)
orclaci: access to attr=(*) by group="cn=odisgroup,cn=DIPAdmins,
cn=Directory Integration Platform,cn=Products,
cn=OracleContext" (search,read,write,compare)
by group="cn=User Provisioning Admins,
cn=Groups,cn=OracleContext" (search,read,write,compare)
```

The ACLs shown in the example are discussed in the ["Application User Data Location"](#) section.

The application is expected to grant certain privileges to some provisioning services as well as provisioning administrators.

When the second instance of this application installs, the following entries must be created in Oracle Directory Integration and Provisioning, assuming the name of this application, decided at run time, is Content-App2.

```
dn: orclApplicationCommonName=Content-App2,cn=IFS,cn=Products,cn=OracleContext
changetype: add
orclappfullname: Content Application Instance 2
userpassword: welcome123
description: This is a test Application instance.
orclVersion: 1.0
orclaci: access to entry by group="cn=odisgroup,
cn=DIPAdmins,cn=Directory Integration Platform,cn=Products,
cn=OracleContext" (browse,proxy) by group="cn=User Provisioning Admins,
cn=Groups,cn=OracleContext" (browse,proxy)
orclaci: access to attr=(*) by group="cn=odisgroup,cn=DIPAdmins,
cn=Directory Integration Platform,cn=Products,
cn=OracleContext" (search,read,write,compare) by
group="cn=User Provisioning Admins,cn=Groups,cn=OracleContext"
(search,read,write,compare)
```

Once the application creates its entries successfully, the application's identity is registered in Oracle Internet Directory. At this point, the application can add itself to certain privileged groups in Oracle Internet Directory, if it needs specific privileges. [Table C-1, "Some Useful Privilege Groups"](#) shows some of the privileged groups that an application can add itself to. Each of these groups exists in every realm and also in the RootOracleContext. The RootOracleContext Group is a member of the group in all the realms

Table C-1 Some Useful Privilege Groups

Group Name	Privilege
OracleDASCreateUser	Create a public user
OracleDASEditUser	Edit a public user
OracleDASDeleteUser	Delete a public user
OracleDASCreateGroup	Create a new public group
OracleDASEditGroup	Edit a public group
OracleDASDeleteGroup	Delete a public group

For example, the following LDIF file adds the Content-App1 application to cn=OracleCreateUser, which gives it the privilege to create users in all realms.

```
dn: cn=OracleCreateUser,cn=Groups,cn=OracleContext
changetype: modify
add: uniquemember
uniquemember:
orclApplicationCommonName=Content-App1,cn=IFS,cn=Products,cn=OracleContext
```

Provisioning Configuration

An application's provisioning configuration is maintained in its provisioning profile. The provisioning system supports three different provisioning profile versions:

Versions 1.1, 2.0 and 3.0. The provisioning service provides different service for the different profile version. Some generic configuration details are common to all applications, regardless of version.

Differences Between Provisioning Configuration Versions

The differences between the Version 3.0 profile and the Version 2.0 and Version 1.1 profiles are as follows:

- The new provisioning framework recognizes only Version 3.0 applications. Therefore, only applications with provisioning profile Version 3.0 show up as target applications to be provisioned in Oracle Provisioning Console. Applications with Version 2.0 and Version 1.1 profiles do not show them up as applications to be provisioned in the Provisioning Console. Still, the applications are notified about the events that the applications have configured for.
- Creating the provisioning configuration of an application is a multi step process for Version 3.0 profiles. For the earlier version profiles, provisioning registration requires only a single step, running the `oidprovtool` command.
- Applications can subscribe for provisioning events using different interfaces. Two of the interfaces, Java and OID-LDAP, are available only for interface Version 3.0, which is coupled with provisioning configuration Version 3.0. See [Table C-2, "Interfaces and Their Configuration"](#).
- An application can specify its application-specific user attributes configuration in an LDIF file. This is supported only for interface Version 3.0, which is coupled with provisioning configuration Version 3.0. See ["Application User Attribute and Defaults Configuration"](#) on page C-9
- The provisioning status of the user, discussed in the *Oracle Identity Management Integration Guide*, is maintained only for Version 3.0 applications. It is not maintained for applications having profiles earlier than Version 3.0.
- Event propagation configuration parameters vary from one version to another. See [Table C-5, "Event propagation parameters"](#).

Version 3.0-Specific Provisioning Configuration

Unless otherwise stated, the remainder of this section describes the Version 3.0-specific provisioning configuration. [Figure C-1](#) shows the DIT in Oracle Internet Directory used to store the provisioning configuration. All the provisioning configuration information is located under the following container:

```
cn=Provisioning,cn=Directory Integration Platform,cn=Products,cn=OracleContext
```

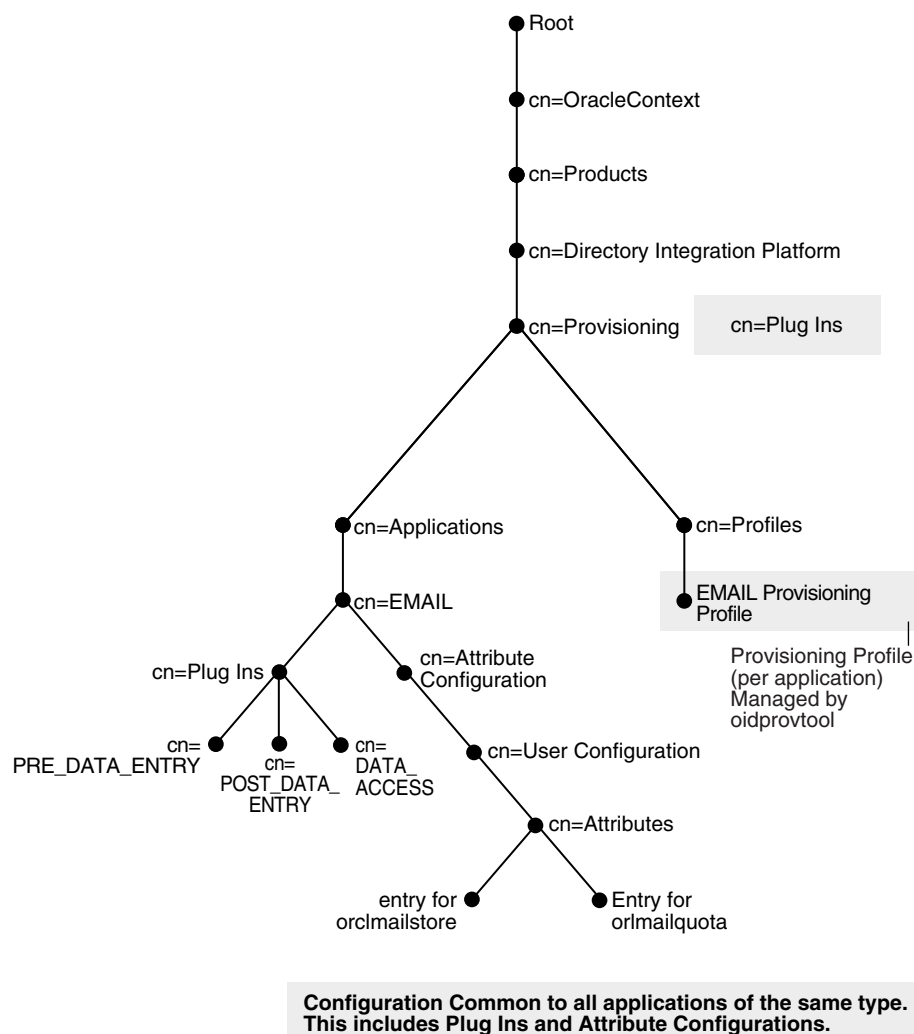
Common provisioning configuration information is stored in entries under the container:

```
cn=Profiles,cn=Provisioning,cn=Directory Integration Platform,  
cn=Products,cn=OracleContext
```

The rest of the provisioning configuration for an application is located under:

```
cn=ApplicationType,cn=Applications,cn=Provisioning,  
cn=Directory Integration Platform,cn=Products,cn=OracleContext
```

All the instances of a specific application type share the configuration under this container. That is, whenever a second instance of an existing application type creates a provisioning profile, all the configuration information under the "`cn=ApplicationType`" container is shared.

Figure C-1 The Directory Information Tree for Provisioning Configuration Data

The `Profiles` container contains the following types of configuration information.

- [Application Identity Information](#)
- [Application Identity Realm Information](#)
- [Application Provisioning and Default Policy](#)
- [Application User Data Location](#)
- [Event Interface Configuration](#)
- [Application User Attribute and Defaults Configuration](#)
- [Application Provisioning Plug-in Configuration](#)
- [Application Propagation Configuration](#)
- [Application Event Propagation Run Time Status](#)

Whenever an instance of an application creates a profile, the new profile is stored as a separate entry under the `Profiles` container in the following naming format:

`orclODIPProfileName=GUID_of_the_Realm_Entry_GUID_of_the_Application_Identity,...`

An application must specify the following information when creating a provisioning configuration:

Application Identity Information An instance of an application is uniquely identified by the following parameters:

- **Application DN**—A unique DN in the Oracle Internet Directory representing the application. This is a mandatory parameter.
- **Application Type**—A parameter that is common to all instances of the same application. Multiple instances of a particular type can share some configuration. This is a mandatory parameter.
- **Application Name**—This can be separately specified. If not specified, it is extracted from the DN. This is an optional parameter.
- **Application Display Name**—A user-friendly name for the application. This shows up on the Provisioning Console as a target provisionable application. This is an optional parameter.

You provide these application identity parameters while creating the provisioning profile by using the following arguments to the `ORACLE_HOME/bin/oidprovtool` command line utility, respectively:

- `application_type`
- `application_dn`
- `application_name`
- `application_display_name`

See Also: The `oidprovtool` command-line tool reference in *Oracle Identity Management User Reference*

Application Identity Realm Information An application registers for a specific realm in order to provide services to the users of that realm only. An application must create a separate provisioning profile for each of the realms it provides services for. In a multi realm scenario, such as a hosted OracleAS Portal scenario, applications must register for individual realms.

Whenever a provisioning administrator for a realm accesses the Provisioning Console, only the applications that are registered for that realm are shown as provisionable target applications.

The application specifies realm information while creating the provisioning profile by using the `ORACLE_HOME/bin/oidprovtool` command line utility with the argument `organization_dn`.

See Also: The `oidprovtool` command-line tool reference in *Oracle Identity Management User Reference*.

Application Provisioning and Default Policy While creating a provisioning profile, an application can specify whether the Provisioning Console should manage provisioning to that application or not. If not, the application does not show up on the Provisioning Console as an application to be provisioned. However, Oracle Directory Integration and Provisioning still processes this profile and propagates the events as expected.

An application specifies this information while creating the provisioning profile by using the `application_isdasvisible` argument to the `ORACLE_HOME/bin/oidprovtool` command line utility. The default value is `TRUE`.

An application can configure a default policy determining whether all the users in that realm should be provisioned for that application by default or no users should be provisioned by default. The valid values are

- PROVISIONING_REQUIRED—all users will be provisioned by default
- PROVISIONING_NOT_REQUIRED—no users will be provisioned by default

The default is set to PROVISIONING_REQUIRED

You can override the default policy with application-provided policy plug-ins at run time. In addition, an administrator can override both the default policy and the decision of the policy plug-in.

An application provides the default policy information by using the `default_provisioning_policy` argument to the `ORACLE_HOME/bin/oidprovtool` command line utility.

Application User Data Location Application-specific user information is stored in the application-specific containers. If this data is to be managed by the provisioning system, the application must specify the location of these containers during provisioning registration. An application specifies its user data location by using the `user_data_location` argument to the `ORACLE_HOME/bin/oidprovtool` command line utility. The application must ensure that the ACLs on this container allow Oracle Delegated Administration Services and Oracle Directory Integration and Provisioning to manage the information in this container.

Event Interface Configuration Applications can subscribe for provisioning events using different interfaces: PLSQL, Java, and OID-LDAP. [Table C-2, "Interfaces and Their Configuration"](#) lists the supported interfaces and their associated configuration. Note that `INTERFACE_VERSION` is coupled with provisioning profile version.

Table C-2 Interfaces and Their Configuration

Configuration Parameter	PLSQL	Java	OID-LDAP
INTERFACE_VERSION	1.1, 2.0, 3.0	3.0	3.0
INTERFACE_NAME	The name of the PLSQL package that implements the Interface	Not used	Not used
INTERFACE_CONNECT_INFO	The Database Connect String. Multiple formats supported for all versions.	Not used	Not used

Table C–2 (Cont.) Interfaces and Their Configuration

Configuration Parameter	PLSQL	Java	OID-LDAP
INTERFACE_ADDITIONAL_INFO	Not used	Not used	Not used
Plugin types	PRE_DATA_ENTRY,POST_DATA_ENTRY,DATA_ACCESS	PRE_DATA_ENTRY,POST_DATA_ENTRY,DATA_ACCESS,EVENT_DELIVERY (MUST)	PRE_DATA_ENTRY,POST_DATA_ENTRY,DATA_ACCESS
Description	Mainly for applications that have an Oracle Database backend. The DIP Server pushes the event to the remote Database by invoking the PLSQL procedure.	If the Interface Type is JAVA, an event delivering plug-in must be configured or the server will give errors. The plug-in configuration determines the rest of the configuration. See Application Provisioning Plug-in Configuration .	Mainly used in cases where the application is very tightly bound to Oracle Internet Directory and event delivery through the PLSQL interface or the JAVA Event Delivery Plug-in is unnecessary. This interface will be deprecated in future. Please use the JAVA Interface instead.

Applications can use the following arguments to `ORACLE_HOME/bin/oidprovtool` when specifying an event interface configuration:

- `interface_type` (Default is PLSQL)
- `interface_version` (Default is 2.0)
- `interface_name`
- `interface_connect_info`
- `interface_additional_info`

[Table C–3, "Information Formats Supported by the PLSQL Interface"](#) lists the interface connection information formats that the PL/SQL interface supports when it connects to a remote database. All the formats are supported for all interface versions.

Table C–3 Information Formats Supported by the PLSQL Interface

Format	Description
<code>dbHost:dbPort:dbSID:username:password</code>	Old format, not recommended. Oracle Directory Integration and Provisioning passes this to the thin JDBC Driver.
<code>dbHost:dbPort:dbServiceName:username:password</code>	Newer format. Not Recommended for High Availability implementations, as the database host and port might change in such scenarios. DIP passes this to the thin JDBC Driver.
<code>DBSVC=DB_TNS_Connect_Sring_Alias:username:password</code>	Used by JDBC thick OCI Driver. The local <code>tnsnames.ora</code> file must contain this alias on the node where DIP is running.
<code>DBURL=ldap://LDAP_host:LDAP_port/ServiceName,cn=OracleContext</code>	Recommended format, as it takes care of High Availability requirements. DIP passes this to the thin JDBC Driver and the driver looks up the Database Registration entry in Oracle Internet Directory to get the actual Database connection information.

Some examples of supported formats are:

```
localhost:1521:iasdb:scott:tiger

localhost:1521:iasdbsvc:scott:tiger

DBSVC=TNSALIAS:scott:tiger

DBURL=ldap://acme.com:389/sampledbname:scott:tiger
```

Application User Attribute and Defaults Configuration An application can specify its application-specific user attributes configuration in an LDIF file. This is supported only for interface version 3.0.

As shown in [Figure C-1, "The Directory Information Tree for Provisioning Configuration Data"](#), the configuration for a particular attribute is stored as a separate entry under the container:

```
"cn=Attributes,cn=User Configuration,cn=Attribute configuration,cn=Application_
Type, cn=Applications,cn=Provisioning,cn=Directory Integration
Platform,cn=Products,cn=OracleContext"
```

There is no argument to `oidprovtool` for uploading this information. The application must use an LDAP file and command-line tools to upload its attribute configuration information to Oracle Internet Directory.

Each application-specific attribute is represented as a separate entry. The following example is for the attribute `orclContentDomain`:

```
dn: cn=orclContentDomain,cn=Attributes,cn=User configuration,cn=Attribute
configuration,.....
changetype: add
orclDasAdminModifiable: 1
orclDasViewable: 1
displayname: Content Domain
orclDasMandatory: 1
orclDasUIType: LOV
orclDasLOV: us.oracle.com
orclDasLOV: oraclecorp.com
orclDASAttrIsUIField: 1
orclDASAttrIsFieldForCreate: 1
orclDASAttrIsFieldForEdit: 1
orclDASAttrToDisplayByDefault: 1
orclDASSelfModifiable: 1
orclDASAttrDisplayOrder: 1
orclDASAttrDefaultValue: oraclecorp.com
orclDASAttrObjectClass: orclCONTENTUser
objectclass: orclDASConfigAttr
```

[Table C-4, "Properties Stored as Attributes in the Attribute Configuration Entry"](#) explains the significance of each of the properties that are stored as attributes in the attribute configuration entry.

Table C–4 Properties Stored as Attributes in the Attribute Configuration Entry

Property Name	Description	Comments
orclDASIsUIField	Whether this property is to be shown in the DAS Console or not	Not Used in 10g Release 1 (10.1.1). All attributes are shown.
orclDASUIType	The Type of the UI Field: singletext, multitext, LOV, DATE, Number, password.	Used by Oracle Internet Directory Self-Service Console only
orclDASAdminModifiable	Whether the field is modifiable by the administrator or not.	Not Used in 10g Release 1 (10.1.1). All attributes are modifiable by administrator.
orclDASViewAble	Whether this attribute is a read-only attribute in the Oracle Internet Directory Self-Service Console.	Not Used in 10g Release 1 (10.1.1).
displayName	The Localized Name of the attribute as it shows on the Oracle Internet Directory Self-Service Console.	
orclDASIsMandatory	Whether this attribute is mandatory or not.	If a mandatory attribute is not populated, the Oracle Internet Directory Self-Service Console complains.
orclDASAttrIsFieldForCreate	Whether to expose this attribute only during user creation.	Not Used in 10g Release 1 (10.1.1).
orclDASAttrIsFieldForEdit	Whether to expose this attribute only during user editing.	Not Used in 10g Release 1 (10.1.1).
orclDASAttrToDisplayByDefault	Whether to hide the attribute by default under a collapsed section.	Not Used in 10g Release 1 (10.1.1).
orclDASSelfModifiable	Whether this attribute is modifiable by the user or not.	Not Used in 10g Release 1 (10.1.1), as Oracle Internet Directory Self-Service Console is only for application-specific attributes. Users cannot change their user preferences from the Oracle Internet Directory Self-Service Console.
OrclDASAttrDisplayOrder	The order is which the attribute is to be displayed in the application-specific section	Not Used in 10g Release 1 (10.1.1).
OrclDASAttrDefaultValue	The initial default value for the attribute that is used by the provisioning components: Oracle Internet Directory Self-Service Console, Oracle Directory Integration and Provisioning, Bulk Provisioning Tool	Can be changed using the Oracle Internet Directory Self-Service Console Application Management Page. The Plug-ins or the administrator can override the initial default values.
OrclDASAttrObjectClass	The LDAP object class that the attribute belongs to.	Used to create the application-specific user entries that the provisioning system maintains.

If an application has application-specific attributes, you can specify that the provisioning system manage its attributes defaults. You do that by using the `manage_application_defaults` argument to `ORACLE_HOME/bin/oidprovtool`. This argument is `TRUE` by default.

Application Provisioning Plug-in Configuration Application provisioning plug-ins are discussed in

["Java Plug-ins for User Provisioning"](#) on page C-17.

Application Propagation Configuration Event propagation configuration parameters vary from one profile version to another. [Table C–5, "Event propagation parameters"](#) lists and describes configuration parameters for event propagation.

Table C–5 Event propagation parameters

Parameter	Supported Version	Description
profile_mode	2.0,3.0	Whether the application is to receive outbound provisioning events from Oracle Internet Directory, to send inbound events, or both. Values are OUTBOUND (default), INBOUND, and BOTH.
Schedule	1.1, 2.0, 3.0	The scheduling interval after which pending events are propagated
enable_bootstrap	3.0	Enables events for application bootstrapping. This specifies that the application should be notified of users that existed in Oracle Internet Directory before the application created its provisioning profile.
enable_upgrade	3.0	Enables events for application user upgrade. This specifies that the application should be notified of users that existed in Oracle Internet Directory before the upgrade. If the application was present before the upgrade, users might already exist in the application. For such users, Oracle Directory Integration and Provisioning sends an Upgrade Event to the application so that the user is handled differently from a normal new user.
lastchangenumber	3.0	The change number in Oracle Internet Directory from which the events need to be sent to the application.
max_prov_failure_limit	3.0	The maximum number of retries that the Oracle Directory Integration and Provisioning server attempts when provisioning a user for that application.
max_events_per_invocation	2.0, 3.0	For bulk event propagation, this specifies the maximum number of events that can be packaged and sent during one invocation of the event interface.
max_events_per_schedule	2.0	Maximum number of events that Oracle Directory Integration and Provisioning sends to an application in one execution of the profile. The default is 25. In deployments with many profiles and applications, this enables Oracle Directory Integration and Provisioning, which is multi threaded, to execute threads for multiple profiles.

Table C-5 (Cont.) Event propagation parameters

Parameter	Supported Version	Description
event_subscription	1.1, 2.0, 3.0	Defines the types of OUTBOUND events an application is to receive from the event propagation service. The format is: <i>Object_Type:Domain:Operation(Attributes,...)</i> For example: USER:cn=users,dc=acme,dc=com:ADD(*) specifies that USER_ADD event should be sent if the user that was created is under the specified domain and that all attributes should also be sent. USER:cn=users,dc=acme,dc=com:MODIFY(cn,sn.mail,telephonenumber) specifies that USER_MODIFY event should be sent if the user that was modified is under the specified domain and any of the listed attributes were modified USER:cn=users,dc=acme,dc=com:DELETE specifies that USER_DELETE event should be sent if a user under the specified domain was deleted
event_permitted_operations	2.0	Defines the types of INBOUND events an application is privileged to send to the Oracle Directory Integration and Provisioning server. The format is: <i>Object_Type:Domain:Operation(Attributes,...)</i> For example: IDENTITY:cn=users,dc=acme,dc=com:ADD(*) specifies that IDENTITY_ADD event is allowed for the specified domain and all attributes are also allowed. This means that the application is allowed to create users in Oracle Internet Directory. IDENTITY:cn=users,dc=acme,dc=com:MODIFY(cn,sn.mail,telephonenumber) Specifies that IDENTITY_MODIFY is allowed for only the attributes in the list. Other attributes are silently ignored. This means that the application is allowed to modify the listed attributes of the users in Oracle Internet Directory. IDENTITY:cn=users,dc=acme,dc=com:DELETE Specifies that the application is allowed to delete users in Oracle Internet Directory
event_mapping_rules	2.0	For INBOUND profiles, this specifies the type of object received from an application and a qualifying filter condition to determine the domain of interest for this event. Multiple rules are allowed. The format is: <i>Object_Type: Filter_condition: Domain_Of_Interest</i> For example: EMP::cn=users,dc=acme,dc=com specifies that if the object type received is EMP, the event is meant for the domain "cn=users,dc=acme,dc=com". EMP:l=AMERICA:l=AMER,cn=users,dc=acme,dc=com specifies that if the object type received is EMP, and the event has the attribute l (locality) and its value is AMERICA, the event is meant for the domain "l=AMER,cn=users,dc=acme,dc=com".

Application Event Propagation Run Time Status The Oracle Provisioning Service records a user's provisioning status in Oracle Internet Directory for each provisioning-integrated application. This is described in the Deploying and Configuring Provisioning chapter of *Oracle Identity Management Integration Guide*.

Application Configuration Classes

The `oracle.idm.user.provisioning.configuration.Configuration` class enables you to obtain provisioning schema information. The `oracle.idm.user.provisioning.configuration.Application` class enables you to obtain metadata for registered applications. These classes are documented under the package `oracle.idm.provisioning.configuration`.

The `Configuration` class provides access to application configurations. To construct a `Configuration` object, you must specify the realm. For example:

```
Configuration cfg = new Configuration ("us");
```

Then you use `Configuration` class methods to get one or all application configurations in a realm. You must supply the LDAP context of the realm.

The `Configuration` object is a fairly heavy weight object, as its creation requires access to the Oracle Internet Directory metadata. Best practice is to create a `Configuration` object once during initialization of an application, then to reuse it for all operations that require it.

The `Application` object represents an application instance. Its methods provide metadata about a registered application in the infrastructure.

User Management

When Oracle Directory Integration and Provisioning or Oracle Delegated Administration Services invokes a provisioning plug-in, it passes information about the user being provisioned. A deployed application can use the user object to modify the user.

The user management provisioning classes provide the following operations:

- Create, modify, and delete a base user
- Create, modify, and delete application-specific user information
- Search base users
- Retrieve user provisioning status for applications

This section includes the following topics:

- [UserFactoryBuilder and UserFactory](#)
- [UserFactoryControl](#)
- [Creating a User](#)
- [Modifying a User](#)
- [Deleting a User](#)
- [Looking Up a User](#)

UserFactoryBuilder and UserFactory

The entry point into the user management provisioning API is the `oracle.idm.user.UserFactoryBuilder` class. You use `UserFactoryBuilder` methods to create a user factory object, `oracle.idm.user.UserFactory`. Then you use `UserFactory` methods to create and manage users. All these methods are documented in the Oracle Internet Directory API reference, under the package `oracle.idm.user`.

UserFactoryBuilder provides static createUserFactory methods to create a UserFactory object. Some of the UserFactoryBuilder methods use the JNDI access method for the default realm.

You create, modify, delete, and look up users using the UserFactory interface methods. In deployments of Oracle Collaboration Suite, you can use plug-ins to customize provisioning policy evaluation and data validation performed by the UserFactory methods.

See Also: ["Java Plug-ins for User Provisioning"](#) on page C-17 for more information about provisioning plug-ins.

The following code snippet shows creation of a UserFactory:

```
// Context to Identity Management Repository.  
DirContext dirCtx = new InitialLdapContext();  
UserFactory userFactory = UserFactoryBuilder.createUserFactory(dirCtx, "US");
```

Best practice is to create only one UserFactory object during the initialization phase of your application. Then, whenever you need to create, modify, delete, or look up a user, you use the same UserFactory. For performance reasons, the API does not provide thread safety for UserFactory objects. If you are creating a multi threaded application, you must implement your own thread synchronization.

Alternatively, you can create a pool of UserFactory objects. Then, whenever you need to perform a user management function, you use one of the objects.

UserFactoryControl

A user factory control object, `oracle.idm.user.UserFactoryControl`, encapsulates information that controls the behavior of the UserFactory class methods. The UserFactoryControl can contain the following information:

- The applications for which the user needs to be provisioned
- Whether the base user can be created, modified, or deleted
- Whether the application-specific user can be created, modified, or deleted
- Whether or not to perform the Oracle Delegated Administration Services mandatory attribute check
- The stream for writing logging information

Creating a User

Creating a user in the Oracle Identity Management repository consists of two steps:

1. Creating basic user information in the specified realm. This information is referred to as the base user.
2. Creating the application-specific user attributes, or footprint. This information is referred to as the application user.

The combination of the base user and application user in the repository is referred to as the Oracle Identity Management user. Some methods create only the base user and other create both components of the Oracle Identity Management user.

The minimum information required to create a user is a set of attributes representing the base user. The attributes are in the form of name-value pairs. These user attributes are represented as Java objects using the class `oracle.ldap.util.ModPropertySet`.

Some user creation methods require you to specify the DN of the entry that you want to create in the Oracle Identity Management user repository. Other methods do not require the DN. Instead, they construct the Oracle Identity Management user using the metadata configuration information from the Realm in which the user is created.

The following `UserFactoryControl` information affects Oracle Identity Management user creation:

- Whether or not to create the base user
- Whether or not to create the application user
- The list of applications for which the application user needs to be created.

If the creation of the base user and application user succeeds, then the creation method returns an `IdmUser` object. You use this object to manage the attributes of the base user and application user.

Modifying a User

Modifying a base user in the Oracle Identity Management repository results in

- Modifying the base user information
- Creating or modifying application user information

You must supply the following information in order to modify an Oracle Identity Management user:

1. The user's DN, GUID, or `IdmUser` object reference.
2. The desired changes to the base user attributes, represented as an `oracle.ldap.util.ModPropertySet`

Some user modification methods modify only the base user attributes. Others modify the application user attributes as well.

Deleting a User

Deleting a base user in the Oracle Identity Management repository produces the following results:

- Deleting the base user information
- Deleting the application user information

To modify an Oracle Identity Management user, you must supply the DN, GUID, or `IdmUser` object reference.

As result of this operation, the base user and the application user attributes are deleted.

Looking Up a User

The lookup methods provide two lookup options:

- Look up a specific Oracle Identity Management user using GUID or DN
- Look up a set of Oracle Identity Management users using a search filter

In order to look up Oracle Identity Management users, you must provide the DN or GUID.

The output of a lookup method is one of the following:

- A single IdmUser object
- A list of IdmUser objects

Debugging

Set `UtilDebug.MODE_PROVISIONING_API` mode to enable debugging and trace information. If you do not specify an output stream for the log messages, they are written to standard output.

The following snippet shows how to set `UtilDebug.MODE_PROVISIONING_API` mode and specify an output stream:

```
Import oracle.ldap.util.UtilDebug;
FileOutputStream logStream = new FileOutputStream("ProvAPI.log")
...
UtilDebug.setDebugMode(UtilDebug.MODE_PROVISIONING_API);
UtilDebug.setPrintStream(logStream);
```

Sample Code

The following code example shows how to create, modify, and look up a user and how to get user provisioning status for an application.

```
UtilDebug.setDebugMode(UtilDebug.MODE_PROVISIONING_API);
...
Configuration cfg = new Configuration(realm);
try {
    debug("Connecting...");
    InitialLdapContext ctx =
        ConnectionUtil.getDefaultDirCtx(hostName, port, bindDn, passwd);
    debug("Connected...");
    UserFactory factory = UserFactoryBuilder.createUserFactory(
        ctx, cfg);

    // Create
    ModPropertySet mpSet = new ModPropertySet();
    mpSet.addProperty("cn", "Heman");
    mpSet.addProperty("sn", "The Master");
    mpSet.addProperty("uid", "Heman");
    IdmUser idmUser = factory.createUser(mpSet);

    // Modify
    mpSet = new ModPropertySet();
    mpSet.addProperty(LDIF.ATTRIBUTE_CHANGE_TYPE_REPLACE,
        "sn", "Heman The Master");
    mpSet.addProperty("givenName", "Master of the Universe");
    factory.modifyUser(idmUser, mpSet);

    // Lookup
    List users = factory.searchUsers(Util.IDTYPE_SIMPLE, "Hema*",
        null);
    ...

    // Get user provisioning status for an application.
    Application app = cfg.getApplication(lCtx, "Content",
        "ContentInstance");
    String status = idmUser.getProvisioningStatus(app);
```

```

        // Another way to get user provisioning status
        String userDn = idmUser.getDn();
        String status = ProvUtil.getUserProvisioningStatus(directx,
            Util.IDTYPE_DN, userDn, app.getType(), app.getName());
    } catch (Exception ex) {
        ex.printStackTrace();
        //
    }

```

Java Plug-ins for User Provisioning

This appendix explains how to use plug-ins to customize provisioning policy evaluation and data validation in deployments of Oracle Collaboration Suite. These plug-ins can be used by PL/SQL and Java interfaces.

Oracle Directory Integration and Provisioning cannot support all of the provisioning needs of a deployment. Hence, hooks are provided at various stages of user creation, modification, and deletion. These hooks enable an enterprise to incorporate its own business rules and to tailor footprint creation to its needs. The hooks take the form of Java plug-ins.

The appendix contains these topics:

- [Plug-in Types and Their Purpose](#)
- [Plug-in Requirements](#)
- [Data Entry Plug-in](#)
- [Pre-Data-Entry Plug-in](#)
- [Post-Data-Entry Plug-in](#)
- [Data Access Plug-in](#)
- [Plug-in Return Status](#)
- [Configuration Template](#)
- [Sample Code](#)

Plug-in Types and Their Purpose

There are two types of plug-ins:

- Data entry plug-ins
- Data access plug-ins

Oracle Delegated Administration Services, Oracle Internet Directory Integration and Provisioning, and other mechanisms that affect the base user footprint in the directory invoke these plug-ins when the footprint is created. By configuring a data entry plug-in, a deployment can do any of the following:

- Validate attribute values for application users
- Validate attribute values for base users
- Enhance attribute values for application users
- Enhance attribute values for base users
- Evaluate provisioning policies

If you want the deployed application to maintain application user information you must configure a data access plug-in for it. This type of plug-in enables you to maintain the application footprint either outside of the directory or within it as several entries.

Data entry and data access plug-ins are typically invoked from one of these environments:

- User provisioning console for Oracle Delegated Administration Services
- Oracle Directory Integration and Provisioning service
- Provisioning API
- Bulk Provisioning Tools

Plug-in Requirements

All of the plug-ins that you provide for an application must be in a JAR file that can be uploaded to the directory with the standard LDIF template. See ["Configuration Template"](#) on page C-23 for an example. The plug-in interface definitions are found in `ORACLE_HOME/jlib/ldapjclnt10.jar`. Refer to *Oracle Internet Directory API Reference* and the public interfaces for a more detailed description. If the application requires additional jar files, you can upload them too.

Data Entry Plug-in

Data entry plug-ins take two forms:

- Pre-data-entry plug-ins
- Post-data-entry plug-ins

If you want to use either of these plug-ins, you must implement the `oracle.idm.provisioning.plugin.IdataEntryPlugin` interface. This interface has three methods. Here it is:

```
/**
 * The applications can perform a post data entry operation by
 * implementing this method.
 *
 * @param appCtx the application context
 * @param idmUser the IdmUser object
 * @param baseUserAttr Base user properties
 * @param appUserAttr App user properties
 * @throws PluginException when an exception occurs.
 */
public PluginStatus process(ApplicationContext appCtx,
    IdmUser idmUser, ModPropertySet baseUserAttr,
    ModPropertySet appUserAttr) throws PluginException;

/**
 * Returns the Modified Base User properties
 *
 * @return ModPropertySet modified base user properties.
 */
public ModPropertySet getBaseAttrMods();

/**
 * Returns the Modified App User properties
 *
 * @return ModPropertySet modified app user properties.
 */
```

```
public ModPropertySet getAppAttrMods();
```

Typically the plug-in implementor uses these methods to validate data or to decide whether a user should be provisioned. In the latter case, a base user attribute is used to make the decision.

The application context object contains this information:

- LDAP directory context

If you want the application to perform a directory operation, you can have it obtain the LDAP context from the application object. Note that this LDAP context should not be closed in the plug-in.

- Plug-in call mode

The plug-in is called from Oracle Delegated Administration Services, Oracle Directory Integration and Provisioning, or another environment that invokes the provisioning API. If the calling environment is Oracle Directory Integration and Provisioning, the provisioning service calls the plug-in. The two possible values are `INTERACTIVE_MODE` and `AUTOMATIC_MODE`. The first indicates that the plug-in was invoked through interaction between Oracle Delegated Administration Services and a client application. The second indicates that the plug-in was invoked by Oracle Directory Integration and Provisioning, where user intervention does not occur.

- Client locale

The plug-in may want to know what the client locale is, especially if it is invoked from Oracle Delegated Administration Services.

- Plug-in call operation

You may decide to have data entry plug-ins for both create and modify user operations. You may even implement these plug-ins in the same class. Under these conditions, the plug-in must determine which operation is invoked. The application context object uses the values `OP_CREATE` and `OP_MODIFY` to identify the operation.

- Plug-in invocation point

The data entry plug-in is typically used to determine whether a user needs to be provisioned for an application. The policy evaluation and data validation that occurs can be performed in either a pre-data-entry plug-in or a post-data-entry plug-in. You may choose either or both. If you choose both, you can implement them in the same class. The application context object specifies which one is actually invoked. It uses the values `PRE_DATA_ENTRY` and `POST_DATA_ENTY` to do this.

- Callback context

If you decide to have both pre and post plug-ins for an operation and you want the pre plug-in to share information with the post plug-in, you can set the callback context in the application context object of the pre-data-entry plug-in. The post-data-entry plug-in can then obtain and use this callback context.

- Logging

You can use the log methods provided in the application context object to log information for the plug-in.

The calling sequence looks like this:

1. Download and instantiate a plug-in object based on the configuration information object in Oracle Internet Directory
2. Construct an application context object that will be passed to the plug-in.
3. Call `process method()`
4. Call `getBaseAttrMods()` to obtain base user attributes that are modified in `process()`.
5. Merge the base user attributes returned by `getBaseAttrMods()` with the base user attributes, depending on the plug-in execution status. The execution status can be either `success` or `failure`. The plug-in implementor must return a valid plug-in execution status object. If null is returned, the execution status is considered a failure.
6. Merging of the base user will only be done if the plug-in execution status is successful.
7. Call `getAppAttrMods()` for the plug-in. This method obtains application user attributes that are modified in `process()`.
8. Merge the application user attributes returned by `getAppAttrMods()` with the application user attributes, depending on the user provisioning status returned by the plug-in.

Pre-Data-Entry Plug-in

The pre-data-entry plug-in generates values for application attributes. The attribute defaults specified during application registration are passed to this plug in along with the current base user attributes. The returned values are displayed in the UI if the invocation environment is interactive like Oracle Delegated Administration Services.

The pre-data-entry plug-in can decide whether the user should be provisioned for an application. The plug-in examines base user attributes to make the decision. It is invoked during create and modify operations. You can support both operations with one plug-in class, or you can assign one class to each.

If the application decides to have pre-data- entry plug-ins for create and modify operations, two configuration entries must be created in Oracle Internet Directory under the application container. The first entry is for the create operation:

This

```
dn: cn=PRE_DATA_ENTRY_CREATE, cn=Plugins, cn=CONTENT, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectClass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: oracle.myapp.provisioning.UserCreatePlugin
orclODIPPluginAddInfo: Pre Data Entry Plugin for CREATE operation
```

The second entry is for the modify operation:

```
dn: cn=PRE_DATA_ENTRY_MODIFY, cn=Plugins, cn=CONTENT, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectClass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: oracle.myapp.provisioning.UserModifyPlugin
orclODIPPluginAddInfo: Pre Data Entry Plugin for MODIFY operation
```

In this example, separate classes for create and modify plug-ins are shown.

Post-Data-Entry Plug-in

The post-data-entry plug-in validates data entered by the user in the UI. In addition, it generates derived attribute values. If the plug in fails for any one application, the UI does not proceed. All applications must successfully validate the data before a user entry can be created in the directory. However, in the case of non-UI environment or automatic route, the plug-in implementor can decide to raise an error or continue, based on the plug-in call mode (INTERACTIVE_MODE or AUTOMATIC_MODE).

Like the pre-data-entry plug-in, the post-data-entry plug-in is invoked during create and modify operations. The application can decide to implement one plug-in class for both operations or a separate class for each.

If you decide to have post-data-entry plug-ins for create and modify operations, create two configuration entries in Oracle Internet Directory under the application container. The first entry is for the create operation:

```
dn: cn=POST_DATA_ENTRY_CREATE, cn=Plugins, cn=CONTENT, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectClass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: oracle.myapp.provisioning.UserMgmtPlugin
orclODIPPluginAddInfo: Post Data Entry Plugin for CREATE and MODIFY
operations
```

The second entry is for the modify operation:

```
dn: cn=POST_DATA_ENTRY_MODIFY, cn=Plugins, cn=CONTENT, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectClass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: oracle.myapp.provisioning.UserMgmtPlugin
orclODIPPluginAddInfo: Post Data Entry Plugin for MODIFY and CREATE operation
```

In this example, too, separate classes for create and modify plug-ins are shown.

Data Access Plug-in

The primary purpose of the data access plug in is to manage the application-specific footprint of the user in the directory. You can use this plug-in to create and retrieve the footprint.

The data access plug-in invoked whenever a user is created and is requesting provisioning for an application—whether by Oracle Delegated Administration Services, by Oracle Directory Integration and Provisioning, or by bulk provisioning tools.

The data access plug-in is invoked during modify and delete operations as well. It can update the application footprint or remove it.

If you want to use the data access plug-in, implement the interface `oracle.idm.provisioning.plugin.IDataAccessPlugin`. Here is the interface:

```
/**
```

```
* The applications can create/modify/delete the user footprint by
* implementing this method.
*
* @param appCtx the application context
* @param idmUser IdmUser object
* @param baseUserAttr Base user properties
* @param appUserAttr App user properties
*
* @return PluginStatus a plugin status object, which must contain
* the either <code>IdmUser.PROVISION_SUCCESS</CODE> or
* <code>IdmUser.PROVISION_FAILURE</CODE> provisioning status
*
* @throws PluginException when an exception occurs.
*/
public PluginStatus process(ApplicationContext appCtx,
    IdmUser idmUser, ModPropertySet baseUserAttr,
    ModPropertySet ppUserAttr) throws PluginException;

/**
* The applications can return their user footprint by
* implementing this method. Use <CODE>
* oracle.ldap.util.VarPropertySet </CODE>
* as the return object
*
* <PRE>
* For Ex.
*   PropertySet retPropertySet = null;
*   retPropertySet = new VarPropertySet();
*
*   //Fetch the App data and add it to retPropertySet
*   retPropertySet.addProperty("name", "value");
*   ..
*   return retPropertySet;
* </PRE>
*
* @throws PluginException when an exception occurs.
*/
public PropertySet getAppUserData(ApplicationContext appCtx,
    IdmUser user, String reqAttrs[]) throws PluginException;
```

If you want to manage the user footprint for an application, create a plug-in configuration entry in the directory under the application container. The example that follows shows what this entry looks like:

```
dn: cn=DATA_ACCESS, cn=Plugins, cn=FILES, cn=Applications,
    cn=Provisioning, cn=Directory Integration Platform, cn=Products,
    cn=OracleContext
changetype: add
objectClass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: oracle.myapp.provisioning.UserDataAccPlugin
orclODIPPluginAddInfo: Data Access Plugin
```

Plug-in Return Status

Each of the provisioning plug-ins must return an object of the class `oracle.idm.provisioning.plugin.PluginStatus`. This object indicates the execution status, which is either success or failure. The object can return the user provisioning status as well.

Configuration Template

The LDIF template provided here is used in Oracle Collaboration Suite 10g Release 1 (10.1.1) to specify the application plug-in. You must create a directory entry for the application and upload the JAR file that contains the classes that implement the plug-in.

```
dn: cn=Plugins, cn=APPTYPE, cn=Applications, cn=Provisioning,
   cn=Directory Integration Platform, cn=Products, cn=OracleContext
changetype: add
add: orclODIPPluginExecData
orclODIPPluginExecData: full_path_name_of_the_JAR_file
objectclass: orclODIPPluginContainer
```

```
dn: cn=PRE_DATA_ENTRY_CREATE, cn=Plugins, cn=APPTYPE, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectclass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: Name_of_the_class_that_implements_the_plug-in
orclODIPPluginAddInfo: Pre Data Entry Plugin for CREATE operation
```

```
dn: cn=PRE_DATA_ENTRY_MODIFY, cn=Plugins, cn=APPTYPE, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectclass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: Name_of_the_class_that_implements_the_plug-in
orclODIPPluginAddInfo: Pre Data Entry Plugin for MODIFY operation
```

```
dn: cn=POST_DATA_ENTRY_CREATE, cn=Plugins, cn=APPTYPE, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectclass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: Name_of_the_class_that_implements_the_plug-in
orclODIPPluginAddInfo: Post Data Entry Plugin for CREATE and modify operations
```

```
dn: cn=POST_DATA_ENTRY_MODIFY, cn=Plugins, cn=APPTYPE, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectclass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: Name_of_the_class_that_implements_the_plug-in
orclODIPPluginAddInfo: Post Data Entry Plugin for MODIFY and CREATE operation
```

```
dn: cn=DATA_ACCESS, cn=Plugins, cn=APPTYPE, cn=Applications,
   cn=Provisioning, cn=Directory Integration Platform, cn=Products,
   cn=OracleContext
changetype: add
objectclass: orclODIPPlugin
orclStatus: ENABLE
orclODIPPluginExecName: Name_of_the_class_that_implements_the_plug-in
orclODIPPluginAddInfo: Data Access Plugin
```

Sample Code

```
/* Copyright (c) 2004, Oracle. All rights reserved. */
/**
DESCRIPTION
Sample PRE DATA Entry Plugin for CREATE operation that
validates the attribute.
PRIVATE CLASSES
None.
NOTES
This class implements the PRE_DATA_ENTRY_CREATE plugin ONLY
MODIFIED (MM/DD/YY)
svenugop 12/15/04 \226 Creation
*/
package oracle.ldap.idm;

import java.util.*;
import javax.naming.*;
import javax.naming.ldap.*;
import javax.naming.directory.*;
import oracle.ldap.util.*;
import oracle.idm.provisioning.plugin.*;
/**
 * This class implements the PRE_DATA_ENTRY_CREATE plugin ONLY
 *
 * @author Siva Venugopal
 * @since Oracle Collaboration Suite 2.1
 */
public class SamplePreDataEntryCreatePlugin implements IDataEntryPlugin
{
    public ModPropertySet mpBaseUser = null;
    public ModPropertySet mpAppUser = null;

    public PluginStatus process(ApplicationContext appCtx, IdmUser idmuser,
        ModPropertySet baseUserAttr, ModPropertySet appUserAttr)
        throws PluginException
    {
        PluginStatus retPluginStatus = null;
        String retProvStatus = null;
        String retProvStatusMsg = null;

        LDIFRecord lRec = null;
        LDIFAttribute lAttr = null;
        String val = null;
        if(null == baseUserAttr.getModPropertyValue("\223departmentNumber\224"))
        {
            mpBaseUser = new ModPropertySet();
            mpBaseUser.addProperty("departmentNumber", "ST");
            appCtx.log("\223Base user attribute \226 departmentNumber missing\224 +
                \223Setting default - ST\224");
        }
        else if ( baseUserAttr.getModPropertyValue("\223departmentNumber\224")
            .notIn("\223ST\224, \223APPS\224, \224CRM\224) )
        {
            throw new PluginException("\223Invalid department Number\224");
        }
        if((null == appUserAttr) ||
            null == appUserAttr.getModPropertyValue("\223emailQouta\224"))
        {
            mpAppUser = new ModPropertySet();
            mpAppUser.addProperty("emailQouta", "50M");
        }
    }
}
```

```

        appCtx.log("\223Application user attribute - email Qouta missing \224 +
        \223Setting default - 50M\224);
    }
    return new PluginStatus(PluginStatus.SUCCESS, null, null);
}

public ModPropertySet getBaseAttrMods()
{
    return mpBaseUser;
}

public ModPropertySet getAppAttrMods()
{
    return mpAppUser;
}
}
/* Copyright (c) 2004, Oracle. All rights reserved. */
/**
DESCRIPTION
Sample POST DATA Entry Plugin for CREATE operation. Implementing a
policy check to provision only those users who belong to \223SALES\224.
PRIVATE CLASSES
None.
NOTES
This class implements the POST_DATA_ENTRY_CREATE plugin ONLY
MODIFIED (MM/DD/YY)
svenugop 12/15/04 \226 Creation
*/
package oracle.ldap.idm;

import java.util.*;
import javax.naming.*;
import javax.naming.ldap.*;
import javax.naming.directory.*;
import oracle.ldap.util.*;
import oracle.idm.provisioning.plugin.*;
/**
 * This class implements the POST_DATA_ENTRY_CREATE plugin ONLY
 *
 * @author Siva Venugopal
 * @since Oracle Collaboration Suite 2.1
 */
public class SamplePostDataEntryCreatePlugin
{
    public ModPropertySet mpBaseUser = null;
    public ModPropertySet mpAppUser = null;

    public PluginStatus process(ApplicationContext appCtx, IdmUser idmuser,
        ModPropertySet baseUserAttr, ModPropertySet appUserAttr)
        throws PluginException
    {
        PluginStatus retPluginStatus = null;
        String retProvStatus = null;
        String retProvStatusMsg = null;

        if(null == baseUserAttr.getModPropertyValue("\223departmentNumber\224))
        {
            mpBaseUser = new ModPropertySet();
            mpBaseUser.addProperty("departmentNumber ", "SALES");
            appCtx.log("Base user attribute \221c\222 is missing");

```

```
        retProvStatus = IdmUser.PROVISION_ REQUIRED;
        retProvStatusMsg = "Provision policy: Only \221SALES\222\224.
    }
    else if (baseUserAttr.getModPropertyValue(\223deptartmentNumber\224)
        .equals(\223SALES\224))
    {
        retProvStatus = IdmUser.PROVISION_ REQUIRED;
        retProvStatusMsg = "Provision policy: Only \221SALES\222\224.
    }
    else
    {
        // do not provision those users who do not belong to SALES.
        retProvStatus = IdmUser.PROVISION_NOT_REQUIRED;
        retProvStatusMsg =
            "Do not provision the person who is not from \221SALES\222";
    }

    return new PluginStatus(PluginStatus. SUCCESS, retProvStatusMsg,
        retProvStatus);
}

public ModPropertySet getBaseAttrMods()
{
    return mpBaseUser;
}

public ModPropertySet getAppAttrMods()
{
    return mpAppUser;
}
}

/* Copyright (c) 2004, Oracle. All rights reserved. */
/**
DESCRIPTION
Sample DATA Access Plugin.
NOTES
This class implements the DATA_ACCESS plugin
MODIFIED (MM/DD/YY)
svenugop 12/15/04 \226 Creation
*/
package oracle.ldap.idm;

import javax.naming.*;
import javax.naming.ldap.*;
import javax.naming.directory.*;
import oracle.ldap.util.*;
import oracle.idm.provisioning.plugin.*;
/**
 * This class implements the DATA_ACCESS plugin ONLY
 *
 * @author Siva Venugopal
 * @since Oracle Collaboration Suite 2.1
 */
public class SampleDataAccessPlugin
{
    public PluginStatus process(ApplicationContext appCtx, IdmUser idmuser,
        ModPropertySet baseUserAttr, ModPropertySet appUserAttr)
        throws PluginException
    {
```

```

    try {
        DirContext dirCtx = appCtx.getDirCtx();
        if ( appCtx.getCallOp().equals(ApplicationContext.OP_CREATE )
        {
            // Use the directory context and create the entry.
        }
        elseif ( appCtx.getCallOp().equals(ApplicationContext.OP_MODIFY)
        {
            // Use the directory context and modify the entry.
        }
    } catch (Exception e) {
        throw new PluginException(e);
    }
    return new PluginStatus(PluginStatus.SUCCESS, null, null);
}

public PropertySet getAppUserData(ApplicationContext appCtx,
    IdmUser idmuser, String [] reqAttrs) throws PluginException
{
    VarPropertySet vpSet = null;
    DirContext dirCtx = appCtx.getDirCtx();

    try {
        Attributes attrs= dirCtx.getAttributes("\223myAppContainer\224");
        vpSet = new VarPropertySet(); // Populate the VarPropertySet from attrs
    } catch(Exception ne) {
        throw new PluginException(e);
    }
    return vpSet;    }
}

```

Glossary

API

See [application programming interface \(API\)](#).

application programming interface (API)

A series of software routines and development tools that comprise an interface between a computer application and lower-level services and functions (such as the operating system, device drivers, and other software applications). APIs serve as building blocks for programmers putting together software applications. For example, LDAP-enabled clients access Oracle Internet Directory information through programmatic calls available in the LDAP API.

application service provider

Application Service Providers (ASPs) are third-party entities that manage and distribute software-based services and solutions to customers across a wide area network from a central data center. In essence, ASPs are a way for companies to outsource some or almost all aspects of their information technology needs.

Applications tier

The tier of Oracle Collaboration Suite that runs the server applications that provide specific functionality to end users. The term "Applications tier" replaces the term "middle tier" that was used in previous releases. Each Applications tier corresponds to an instance of Oracle Application Server. See also [Oracle Collaboration Suite Applications](#).

access control

The ability of a system to grant or limit access to specific data for specific clients or groups of clients.

attribute

Directory attributes hold a specific data element such as a name, phone number, or job title. Each directory [entry](#) is comprised of a set of attributes, each of which belongs to an [object class](#). Moreover, each attribute has both a *type*, which describes the kind of information in the attribute, and a *value*, which contains the actual data.

attribute configuration file

In an Oracle Directory Integration and Provisioning environment, a file that specifies attributes of interest in a connected directory.

attribute type

Attribute types specify information about a data element, such as the data type, maximum length, and whether it is single-valued or multivalued. The attribute type provides the real-world meaning for a value, and specifies the rules for creating and storing specific pieces of data, such as a name or an e-mail address.

attribute uniqueness

An Oracle Internet Directory feature that ensures that no two specified **attributes** have the same value. It enables applications synchronizing with the enterprise directory to use attributes as unique keys.

attribute value

Attribute values are the actual data contained within an **attribute** for a particular **entry**. For example, for the attribute type `email`, an attribute value might be `sally.jones@oracle.com`.

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.

base

The root of a subtree search in an **LDAP**-compliant directory.

central directory

In an Oracle Directory Integration and Provisioning environment, the directory that acts as the central repository. In an Oracle Directory Integration and Provisioning environment, Oracle Internet Directory is the central directory.

certificate

An ITU X.509 Version 3 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.

A certificate contains the entity's name, identifying information, and public key. It is also likely to contain a serial number, expiration date, and information about the rights, uses, and privileges associated with the certificate. Finally, it contains information about the certificate authority that issued it.

certificate authority

A trusted third party that certifies that other entities—users, databases, administrators, clients, servers—are who they say they are. When it certifies a user, the certificate authority first seeks verification that the user is not on the certificate revocation list (CRL), then verifies the user's identity and grants a certificate, signing it with the

certificate authority's private key. The certificate authority has its own certificate and public key which it publishes. Servers and clients use these to verify signatures the certificate authority has made. A certificate authority might be an external company that offers certificate services, or an internal organization such as a corporate MIS department.

change logs

A database that records changes made to a directory server.

checksumming

A mechanism that computes a value for a message packet, based on the data it contains, and passes it along with the data to authenticate that the data has not been tampered with. The recipient of the data recomputes the cryptographic checksum and compares it with the cryptographic checksum passed with the data; if they match, it is "probabilistic" proof the data was not tampered with during transmission.

client

A client relies on a service. A client can sometimes be a user, sometimes a process acting on behalf of the user during a database link (sometimes called a proxy).

Client tier

The tier of Oracle Collaboration Suite that consists of the end-user applications that reside on client devices, such as desktops, laptops, wireless phones, and PDAs. See also [Oracle Collaboration Suite Applications](#).

cluster

A collection of interconnected usable whole computers that is used as a single computing resource. Hardware clusters provide high availability and scalability.

Collaboration Suite Database

The default database shipped with Oracle Collaboration Suite to hold application data.

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 Oracle databases. The network route provides, at a minimum, the location of the [listener](#) through use of a network address. See [connect identifier](#)

connect identifier

A [connect descriptor](#) or a name that maps to a connect descriptor. A connect identifier can be a [net service name](#), database service name, or [net service alias](#). Users initiate a connect request by passing a user name and password along with a connect identifier in a connect string for the service to which they wish to connect:

```
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
```

connected directory

In an Oracle Directory Integration and Provisioning environment, an information repository requiring full synchronization of data between Oracle9i Application Server and itself—for example, an Oracle human resources database.

credentials

A [username](#), password, or certificate used to gain access to the database.

dads.conf

A configuration file for Oracle HTTP Server that is used to configure a [database access descriptor \(DAD\)](#).

DAS

See [Oracle Delegated Administration Services](#). (DAS).

data dictionary

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

database access descriptor (DAD)

Database connection information for a particular Oracle Collaboration Suite component, such as the OracleAS Single Sign-On schema.

Database Administrator

(1) A person responsible for operating and maintaining an Oracle Server or a database application. (2) An Oracle username that has been given DBA privileges and can perform database administration functions. Usually the two meanings coincide. Many sites have multiple DBAs.

database alias

See [net service name](#)

database link

A network object stored in the local database or in the network definition that identifies a remote database, a communication path to that database, and optionally, a username and password. Once defined, the database link is used to access the remote database.

A public or private database link from one database to another is created on the local database by a DBA or user.

A global database link is created automatically from each database to every other database in a network with Oracle Names. Global database links are stored in the network definition.

default identity management realm

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such hosted environments, the enterprise performing the hosting is called the default identity management realm, and the enterprises that are hosted are each associated with their own identity management realm in the [directory information tree \(DIT\)](#).

Delegated Administration Services

See [Oracle Delegated Administration Services](#).

directory information base (DIB)

The complete set of all information held in the directory. The DIB consists of entries that are related to each other hierarchically in a [directory information tree \(DIT\)](#).

directory information tree (DIT)

A hierarchical tree-like structure consisting of the DNs of the entries in an LDAP directory. See [distinguished name \(DN\)](#)

directory integration and provisioning server

In an Oracle Directory Integration and Provisioning environment, the server that drives the synchronization of data between Oracle Internet Directory and a [connected directory](#).

directory integration profile

In an Oracle Directory Integration and Provisioning environment, an entry in Oracle Internet Directory that describes how Oracle Directory Integration and Provisioning communicates with external systems and what is communicated.

Directory Manager

See [Oracle Directory Manager](#).

directory naming

A [naming method](#) that resolves a database service, [net service name](#), or [net service alias](#) to a [connect descriptor](#) stored in a central directory server.

directory provisioning profile

A special kind of [directory integration profile](#) that describes the nature of provisioning-related notifications that Oracle Directory Integration and Provisioning sends to the directory-enabled applications.

directory server instance

A discrete invocation of a directory server. Different invocations of a directory server, each started with the same or different configuration set entries and startup flags, are said to be different directory server instances.

directory-specific entry (DSE)

An entry specific to a directory server. Different directory servers may hold the same [directory information tree \(DIT\)](#) name, but have different contents—that is, the contents can be specific to the directory holding it. A DSE is an entry with contents specific to the directory server holding it.

directory synchronization profile

A special kind of [directory integration profile](#) that describes how synchronization is carried out between Oracle Internet Directory and an external system.

directory user agent (DUA)

The software that accesses a directory service on behalf of the directory user. The directory user may be a person or another software element.

DIS

See [directory integration and provisioning server](#).

distinguished name (DN)

A [X.500](#) distinguished name (DN) is a unique name for a node in a directory tree. A DN is used to provide a unique name for a person or any other directory entry. A DN is a concatenation of selected [attributes](#) from each node in the tree along the path from the root node to the named entry's node. For example, in LDAP notation, the DN for a person named John Smith working at Oracle's US office would be: "cn=John Smith, ou=People, o=Oracle, c=us".

DIT

See [directory information tree \(DIT\)](#).

DN

See [distinguished name \(DN\)](#).

domain

Any tree or subtree within the [Domain Name System \(DNS\)](#) namespace. Domain most commonly refers to a group of computers whose host names share a common suffix, the domain name.

domain component attribute

The domain component (dc) attribute can be used in constructing a [distinguished name \(DN\)](#) from a domain name. For example, using a domain name such as "oracle.com", one could construct a DN beginning with "dc=oracle, dc=com", and then use this DN as the root of its subtree of directory information.

Domain Name System (DNS)

A system for naming computers and network services that is organized into a hierarchy of [domains](#). DNS is used in TCP/IP networks to locate computers through user-friendly names. DNS resolves a friendly name into an IP address, which is understood by computers.

In [Oracle Net Services](#), DNS translates the host name in a TCP/IP address into an IP address.

Enterprise Manager

See [Oracle Enterprise Manager](#).

entry

An entry is a unique record in a directory that describes an object, such as a person. An entry consists of [attributes](#) and their associated [attribute values](#), as dictated by the [object class](#) that describes that entry object. All entries in an LDAP directory structure are uniquely identified through their [distinguished name \(DN\)](#).

export agent

In an Oracle Directory Integration and Provisioning environment, an agent that exports data out of Oracle Internet Directory.

export data file

In an Oracle Directory Integration and Provisioning environment, the file that contains data exported by an [export agent](#).

export file

See [export data file](#).

external application

Applications that do not delegate authentication to the OracleAS Single Sign-On server. Instead, they display HTML login forms that ask for application user names and passwords. At the first login, users can choose to have the OracleAS Single Sign-On server retrieve these credentials for them. Thereafter, they are logged in to these applications transparently.

FTP

FTP, the File Transfer Protocol, is one of three protocols supported by [Oracle Content Services](#). It is used for file transfers across Wide Area Networks such as the Internet. FTPS, also known as secure FTP, is also supported by Oracle Content Services.

global administrator

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such an environment, a global administrator performs activities that span the entire directory.

global unique identifier (GUID)

An identifier generated by the system and inserted into an entry when the entry is added to the directory. In a multimaster replicated environment, the GUID, not the DN, uniquely identifies an entry. The GUID of an entry cannot be modified by a user.

global user inactivity timeout

An optional feature of Oracle Application Server Single Sign-On that forces users to reauthenticate if they have been idle for a pre configured amount of time. The global user inactivity timeout is much shorter than the single sign-out session timeout.

globally unique user ID

A numeric string that uniquely identifies a user. A person may change or add user names, passwords, and distinguished names, but her globally unique user ID always remains the same.

grid computing

A computing architecture that coordinates large numbers of servers and storage to act as a single large computer. Oracle Grid Computing creates a flexible, on-demand computing resource for all enterprise computing needs. Applications running on the Oracle 10g grid computing infrastructure can take advantage of common infrastructure services for failover, software provisioning, and management. Oracle Grid Computing analyzes demand for resources and adjusts supply accordingly.

group search base

In the Oracle Internet Directory default [directory information tree \(DIT\)](#), the node in the identity management realm under which all the groups can be found.

GUID

See [global unique identifier \(GUID\)](#).

HTTP

Hypertext Transfer Protocol: The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

HTTP Server

See [Oracle HTTP Server](#).

httpd.conf

The file used to configure [Oracle HTTP Server](#).

HTTPS

The use of Secure Sockets Layer (SSL) as a sublayer under the regular HTTP application layer.

identity management

The process by which the complete security life cycle for network entities is managed in an organization. It typically refers to the management of an organization's application users, where steps in the security life cycle include account creation, suspension, privilege modification, and account deletion. The network entities managed may also include devices, processes, applications, or anything else that needs to interact in a networked environment. Entities managed by an identity management process may also include users outside of the organization, for example customers, trading partners, or Web services.

identity management infrastructure database

The database that contains data for OracleAS Single Sign-On and Oracle Internet Directory.

identity management realm

A collection of identities, all of which are governed by the same administrative policies. In an enterprise, all employees having access to the intranet may belong to one realm, while all external users who access the public applications of the enterprise may belong to another realm. An identity management realm is represented in the directory by a specific [entry](#) with a special [object class](#) associated with it.

identity management realm-specific Oracle Context

An Oracle Context contained in each identity management realm. It stores the following information:

- User naming policy of the identity management realm—that is, how users are named and located.
- Mandatory authentication attributes.
- Location of groups in the identity management realm.
- Privilege assignments for the identity management realm—for example: who has privileges to add more users to the realm.
- Application specific data for that realm including authorizations.

IMAP

Internet Message Access Protocol is an Internet protocol for accessing e-mail on a remote server from a local client. It enables efficient operation such as downloading only essential data by first getting the e-mail header before the actual e-mail download. This makes the protocol well suited to remote environments.

IMAP client

A client that uses the IMAP standard to access e-mail.

Infrastructure tier

The tier of Oracle Collaboration Suite that consists of the components that provide services, such as identity management and metadata storage, for the Applications tier. Components of the Infrastructure tier include [Oracle Collaboration Suite Database](#) and [Oracle Identity Management](#). See also [Oracle Collaboration Suite Infrastructure](#).

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

Interactive Voice Response (IVR)

Interactive Voice Response The IVR plays messages, transfers calls, searches the user directory, offers simple DTMF (Dual-Tone Multifrequency) menus, and integrates with the Recording Service and Retrieval Service. Sometimes referred to as an auto attendant.

Internet Directory

See [Oracle Internet Directory](#).

Internet Message Access Protocol (IMAP)

A protocol allowing a client to access and manipulate electronic mail messages on a server. It permits manipulation of remote message folders, also called mailboxes, in a way that is functionally equivalent to local mailboxes.

IVR (Interactive Voice Response) Service

The IVR Service runs simple call answering programs that administrators can define and customize. The IVR Service supports multiple administrator-defined IVR deployment items, each of which may specify a behavior for business hours, non-business hours, holidays, and special times that fit none of these categories.

J2EE

See [Java 2 Platform, Enterprise Edition \(J2EE\)](#).

Java 2 Platform, Enterprise Edition (J2EE)

Java 2 Platform, Enterprise Edition (J2EE) is an environment for developing and deploying enterprise applications, defined by Sun Microsystems Inc. The J2EE platform consists of a set of services, application programming interfaces (APIs), and protocols that provide the functionality for developing multi tiered, Web-based applications.

Java Database Connectivity (JDBC)

An industry-standard Java interface for connecting to a relational database from a Java program, defined by Sun Microsystems.

Java Server Page (JSP)

JavaServer Pages (JSP), a server-side technology, are an extension to the Java servlet technology that was developed by Sun Microsystems. JSPs have dynamic scripting capability that works in tandem with HTML code, separating the page logic from the static elements (the design and display of the page). Embedded in the HTML page, the

Java source code and its extensions help make the HTML more functional, being used in dynamic database queries, for example.

JDBC

See [Java Database Connectivity \(JDBC\)](#)

JSP

See [Java Server Page \(JSP\)](#).

LDAP

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

ldap.ora file

A file created by Oracle Net Configuration Assistant that contains the following directory server access information:

- Type of directory server
- Location of the directory server
- Default [identity management realm](#) or [Oracle Context](#) (including ports) that the client or server will use

LDAP connection cache

To improve throughput, the OracleAS Single Sign-On server caches and then reuses connections to Oracle Internet Directory.

LDIF (LDAP Data Interchange Format)

The set of standards for formatting an input file for any of the LDAP command-line utilities.

Lightweight Directory Access Protocol (LDAP)

A set of protocols for accessing information in directories. LDAP supports TCP/IP, which is necessary for any type of Internet access. Its framework of design conventions supports industry-standard directory products, such as Oracle Internet Directory. Because it is a simpler version of the [X.500](#) standard, LDAP is sometimes called X.500 light.

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 file

A configuration file for the listener that identifies the:

- Listener name
- Protocol addresses that it is accepting connection requests on
- Services it is listening for

The `listener.ora` file typically resides in `ORACLE_HOME/network/admin` on UNIX platforms and `ORACLE_BASE\ORACLE_HOME\network\admin` on Windows.

load balancer

Hardware devices and software that balance connection requests between two or more servers, either due to heavy load or failover. BigIP, Alteon, or Local Director are all popular hardware devices. Oracle Application Server Web Cache is an example of load balancing software.

mod_osso

A module on the Oracle HTTP Server that enables applications protected by OracleAS Single Sign-On to accept HTTP headers in lieu of a user name and password once the user has logged into the OracleAS Single Sign-On server. The values for these headers are stored in the [mod_osso cookie](#).

mod_osso cookie

User data stored on the HTTP server. The cookie is created when a user authenticates. When the same user requests another application, the Web server uses the information in the mod_osso cookie to log the user in to the application. This feature speeds server response time.

naming attribute

The attribute used to compose the RDN of a new user entry created through Oracle Delegated Administration Services or Oracle Internet Directory Java APIs. The default value for this is `cn`.

naming method

The resolution method used by a client application to resolve a [connect identifier](#) to a [connect descriptor](#) when attempting to connect to a database service.

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](#), or [database alias](#).

net service alias

An alternative name for a [directory naming](#) object in a directory server. A directory server stores net service aliases for any defined [net service name](#) or database service. A net service alias entry does not have connect descriptor information. Instead, it only references the location of the object for which it is an alias. When a client requests a directory lookup of a net service alias, the directory determines that the entry is a net service alias and completes the lookup as if it was actually the entry it is referencing.

network listener

A listener on a server that listens for connection requests for one or more databases on one or more protocols. See [listener](#)

object class

A named group of [attributes](#). When you want to assign attributes to an entry, you do so by assigning to that entry the object classes that hold those attributes. All objects associated with the same object class share the same attributes.

In LDAP, object classes are used to group information. Typically an object class models a real-world object such as a person or a server. Each directory entry belongs to one or more object classes. The object class determines the attributes that make up an entry. One object class can be derived from another, thereby inheriting some of the characteristics of the other class.

obfuscation

A process by which information is scrambled into a non-readable form, such that it is extremely difficult to de-scramble if the algorithm used for scrambling is not known.

OC4J

See [Oracle Containers for J2EE \(OC4J\)](#).

OID

See [Oracle Internet Directory](#).

OID Database Password Utility

The utility used to change the password with which Oracle Internet Directory connects to an Oracle Database.

OID Monitor

The Oracle Internet Directory component that initiates, monitors, and terminates the Oracle Internet Directory Server processes. It also controls the replication server if one is installed, and Oracle Directory Integration and Provisioning Server.

Oracle Application Server Single Sign-On

OracleAS Single Sign-On consists of program logic that enables you to log in securely to applications such as expense reports, mail, and benefits. These applications take two forms: [partner applications](#) and [external applications](#). In both cases, you gain access to several applications by authenticating only once.

Oracle Certificate Authority

Oracle Application Server Certificate Authority is a [certificate authority](#) for use within your Oracle Application Server environment. OracleAS Certificate Authority uses Oracle Internet Directory as the storage repository for certificates. OracleAS Certificate Authority integration with OracleAS Single Sign-On and Oracle Internet Directory provides seamless certificate provisioning mechanisms for applications relying on them. A user provisioned in Oracle Internet Directory and authenticated in OracleAS Single Sign-On can choose to request a digital certificate from OracleAS Certificate Authority.

Oracle Collaboration Suite

An integrated suite of software applications to enable communication, messaging, and content sharing in an enterprise environment. At an architectural level, it includes three tiers: an [Applications tier](#), which consists of server applications that provide the basic functionality, a [Client tier](#), which consists of applications on desktops, laptops, and wireless devices, and an [Infrastructure tier](#), which provides centralized services, such as identity management and metadata storage, for the applications.

Oracle Collaboration Suite Applications

The applications that make up Oracle Collaboration Suite, namely:

- Oracle Calendar
- Oracle Collaboration Suite Search
- Oracle Content Services
- Oracle Discussions
- Oracle Mail
- Oracle Mobile Collaboration

-
- Oracle Real-Time Collaboration
 - Oracle Voicemail & Fax
 - Oracle Workspaces

Each of the preceding applications is a component of Oracle Collaboration Suite Applications. These applications rely on the services provided by the [Infrastructure tier](#). See also [Applications tier](#).

Oracle Collaboration Suite Database

The default database included with Oracle Collaboration Suite to hold application data and metadata. The Oracle Collaboration Suite Database is part of the [Oracle Collaboration Suite Infrastructure](#).

Oracle Collaboration Suite Infrastructure

The underlying components that support Oracle Collaboration Suite and provide centralized product metadata and security services, configuration information, and data repositories for [Oracle Collaboration Suite Applications](#). Oracle Collaboration Suite Infrastructure uses and builds on OracleAS Infrastructure. It includes the [Oracle Collaboration Suite Database](#) and [Oracle Identity Management](#). See also [Infrastructure tier](#).

Oracle Collaboration Suite Portal

The customized edition of [OracleAS Portal](#) provided with [Oracle Collaboration Suite](#).

Oracle Containers for J2EE (OC4J)

A lightweight, scalable container for [Java 2 Platform, Enterprise Edition \(J2EE\)](#).

Oracle Content Services

Oracle Content Services is a content management application that provides a secure place to store and share content. It offers collaboration features such as check-in/check-out, role-based security, workflow, custom metadata, and file system access through standard protocols.

Oracle Content Services domain

An [Oracle Content Services](#) domain is a logical grouping of [Oracle Content Services nodes](#), and an Oracle database instance (called the [Collaboration Suite Database](#)) that contains the Oracle Content Services data.

Oracle Content Services nodes

An [Oracle Content Services](#) node is the application software that comprises the product, along with the underlying Java Virtual Machine (JVM) required to support the software at runtime. There are two types of nodes: regular nodes, and HTTP nodes. Each node is based on a particular node configuration.

Oracle Context

An entry in an LDAP-compliant internet directory called `cn=OracleContext`, under which all Oracle software relevant information is kept, including entries for [Oracle Net Services](#) directory naming and [checksumming](#) security.

There can be one or more Oracle Contexts in a directory. An Oracle Context is usually located in an [identity management realm](#). See also: [identity management realm-specific Oracle Context](#).

Oracle Database Advanced Replication

A feature in the Oracle Database that enables database tables to be kept synchronized across two Oracle databases.

Oracle Delegated Administration Services

A set of individual, pre-defined services—called Oracle Delegated Administration Services units—for performing directory operations on behalf of a user. Oracle Internet Directory Provisioning Console makes it easier to develop and deploy administration solutions for both Oracle and third-party applications that use Oracle Internet Directory.

Oracle Directory Integration and Provisioning

A collection of interfaces and services for integrating multiple directories by using Oracle Internet Directory and several associated plug-ins and connectors. A feature of Oracle Internet Directory that enables an enterprise to use an external user repository to authenticate to Oracle products.

Oracle Directory Integration and Provisioning Server

In an Oracle Directory Integration and Provisioning environment, a daemon process that monitors Oracle Internet Directory for change events and takes action based on the information present in the [directory integration profile](#).

Oracle Directory Integration Platform

A component of [Oracle Internet Directory](#). It is a framework developed to integrate applications around a central LDAP directory like Oracle Internet Directory.

Oracle Directory Manager

A Java-based tool with a graphical user interface for administering Oracle Internet Directory.

Oracle Enterprise Manager

Oracle Enterprise Manager is the Oracle integrated management solution for managing the Oracle environment.

Oracle HTTP Server

Software that processes Web transactions that use the Hypertext Transfer Protocol (HTTP). Oracle uses HTTP software developed by the Apache Group.

Oracle Identity Management

An integrated set of components that provide distributed security to Oracle products and make it possible to centrally and securely manage enterprise identities and their access to applications in the enterprise. It includes the following components: [Oracle Internet Directory](#), Oracle Directory Integration and Provisioning, [Oracle Delegated Administration Services](#), OracleAS Single Sign-On, and Oracle Application Server Certificate Authority.

Oracle Internet Directory

A general purpose directory service that enables retrieval of information about dispersed users and network resources. It combines [Lightweight Directory Access Protocol \(LDAP\)](#) Version 3 with the high performance, scalability, robustness, and availability of the Oracle Database.

Oracle Internet Directory Self-Service Console

An interface constructed using [Oracle Delegated Administration Services](#); a single graphical interface for end users to manage their personal profile, including password, photo, time zone, and resource access information. When administrators, with the required privileges, log in they instead see the [Oracle Internet Directory Provisioning Console](#).

Oracle Internet Directory Provisioning Console

An interface constructed using [Oracle Delegated Administration Services](#); a single graphical interface for managing user accounts and user groups, setting user attribute defaults, creating, enabling, disabling, locking, de-provisioning, and deleting user accounts, and managing [identity management realms](#). When users lacking provisioning privileges log in to the console, they instead see the [Oracle Internet Directory Self-Service Console](#).

Oracle Net Services

An Oracle product that enables two or more computers that run the Oracle server or Oracle tools such as Designer/2000 to exchange data through a third-party network. Oracle Net Services support distributed processing and distributed database capability. Oracle Net Services is an open system because it is independent of the communication protocol, and users can interface Oracle Net to many network environments.

Oracle Process Manager and Notification Server (OPMN)

Oracle Process Manager and Notification Server (OPMN) manages Oracle HTTP Server and OC4J processes within an application server instance as well as other processes such as the Oracle Voicemail & Fax services. It acts as a manager daemon to restart managed services, when necessary.

Oracle Records Management

Oracle Records Management is a new component of [Oracle Content Services](#) that provides support for compliance solutions like enforced recordization and retention policies. Records Administrators can use Oracle Records Management to specify file plans and create record categories.

Oracle Universal Installer (OUI)

A Java-based graphical user interface application that enables you to install Oracle components from a CD, multiple CDs, or the Web. It is used for installing or upgrading all Oracle products, including Oracle Collaboration Suite, Oracle Application Server, Oracle Database 10g, and the various components of each of those products.

OracleAS Portal

An OracleAS Single Sign-On [partner application](#) that provides a mechanism for integrating files, images, applications, and Web sites. The External Applications portlet provides access to external applications.

In Oracle Collaboration Suite, Oracle Collaborative Portlets provides access to the Oracle Collaboration Suite applications via a set of ready-made portlets.

partner application

An Oracle Application Server application or non-Oracle application that delegates the authentication function to the OracleAS Single Sign-On server. This type of application spares users from re authenticating by accepting [mod_osso](#) headers.

profile

See [directory integration profile](#).

provisioned applications

Applications in an environment where user and group information is centralized in Oracle Internet Directory. These applications are typically interested in changes to that information in Oracle Internet Directory.

In [Oracle Collaboration Suite](#), provisioned applications include:

- Oracle Calendar
- Oracle Content Services
- Oracle Mail
- Oracle Real-Time Collaboration
- Oracle Voicemail & Fax

If Oracle Discussions is configured, it is provisioned whenever Oracle Mail is provisioned.

provisioning

The process of providing users with access to configured [Oracle Collaboration Suite](#) applications.

provisioning integration profile

A special kind of [directory integration profile](#) that describes the nature of provisioning-related notifications that Oracle Directory Integration and Provisioning sends to the directory-enabled applications.

proxy authentication

A process typically employed in an environment with a Applications tier such as a firewall, wherein the end user authenticates to the Applications tier, which thence authenticates to the directory on the user's behalf—as its *proxy*. The Applications tier logs into the directory as a *proxy user*. A proxy user can switch identities and, once logged into the directory, switch to the end user's identity. It can perform operations on the end user's behalf, using the authorization appropriate to that particular end user.

proxy server

A server between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server. In OracleAS Single Sign-On, proxies are used for load balancing and as an extra layer of security.

See also: [load balancer](#).

realm

Short for [identity management realm](#).

realm Oracle Context

An [Oracle Context](#) that is part of an [identity management realm](#) in Oracle Internet Directory.

registry

A Windows repository that stores configuration information for a computer.

relational database

A structured collection of data that stores data in tables consisting of one or more rows, each containing the same set of columns. Oracle makes it very easy to link the data in multiple tables. This is what makes Oracle a relational database management system, or RDBMS. It stores data in two or more tables and enables you to define relationships between the tables. The link is based on one or more fields common to both tables.

relative distinguished name (RDN)

The local, most granular level entry name. It has no other qualifying entry names that would serve to uniquely address the entry. In the example, `cn=Smith, o=acme, c=US`, the RDN is `cn=Smith`.

root Oracle Context

In the Oracle Identity Management infrastructure, the root Oracle Context is an entry in Oracle Internet Directory containing a pointer to the default identity management realm in the infrastructure. It also contains information on how to locate an identity management realm given a simple name of the realm.

scalability

The ability of a system to provide throughput in proportion to, and limited only by, available hardware resources.

schema

1. Database schema: A named collection of objects, such as tables, [views](#), clusters, procedures, packages, [attributes](#), [object classes](#), and their corresponding matching rules, which are associated with a particular user. 2. LDAP directory schema: The collection of attributes, object classes, and their corresponding matching rules.

Secure Sockets Layer (SSL)

An industry standard protocol designed by Netscape Communications Corporation for securing network connections. SSL provides authentication, encryption, and data integrity using public key infrastructure (PKI).

server

A provider of a service.

service

1. A network resource used by clients; for example, an Oracle database server.
2. An executable process installed in the Windows [registry](#) and administered by Windows. Once a service is created and started, it can run even when no user is logged on to the computer.

SGA

See [System Global Area \(SGA\)](#).

SID

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

Single Sign-On (SSO)

The ability of a user to *authenticate once*, combined with strong authentication occurring transparently in subsequent connections to other databases or applications. Single sign-on lets a user access multiple accounts and applications with a single

password, entered during a single connection. *Single password, single authentication.* Oracle Advanced Security supports Kerberos, DCE, and SSL-based single sign-on.

SMTP

Simple Mail Transfer Protocol is the main protocol used to control the transfer of electronic mail (e-mail) messages on the Internet. SMTP is the TCP/IP protocol, and this specifies the format of the messages, and how servers and terminals are to interact.

SMTP is usually employed for the sending of the messages, with other protocols used to receive them, for example, POP3 or IMAP, which can save the messages in a mailbox for download from the server to a particular terminal, as required by the user. ESMTP, Extended Simple Mail Transfer Protocol, allows multimedia files to be sent as e-mail.

SSL

See [Secure Sockets Layer \(SSL\)](#).

SSO

See [Single Sign-On \(SSO\)](#)

subtree

A section of a directory hierarchy, which is also called a [directory information tree \(DIT\)](#). The subtree typically starts at a particular directory node and includes all subdirectories and objects below that node in the directory hierarchy.

super user

A special directory administrator who typically has full access to directory information.

System Global Area (SGA)

A group of shared memory structures that contain data and control information for one Oracle database [instance](#). If multiple users are concurrently connected to the same instance, the data in the instance SGA is shared among the users. Consequently, the SGA is sometimes referred to as the "shared global area." The combination of the background processes and memory buffers is called an Oracle instance.

system identifier (SID)

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

tnsnames.ora

A file that contains connect descriptors; each [connect descriptor](#) is mapped to a [net service name](#). The file may be maintained centrally or locally, for use by all or individual clients. This file typically resides in the following locations depending on your platform:

- (UNIX) `ORACLE_HOME/network/admin`
- (Windows) `ORACLE_BASE\ORACLE_HOME\network\admin`

URI

Uniform Resource Identifier (URI). A way to identify any point of content on the Web, whether it be a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the Web page address, which is a particular form or subset of URI called a [URL](#).

URL

Uniform Resource Locator (URL). The address of a file accessible on the Internet. The file can be a text file, HTML page, image file, a program, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of the file location on the computer.

username

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

user search base

In the Oracle Internet Directory default [directory information tree \(DIT\)](#), the node in the identity management realm under which all the users are placed.

views

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

virtual host

A single physical Web server machine that is hosting one or more Web sites or domains, or a server that is acting as a proxy to other machines (accepts incoming requests and reroutes them to the appropriate server).

In the case of OracleAS Single Sign-On, virtual hosts are used for load balancing between two or more OracleAS Single Sign-On servers. They also provide an extra layer of security.

virtual host name

In an Oracle Application Server Cold Failover Cluster (Identity Management), the host name corresponding to a particular virtual IP address.

virtual IP address

In an Oracle Application Server Cold Failover Cluster (Identity Management), each physical node has its own physical IP address and physical host name. To present a single system image to the outside world, the cluster uses a dynamic IP address that can be moved to any physical node in the cluster. This is called the virtual IP address.

wallet

A wallet is a data structure used to store and manage security credentials for an individual entity. A [Wallet Resource Locator \(WRL\)](#) provides all the necessary information to locate the wallet.

wallet obfuscation

Wallet [obfuscation](#) is used to store and access an Oracle [wallet](#) without querying the user for a password prior to access (supports [Single Sign-On \(SSO\)](#)).

Wallet Resource Locator

A wallet resource locator (WRL) provides all necessary information to locate a [wallet](#). It is a path to an operating system directory that contains a wallet.

WebDAV

Web-based Distributed Authoring and Versioning (WebDAV) is one of three protocols supported by [Oracle Content Services](#). It allows clients to browse and edit files on Oracle Content Services as if they were on the local machine. WebDAV is designed for Wide Area Networks such as the Internet. Currently, the most widespread WebDAV client is the Web Folders extension to Windows Explorer, also known as Network Places in Windows 2000/XP.

WRL

See [Wallet Resource Locator](#)

X.500

X.500 is a standard from the International Telecommunication Union (ITU) that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city.

XML

Extensible Markup Language (XML) is a specification developed by the World Wide Web Consortium (W3C). XML is a pared-down version of Standard Generalized Mark-Up Language (SGML), designed especially for Web documents. XML is a metalanguage (a way to define tag sets) that allows developers to define their own customized markup language for many classes of documents.

Index

A

- access control lists (ACLs)
 - customizing, 9-24
 - for export profiles, 9-25
 - for import profiles, 9-24
 - sample files, 9-25
- accounts
 - deleting, 4-17
- Active Directory
 - and Active Directory Connector, 9-3
 - concepts and architecture for integration with, 9-1
 - configuration of integration with, 9-16
 - configuring connection details for integration, 9-18
 - deployment options for integration with, 9-13
 - domain controller
 - switching to different in same domain, 9-50
 - external authentication plug-in, 9-36
 - enabling, 9-37
 - installing, 9-36
 - managing, 9-49
 - testing, 9-37
 - foreign security principals, 9-12
 - forest, as mapped to Oracle Internet Directory, 9-11
 - integration
 - distinguished name mapping, 9-19
 - post-configuration tasks, 9-47
 - typical management tasks, 9-47
 - managing, 9-47
 - multiple domain
 - synchronizing with, 9-26
 - synchronizing deletions from, 9-23
 - trust relationships between domains, 9-12
- Active Directory Connector
 - what it does, 9-3
- Active Directory domain controller
 - single, integration with, 9-10
- Active Directory domain controllers
 - multiple, integration with, 9-11
- Active Directory External Authentication
 - Plug-in, 9-3
- ActiveChgImp profile, 9-17
- ActiveExport profile
 - synchronization profiles
 - ActiveExport, 9-17
- ActiveImport profile, 9-17
- addNode.bat script, 13-4, 13-8
- addNode.sh script, 13-4, 13-8
- addsub.csh script, 7-5
- Administration tools, 3-1
- advisors
 - Automatic Database Diagnostics Monitor (ADDM), 10-29
 - Buffer Cache Advisor, 10-29
 - description, 10-28
 - Memory Advisor, 10-29
 - using, 10-30
 - performance, 10-28
 - PGA Advisor, 10-29
 - Segment Advisor, 10-29
 - using, 6-31
 - Shared Pool Advisor, 10-29
 - SQL Access Advisor, 10-29
 - using, 10-30
 - SQL Tuning Advisor, 10-29
 - using, 10-29
 - Undo Advisor, 6-35, 10-29
- All Metrics page, 3-14
- allotted port range, A-1
- ALTER DATABASE statement
 - MOUNT clause, 6-20
 - OPEN clause, 6-20
 - READ ONLY clause, 6-20
- ALTER SYSTEM statement
 - ENABLE RESTRICTED SESSION clause, 6-21
- applications
 - adding to deployment, 5-64
- Applications tier
 - starting, 2-7
 - stopping, 2-10
- Applications tiers
 - adding additional, 5-42
 - scripted starting, 2-9
 - scripted stopping, 2-11
 - starting, 2-7
 - starting manually, 2-7
 - stopping, 2-10
 - stopping manually, 2-10
- application-specific user attributes, 4-18
- archive log files

- description, 6-27
- archived redo log backup, 11-5
- ARCHIVELOG mode, 11-6
 - in datafile backup, 11-5
 - in online database backup, 11-4
 - in tablespace backup, 11-5
 - in whole database backup, 11-5
- attribute-level mapping, in integration with Active Directory, 9-20
- attributes
 - for user login name, 9-16
- authentication dynamics
 - identity management realms, 7-3, 7-4
 - Windows native authentication, 9-5
- Automatic Database Diagnostics Monitor (ADDM)
 - description, 10-29
 - modifying behavior, 10-27
 - overview, 10-20
 - viewing performance analysis, 10-26
- automatic shared memory configuration
 - enabling, 6-38
- Automatic Storage Management (ASM), 13-6
- Automatic Workload Repository, 10-21

B

- B2B schema
 - changing password, 6-43, 6-46
- b64InternetCertificate.txt file, 14-18
- Backup
 - ARCHIVELOG mode, 11-6
 - Database Backups, 11-8
 - methodology, 11-6
 - types, 11-4
- backup
 - cold backup, 11-2
 - cold database backup, 11-8
 - online backup, 11-8
 - partial online backup, 11-2
 - types
 - archived redo log backup, 11-5
 - cold backup, 11-2
 - configuration file backup, 11-5
 - control file backup, 11-5
 - datafile backup, 11-5
 - offline database backup, 11-4
 - online database backup, 11-4
 - partial online backup, 11-2
 - tablespace backup, 11-5
 - whole database backup, 11-5
- Backup and Recovery
 - assumptions, 11-3
 - basics, 11-1
 - customized scripts, 11-3
 - restrictions, 11-3
 - RMAN, 11-3
 - roadmap, 11-2
 - strategy, 11-1
 - understanding, 11-3
- backup files
 - database, 6-30

- blackout time periods
 - defining, 6-11
- blackouts, 6-11
- bootstrapping
 - in integration with Active Directory, 9-48
- browser settings
 - Windows native authentication, 9-42
 - Internet Explorer 5.0, 9-41
 - Internet Explorer 6.0, 9-41, 9-42
- Buffer Cache Advisor
 - description, 10-29
- bulk user management, 4-11

C

- caches
 - Oracle Discussions, 10-2
- cache.xml file
 - ports and, 14-17
- CANCEL command
 - in cancel-based recovery, 11-6
- cancel-based recovery, 11-6
- change-based recovery, 11-6
- changing Infrastructure services, 12-1
- character sets
 - LDAP-based replicas and, 12-27
- chgiphost command, 14-38, 14-42
 - errors, 14-50
 - setting log level, 14-48
- Client Connection Manager
 - increasing number of concurrent connections, 10-13
 - increasing processes, 10-12
- clients
 - maximum number of connections to Client Connection Manager, 10-13
- Cluster Node Addition Progress page, 13-5, 13-9
- Cluster Ready Services (CRS), 13-2
- cold backup, 11-2, 11-8
- complete recovery, 11-5
- component home page, 3-10
- components
 - adding to deployment, 5-64
 - component administration tools, 5-1
 - de-provisioning users from, 4-15
 - disabling, 2-20
 - enabling, 2-20
 - enabling and disabling, 2-20
 - managing, 5-1
 - obtaining status, 2-12
 - provisioning, 4-4
 - starting and stopping, 2-12
 - using opmnctl, 2-13
 - using Oracle Collaboration Suite Control, 2-13
 - typical administration tasks, 5-7
- configuration file backup, 11-5
- configuring components, 5-64
- configuring network, 14-1
- configuring synchronization profiles, 9-17
- configuring user account creation, 4-25
- CONNECT command

- starting a database instance, 6-15
- connections
 - maximum client connections to Client Connection Manager, 10-13
- control file
 - description, 6-25
 - multiplexing, 6-25
- control file backup, 11-5
- control files
 - unavailable during database startup, 6-17
- crash recovery, 11-5
- credentials
 - setting preferred, 6-11
- crssetup.exe command, 13-5
- customizing
 - colors, 15-4
 - colors and fonts
 - Oracle Calendar, 15-5
 - Oracle Mobile Collaboration & Voice, 15-6
 - Oracle Real-Time Collaboration, 15-6
 - Oracle Web Conferencing, 15-6
 - Oracle WebMail, 15-5
 - OracleAS Portal, 15-5
 - fonts, 15-4
 - logos, 15-1
 - Oracle Calendar, 15-2
 - Oracle Mobile Collaboration & Voice, 15-4
 - Oracle Web Conferencing, 15-3
 - Oracle WebMail, 15-2
 - OracleAS Portal, 15-1
 - Oracle Calendar
 - colors and fonts, 15-5
 - Oracle Collaboration Suite, 15-1
 - Oracle Content Services, 15-7
 - Oracle Internet Directory Provisioning
 - Console, 15-6
 - Oracle Mobile Collaboration & Voice
 - colors and fonts, 15-6
 - Oracle Real-Time Collaboration, 15-7
 - colors and fonts, 15-6
 - Oracle Web Conferencing
 - colors and fonts, 15-6
 - OracleAS Portal
 - colors and fonts, 15-5

D

- dads.conf file, 14-26
- data
 - deleting user data, 4-17
- data loss, 11-2
- database
 - Oracle Discussions connection parameters, 10-2
- database blackouts, 6-11
- Database Configuration Assistant (DBCA), 13-10
- Database Control
 - description, 6-2
 - features, 6-2
 - granting administrative privileges to use, 6-10
 - introduction, 3-2
 - online help, 6-2

- starting, 6-4
 - starting a database instance, 6-14, 6-21
 - using, 3-2
- database instances
 - aborting, 6-23
 - shutting down immediately, 6-22
 - transactional shutdown, 6-23
- database listener
 - starting, 6-24
- database roles
 - granting, 6-9
- database user accounts
 - unlocking, 6-9
- databases
 - advisors
 - using, 10-28
 - alerts, 10-19
 - responding to alerts, 10-25
 - setting metrics, 10-23
 - setting notification rules, 10-25
 - viewing metrics, 10-21
 - altering availability, 6-20
 - diagnosing performance problems, 10-26
 - metrics thresholds, 10-19
 - monitoring
 - alert-based, 10-19
 - monitoring performance, 10-19
 - mounting a database, 6-18
 - mounting to a database instance, 6-20
 - opening a closed database, 6-20
 - performance
 - advisors, 10-28
 - read-only, opening, 6-20
 - recovery, 6-19
 - starting up, 6-15
 - storage structure
 - logical structures, 6-24
 - physical structures, 6-24
 - tuning, 10-19
 - users
 - administering, 6-5
 - creating, 6-6
 - editing, 6-8
- datafile backup, 11-5
- datafiles
 - description, 6-29
 - unavailable when database is opened, 6-17
- DBCA. *See* Database Configuration Assistant.
- DCM schema
 - changing password, 6-43, 6-46
- dcmCache.xml file
 - ports and, 14-18
- dcmctl, 3-21
- dcmctl command, 2-20
 - updating configuration, 14-31
- dcmctl utility
 - introduction, 3-3
- default port number, A-1
- Delegated Administration Service
 - updating, 14-34

- deleting user accounts, 4-17
- deleting user data, 4-17
- De-provisioning, 4-15
- diagnosing component problems, 8-11
- diagnostics
 - messages, 8-10
 - repository for, 8-21
 - understanding messages, 8-14
- DirSync control-based synchronization, 9-5
- disabling components, 2-20
- disabling users, 4-15
- DISCOVERER5 schema
 - changing password, 6-43
- DISPLAY environment variable, 1-2
- distinguished name (DN)
 - configuring parent DN for a realm, 4-38
- distinguished name mapping
 - in Active Directory integration, 9-19
- Distributed Configuration Management (DCM)
 - message correlation, 8-10
 - ports, A-3
 - changing, 14-18
- distributed databases
 - starting a remote database instance, 6-19
- dms.conf file, 14-20
- dms.transtrace.ecidenabled property, 8-20
- DN. *See* distinguished name.
- Document Conversion Server
 - starting, 2-18
- domain name
 - changing, 14-36
 - Applications tier, 14-36
 - Identity Management, 14-40
- DSGATEWAY schema
 - changing password, 6-43
- Dual Mode, 12-3

E

- ECID
 - See* Execution Context ID (ECID)
- editing users, 4-12
- emctl command, 14-3
 - configuration changes, 14-4
- enabling and disabling components, 2-20
- enabling components, 2-20
- enabling user accounts, 4-15
- enblhstg.csh script, 7-5
- End-User Documentation Portal, 5-30
 - about, 5-31
 - customizing, 5-32
 - directory structure, 5-37
 - editing content, 5-39
 - setting up, 1-12
 - static version, 5-37
 - views, 5-34
- environment variables, 1-1
- error messages
 - log loader, 8-14
- errors
 - ORA-01090, 6-22

- while starting a database, 6-19
- while starting a database instance, 6-19
- EXAMPLE tablespace, 6-28
- Execution Context ID (ECID), 8-10
- export operations
 - restricted mode and, 6-18
- express configuration
 - by using the Oracle Directory Integration and Provisioning Server Administration tool, 9-31
 - of Active Directory Connector profiles, 9-29
 - using, 9-30
- external authentication
 - plug-in
 - Active Directory, 9-49
 - for integration with Active Directory, 9-36
 - for integration with Microsoft Active Directory, 9-3
- external authentication plug-in
 - Active Directory
 - enabling, 9-37
 - installing, 9-36
 - testing, 9-37

F

- Farm home page, 3-7
- file descriptors, increasing, 10-14
- first-fault component isolation, 8-10
- foreign security principal, defined, 9-13
- foreign security principals
 - in Oracle Internet Directory
 - synchronizing with Active Directory, 9-44
- foreign security principals, in Microsoft Active Directory, 9-12

G

- Grid Control
 - Console home page, 3-19
 - installing, 3-18
 - introduction, 3-1
 - logging in, 3-18
 - managing Oracle Collaboration Suite, 3-16
 - managing Oracle Voicemail & Fax, 5-6
 - monitoring with, 3-19
 - password, 3-19
 - starting a database instance, 6-14, 6-21
 - using, 3-2
- Grid Control Console
 - about, 5-3
- groupcreatebase
 - configuring in integration with Active Directory, 9-16
- groups
 - managing, 4-22
- groupsearchbase
 - configuring in integration with Active Directory, 9-16

H

- high-availability, 13-1
- home page
 - using, 3-9
- home pages, 3-2
- host failure, 11-2
- hostname
 - changing, 14-36
 - after Windows 2000 upgrade, 14-50
 - Applications tier, 14-36
 - Identity Management, 14-40
 - references to, 14-39
- httpd.conf file
 - port directive and, 14-11, 14-31

I

- ias.properties file, 12-4
- ias.properties file
 - OID port and, 14-28, 14-29
- iaspt.conf file
 - port tunneling and, 14-21
- Identity Management
 - failover, 12-12
 - moving to a new host, 12-6
- identity management infrastructure database
 - support for multiple realms, 7-1
- Identity Management Realms, 4-37
 - adding, 4-39
- identity management realms
 - about, 9-7
 - access control policies in, 9-9
 - administrative privileges, 7-7
 - authentication dynamics, 7-3, 7-4
 - configuring, 7-4 to 7-7
 - default, 9-8
 - overview, 7-1
 - support for partner applications, 7-3
- identity management realms
 - multiple, 9-8
- IMAP
 - Oracle Web Access Client IMAP mode, 5-55
- IMMEDIATE option for database shutdown, 2-22
- import operations
 - restricted mode and, 6-18
- incomplete recovery, 11-6
- indexing
 - Oracle Content Services, 5-12
- Infrastructure
 - changing services, 12-1
 - ports, A-4
 - changing, 14-22
 - re-association, 12-1
 - starting, 2-4
- Infrastructure Services
 - LDAP-based replica and, 12-26
- Infrastructure tier
 - starting, 2-4
 - stopping, 2-6
- Infrastructure tiers
 - scripted starting, 2-5
 - scripted stopping, 2-7
 - starting, 2-4
 - starting manually, 2-4
 - stopping, 2-6
 - stopping manually, 2-6
- init\$SID.ora file
 - OracleAS Metadata Repository and, 6-40
- initialization parameter file
 - server parameter file, 6-16
- initialization parameters
 - memory parameters, 6-38
 - SPFILE, 6-16
 - viewing, 6-36
- init.ora
 - in configuration file backup, 11-5
- installing
 - Grid Control, 3-18
- instance recovery, 11-5
- instances
 - Oracle Real-Time Collaboration, starting and stopping, 2-18
 - shutting down normally, 6-22
- integration
 - with a single Active Directory domain controller, 9-10
 - with Active Directory, 9-17, 9-19
 - configuring connection details, 9-18
 - configuring mapping rules, 9-18
 - customizing search filter, 9-22
 - in SSL mode, 9-26
 - setting the user login name attribute, 9-16
 - setting user and group search bases, 9-16
 - with Active Directory as the central directory, 9-14
 - with OID as the central directory, 9-13
 - with Microsoft Active Directory
 - Active Directory Connector, 9-3
 - concepts and architecture, 9-1
 - configuration of, 9-16
 - Oracle Directory Integration and Provisioning component, 9-2
 - Oracle Internet Directory component, 9-2
 - setting the user login name attribute, 9-16
 - with multiple Active Directory domain controllers, 9-11
- integration profile
 - enabling, 9-47
- integration with Microsoft Active Directory
 - deployment options, 9-13
- Interactive Voice Response (IVR), 5-7
- INTERNAL username
 - connecting for shutdown, 6-22
- IP address
 - changing, 14-36
- IP schema
 - changing password, 6-43
- IPC Listener
 - KEY value, 14-26
- iSQL*Plus
 - connecting after adding a RAC node, 13-12

- isqlplus
 - starting, 6-13

J

- J2EE
 - ports, A-2
- Java API, user provisioning, C-1
- Java object cache
 - ports, A-3
 - changing, 14-19
- javacache.xml file
 - ports and, 14-19

K

- Kerberos protocol, 9-4

L

- LD_LIBRARY_PATH environment variable, 1-2
- LD_LIBRARY_PATH_64 environment variable, 1-2
- LDAP
 - recommended Oracle Mail connection
 - settings, 10-7
 - LDAP schema, customizing, 9-21
 - LDAP-based replicas, 12-25
 - installing, 12-27
 - ports, 12-27
 - ldapmodify command, 12-27
 - ldap.ora file, 12-4
 - ldap.ora file
 - ports and, 14-28
 - ldapssearch command, 12-27
 - viewing schema passwords with, 6-42
 - limit command, increasing to support simultaneous client connections, 10-13
 - limits.conf file, 10-13
 - List of Cluster Databases page, 13-10
 - listener.ora file, 12-24
 - locked accounts, 4-15
 - log files, B-1
 - component IDs, 8-18
 - limitations, 8-23
 - listing, 8-4
 - names, 8-3
 - naming, 8-2
 - Oracle Content Services, B-1
 - registration, 8-18
 - searching, 8-5, 8-9
 - size, 8-3
 - log loader, 8-2
 - enabling, 8-12
 - file format conversion, 8-18
 - ports, A-3
 - changing, 14-19
 - setting properties, 8-13
 - starting and stopping, 2-21, 8-12
 - log repository, 8-2
 - log sequence number
 - in offline database backup, 11-4
 - log sequence number

- in online database backup, 11-4
- logging
 - configuring options, 8-3
- login scenarios
 - Windows native authentication, 9-43
- logloader.xml file, 8-14
- logos
 - customizing, 15-1
- logs, B-1
 - Oracle Calendar, B-1
 - Oracle Discussions, 10-3
 - Oracle Mail, B-2
 - Oracle Mobile Collaboration, B-2
 - Oracle Real-Time Collaboration, B-3
 - Oracle Voicemail & Fax, B-4
 - OracleAS Wireless, B-2

M

- managing, 9-47
 - groups, 4-22
 - Oracle Collaboration Suite applications, 5-1
 - users and groups, 4-1
 - managing Oracle Collaboration Suite
 - with command-line interfaces, 3-3
 - managing Oracle Collaboration Suite
 - using Oracle Directory Manager, 3-20
 - managing users, 4-7
 - mapping rules
 - customizing for Active Directory
 - integration, 9-19
 - in integration with Active Directory, 9-18
 - media failure, 11-2
 - media recovery, 11-5
 - memory
 - auto tuning, 6-38
 - managing, 6-38
 - Memory Advisor
 - description, 10-29
 - using, 10-30
 - message correlation, 8-10
 - metrics
 - monitoring, 3-19
 - Microsoft Active Directory
 - and Active Directory Connector, 9-3
 - concepts and architecture for integration
 - with, 9-1
 - configuration of integration with, 9-16
 - deployment options for integration with, 9-13
 - external authentication with, 9-3
 - foreign security principals, 9-12
 - forest, as mapped to Oracle Internet Directory, 9-11
 - integration
 - post-configuration tasks, 9-47
 - typical management tasks, 9-47
 - managing, 9-47
 - multiple domain
 - synchronizing with, 9-26
 - synchronizing deletions from, 9-23
 - trust relationships between domains, 9-12

- mod_imeeting HTTP connection
 - port, A-7
- mod_imeeting HTTPS connection
 - port, A-7
- mod_imeeting HTTPS tunnel connection
 - port, A-7
- mod_osso
 - port numbers and, 14-12, 14-33
- modifying users, 4-12
- monitoring
 - components, 3-14
 - J2EE applications, 3-15
 - Oracle Real-Time Collaboration processes, 10-12
 - performance metrics, 3-19
 - with Oracle Collaboration Suite Control, 3-11
- monitoring and tuning, 10-1
- MOUNT clause
 - STARTUP command, 6-18
- mounting a database, 6-18
- multiple Active Directory domain controllers
 - integration with, 9-11
- multiple installations on one host, 1-2
- multiple-domain Active Directory, synchronizing
 - with, 9-26
- Multiplexer
 - increasing number of concurrent
 - connections, 10-13
 - increasing processes, 10-12

N

- network configurations, 14-1
- new features, xxxiii
- NLS_LANG environment variable
 - LDAP-based replicas and, 12-27
- NOARCHIVELOG mode, 11-6
 - in datafile backup, 11-5
 - in offline database backup, 11-5
 - in tablespace backup, 11-5
- Node Addition Summary page, 13-4, 13-8
- NOMOUNT clause
 - STARTUP command, 6-18
- nontransitive trust relationship in Active
 - Directory, 9-13
- notification of alerts
 - alert notification, 6-11

O

- OC4J
 - See* Oracle Application Server Containers for J2EE (OC4J)
- OC4J_OCSClnt process, 2-16
- OCA schema
 - changing password, 6-43
- ocactl command, 14-25
- ODL
 - See* Oracle Diagnostic Logging (ODL)
- ODL Archives, 8-17
- ODL log, 8-17
- ODS schema
 - changing password, 6-43

- offline database backup, 11-4
- oidProvTool paramaters, 4-30
- oidprovtool utility, C-6
- oifcfg utility, 13-10
- olsnodes command, 13-5
- online backup, 11-8
- online database backup, 11-4
- opmnctl
 - starting and stopping components, 2-13
 - using instead of other command-line tools for
 - starting and stopping, 2-20
- opmnctl command, 2-13, 3-21
- opmn.xml file
 - ports and, 14-20
- Oracle Application Server Containers for J2EE (OC4J)
 - configuring for ECIDs, 8-20
 - dms.transtrace.ecidenabled property, 8-20
 - message correlation, 8-10
 - ODL messages, 8-20
 - ports, A-2
 - changing, 14-4, 14-19
 - RMI port
 - changing, 14-3
- Oracle Application Server Portal. *See* OracleAS Portal.
- Oracle Application Server Single Sign-On
 - and integration with Active Directory, 9-3
 - and Windows native authentication, 9-3
- Oracle Application Server Wireless System
 - Management, 5-7
- Oracle Calendar, 5-11
 - access in Oracle Workspaces, 5-62
 - administration tasks, 5-8
 - administration tools, 5-2
 - changing schema password, 6-50
 - command-line utilities, 5-2
 - customizing
 - colors and fonts, 15-5
 - logos, 15-2
 - deleting user data, 4-18
 - logs, B-1
 - performance tuning, 10-1
 - ports, A-5
 - provisioning, 4-4
 - starting and stopping, 2-14
 - unistatus command, 2-14
 - user attributes, 4-19
 - verifying configuration, 1-10
- Oracle Calendar Administrator, 5-2
- Oracle Calendar Application System
 - ports, A-6
- Oracle Calendar Directory Access Server
 - ports, A-5
- Oracle Calendar Engine
 - ports, A-5
- Oracle Calendar ochecklet
 - ports, A-6
- Oracle Calendar Server
 - configuring Manual Cold Failover, 13-19
- Oracle Calendar Server Manager
 - ports, A-6

- Oracle Calendar Synchronous Network Connection ports, A-5
- Oracle Cluster File System (OCFS), 13-6
- Oracle Cluster Registry (OCR), 13-6
- Oracle Collaboration Suite
 - administration tools, 3-1
 - customizing, 15-1
 - Farm home page, 3-7
 - management tools, 3-1
 - monitoring and tuning, 10-1
 - starting and stopping, 2-1
 - overview, 2-2
 - scripted, 2-3
 - Welcome Page, 3-8
- Oracle Collaboration Suite Calendar utilities, 11-3
- Oracle Collaboration Suite components
 - starting and stopping, 2-12
- Oracle Collaboration Suite Control
 - component home page, 3-10
 - displaying the Console, 3-7
 - getting started, 3-6
 - home page
 - using, 3-9
 - introduction, 3-1
 - ports, changing, 14-3
 - starting and stopping components, 2-13
 - underlying technologies, 3-6
 - using, 3-4
- Oracle Collaboration Suite Database
 - adding or deleting RAC nodes, 13-17
 - starting and stopping, 2-11
 - shutting down with the IMMEDIATE option, 2-22
- Oracle Collaboration Suite environment
 - managing, 3-3
- Oracle Collaboration Suite home page, 3-9
- Oracle Collaboration Suite home pages, 3-5
- Oracle Collaboration Suite Search, 5-11
 - configuring, 5-13
 - indexing Oracle Discussions, 5-30
 - monitoring, 5-13
 - starting and stopping, 2-19
- Oracle Collaboration Suite Welcome Page, 3-8
- Oracle Collaboration Suite Welcome page, 1-5
 - accessing, 1-6
- Oracle Collaborative Portlets, 5-40
 - changing host or ports, 5-43
 - configuring after installation, 5-42
 - managing, 5-43
- Oracle Collaborative Portlets Configuration Assistant, 5-43
- Oracle Contacts, 5-15
 - managing default categories, 5-15
 - managing maximum entries, 5-17
- Oracle Content Services
 - access in Oracle Workspaces, 5-62
 - administration tasks, 5-9
 - changing the schema password, 6-50
 - customizing, 15-7
 - deployment options, 1-3
 - enabling and disabling, 2-20
 - getting started, 1-3
 - indexing, 5-12
 - logs, B-1
 - performance tuning, 10-12
 - ports, A-6
 - provisioning, 4-5
 - removing user data, 4-18
 - Site quota notifications, 1-3
 - starting and stopping, 2-15
 - node processes across multiple Applications tiers, 2-15
 - node processes on a single Applications tier, 2-15
 - sub-processes, 2-16
 - verifying configuration, 1-9
 - WebDAV URL, 1-10
- Oracle database listener
 - starting, 6-24
- Oracle Delegated Administration Services (DAS), 4-2
- Oracle Diagnostic Logging (ODL), 8-2
 - file naming, 8-17
 - message format, 8-15
- Oracle Directory Integration and Provisioning
 - as a component in integration with Active Directory, 9-2
 - how it maintains synchronization, 9-5
- Oracle Directory Manager, 3-20
 - introduction, 3-2
 - Password Policies Account Lockout tab
 - page, 4-36
 - Password Policies General tab page, 4-34
 - Password Policies IP Lockout tab page, 4-36
 - Password Policies Password Syntax tab
 - page, 4-36
 - using to edit Service Registry, 7-10
 - viewing schema passwords with, 6-41
- Oracle Discussions, 5-18
 - access control, 5-20
 - access in Oracle Workspaces, 5-63
 - administration tasks, 5-23
 - announcements, 5-28
 - caches, 10-2
 - categories, 5-24
 - clipping, 5-28
 - connection parameters, 10-2
 - database connection parameters
 - Oracle Collaboration Suite Database, 10-2
 - e-mail integration, 5-28
 - forums, 5-25
 - integration with Oracle Mail, 5-19
 - introduction, 5-19
 - locking forums and topics, 5-27
 - logs, 10-3
 - managing roles, 5-23
 - Oracle Internet Directory connection
 - parameters, 10-2
 - performance tuning, 10-1
 - role permissions, 5-22

- RSS, 5-30
- search, 5-30
- setting an administrator account, 1-4
- starting and stopping, 2-16
- Web UI defaults, 5-27
- Oracle Enterprise Manager, 2-5, 2-10
 - ports, A-3, A-4
 - changing, 14-3
- Oracle Enterprise Manager 10g Application Server
 - Control for Collaboration Suite. *See* Oracle Collaboration Suite Control
- Oracle Enterprise Manager 10g Database Control. *See* Database Control
- Oracle Enterprise Manager 10g Grid Control. *See* Grid Control.
- Oracle Enterprise Manager Grid Control
 - See* Grid Control
- Oracle Enterprise Manager Grid Control Console. *See* Grid Control.
- Oracle HTTP Server
 - configuring for ODL, 8-20
 - message correlation, 8-11
 - port directive
 - updating ports, 14-11
 - ports, A-2
 - changing, 14-6, 14-30
 - changing diagnostic, 14-20
 - less than 1024, 14-6, 14-32
- Oracle Identity Management Provisioning Console.
 - See* Oracle Internet Directory Provisioning Console.
- Oracle Identity Management Self-Service Console. *See* Oracle Internet Directory Provisioning Console.
- Oracle Internet Directory
 - as a component in integration with Active Directory, 9-2
 - changing domain name, 14-37
 - changing from Dual Mode to SSL Mode, 12-3
 - changing hostname, 14-37
 - changing modes, 12-3
 - configuring for Windows native authentication, 9-39
 - connection parameters for Oracle Discussions, 10-2
 - modifying RAC database connect string, 13-17
 - ports, A-4
 - changing, 14-27
 - updating, 14-25
 - schema elements for integration with Active Directory, 9-7
- Oracle Internet Directory Provisioning Console
 - getting started, 4-6
 - introduction, 4-1
 - managing users, 4-7
- Oracle Internet Directory Service Registry, 7-7
 - editing, 7-10
 - introduction, 7-7
 - stored URIs, 7-8
- Oracle Mail
 - administration tasks, 5-8
 - administration tools, 5-2
 - architecture, 10-4
 - changing schema password, 6-51
 - command-line utilities, 5-3
 - database process parameter settings, 10-9
 - deleting user data, 4-18
 - integration with Oracle Discussions, 5-19
 - log files, B-2
 - logs, B-2
 - parameter recommendations, 10-7
 - performance tuning, 10-4
 - processes, 10-4
 - provisioning, 4-5
 - recommended database connection settings, 10-7
 - recommended LDAP connection settings, 10-7
 - Setting an administrator account, 1-4
 - starting and stopping, 2-17
 - starting, stopping, 2-17
 - user attributes, 4-20
- Oracle Management Agent, 3-6, 3-18
 - ports, A-5
 - changing, 14-3
- Oracle Management Service
 - ports, A-5
- Oracle Management Watchdog Process, 3-6
- Oracle Mobile Collaboration
 - administration tasks, 5-10
 - administration tools, 5-7
 - changing domain name and, 14-39
 - changing hostname and, 14-39
 - logs, B-2
 - performance tuning, 10-14
 - ports, A-3
 - changing, 14-21
 - updating, 14-15
 - starting and stopping, 2-17
 - verifying configuration, 1-12
- Oracle Mobile Collaboration & Voice
 - customizing
 - colors and fonts, 15-6
- Oracle Process Manager and Notification Server (OPMN)
 - ports, A-2
- Oracle Real Applications Clusters
 - in instance recovery, 11-5
- Oracle Real-Time Collaboration
 - administering using Web Client, 5-4
 - administration tasks, 5-9
 - administration tools, 5-4
 - changing schema password, 6-52
 - customizing, 15-7
 - colors and fonts, 15-6
 - Oracle Mobile Collaboration & Voice
 - logo, 15-4
 - Oracle Web Conferencing logo, 15-3
 - deleting user data, 4-18
- Document Conversion Server
 - starting, 2-18
- logs, B-3
- performance tuning, 10-12

- ports, A-7
- Process Manager
 - port, A-7
- provisioning, 4-5
- Redirector server listening point
 - port, A-7
- Redirector to Oracle Presence Server
 - port, A-7
 - SSL port, A-7
- rtctctl utility, 5-4
- setting a business administrator account, 1-4
- starting and stopping, 2-18
- starting instances, 2-18
- verifying configuration, 1-10
- Voice Conversion Server
 - port, A-7
 - starting, 2-18
- Voice Proxy Server
 - port, A-7
- Oracle Ultra Search, 5-11
 - character sets and, 6-47
 - configuring, 5-13
 - modifying crawler connect string for RAC, 13-18
- Oracle Collaboration Suite Search
 - integration, 5-13
- performance tuning, 10-12
- ports, A-3
- Oracle Universal Installer, definition of, Glossary-xv
- Oracle Voicemail & Fax
 - Accounts Manager, 5-6
 - administration tasks, 5-10
 - administration tools, 5-6
 - configuring, 1-11
 - deleting user data, 4-18
 - de-provisioning users, 4-17
 - Interactive Voice Response (IVR), 5-7
 - logs, B-4
 - performance tuning, 10-14
 - provisioning, 4-5
 - required services, 1-11
 - starting and stopping, 2-19
 - user attributes, 4-21
 - verifying configuration, 1-11
- Oracle Web Access Client, 5-45
 - configuring, 5-47
 - default settings, 5-52
 - IMAP mode, 5-55
 - performance metrics, 5-47
- Oracle Web Conferencing
 - customizing
 - colors and fonts, 15-6
 - stopping instances, 2-18
- Oracle WebMail
 - administering, 5-3
 - customizing
 - colors and fonts, 15-5
 - logos, 15-2
 - performance tuning, 10-9
- Oracle WebMail client
 - accessing, 5-3
- Oracle Workspaces, 5-59
 - access control, 5-61
 - introduction, 5-60
 - managment tasks, 5-64
 - performance tuning, 10-15
 - sizing, 10-15
 - starting and stopping, 2-19
 - verifying configuration, 1-12
- ORACLE_HOME
 - environment variables, 11-3
- ORACLE_HOME environment variable, 1-2
- ORACLE_SID
 - environment variable, 11-3
- ORACLE_SID environment variable, 1-2
- OracleAS Certificate Authority
 - ports
 - updating, 14-25, 14-34
- OracleAS Cluster
 - changing domain name and, 14-37
 - changing hostname and, 14-37
- OracleAS Metadata Repository, 5-42
 - changing, 12-13
 - database features and, 6-39
 - definition, 6-39
 - managing, 3-2
 - managing using Oracle Directory Manager, 3-20
 - moving, 12-13
 - ports, changing, 14-22
 - schema passwords, 6-41
 - schemas
 - deleting, 6-41
 - tuning, 6-40
- OracleAS Portal, 5-40
 - changing domain name and, 14-39
 - changing hostname and, 14-39
 - configuring after installation, 5-42
 - customizing
 - colors and fonts, 15-5
 - logos, 15-1
 - managing, 5-40
 - message correlation, 8-11
 - performance tuning, 10-12
 - ports, A-3
 - changing, 14-21
 - updating, 14-13, 14-17
- OracleAS Single Sign-On
 - ports, updating, 14-25, 14-33
 - scripts
 - addsub.csh, 7-5
 - enblhstg.csh, 7-5
- OracleAS Web Cache
 - message correlation, 8-11
 - ports, A-2
 - changing administration, 14-16
 - changing HTTP listen, 14-10
 - changing HTTPS listen, 14-11
 - changing invalidation, 14-17
 - changing statistics, 14-18
 - less than 1024, 14-10
- OracleAS Wireless

- changing domain name and, 14-39
- changing hostname and, 14-39
- logs, B-2
- performance tuning, 10-14
- ports, A-3
 - changing, 14-21
 - updating, 14-15
- OracleAS Wireless System Management, 5-7
- oraInstRoot.sh script, 13-8
- ORAOCA schema
 - changing password, 6-43
- ORASSO schema
 - changing password, 6-43
- ORASSO_DS schema
 - changing password, 6-43
- ORASSO_PA schema
 - changing password, 6-43
- ORASSO_PS schema
 - changing password, 6-44
- ORASSO_PUBLIC schema
 - changing password, 6-44
- orcladmin account, 1-3
- OWF_MGR schema
 - changing password, 6-44, 6-46

P

- partial online backup, 11-2
- password files
 - database, 6-30
- Password Policies Account Lockout tab page, in Oracle Directory Manager, 4-36
- Password Policies General tab page, in Oracle Directory Manager, 4-34
- Password Policies IP Lockout tab page, in Oracle Directory Manager, 4-36
- Password Policies Password Syntax tab page, in Oracle Directory Manager, 4-36
- passwords
 - changing default policies, 4-32
 - Grid Control, 3-19
 - not migrated from Microsoft Active Directory to Oracle Internet Directory, 9-15
 - OracleAS Metadata Repository, 6-41
 - schema, 6-50, 6-51, 6-52
 - users, 4-14
- PATH environment variable, 1-2
- performance metrics
 - monitoring, 3-19
- performance tuning, 10-1
 - Oracle Calendar, 10-1
 - Oracle Content Services, 10-12
 - Oracle Discussions, 10-1
 - Oracle Mail, 10-4
 - Oracle Mobile Collaboration, 10-14
 - Oracle Ultra Search, 10-12
 - Oracle Voicemail & Fax, 10-14
 - Oracle WebMail, 10-9
 - Oracle Workspaces, 10-15
 - OracleAS Portal, 10-12
 - OracleAS Wireless, 10-14

- performing tuning
 - Oracle Real-Time Collaboration, 10-12
- PGA Advisor
 - description, 10-29
- PITR, 11-6
- planning the Active Directory integration, 9-9
- plug-ins
 - external authentication
 - for integration with Active Directory, 9-36
- point-in-time recovery, 11-6
- policies
 - provisioning, 4-2
- port nubers
 - Oracle Calendar, A-5
- port numbers
 - DCM Discovery, A-3
 - Infrastructure, A-4
 - J2EE, A-2
 - Java object cache, A-3
 - LDAP-based replicas and, 12-27
 - log loader, A-3
 - mod_meeting HTTP connection, A-7
 - mod_meeting HTTPS connection, A-7
 - mod_meeting HTTPS tunnel connection, A-7
 - Oracle Application Server Containers for J2EE (OC4J), A-2
 - Oracle Calendar Application System, A-6
 - Oracle Calendar Directory Access Server, A-5
 - Oracle Calendar Engine, A-5
 - Oracle Calendar ochecklet, A-6
 - Oracle Calendar Server Manager, A-6
 - Oracle Calendar Synchronous Network Connection, A-5
 - Oracle Content Services, A-6
 - Oracle Enterprise Manager, A-3, A-4
 - Oracle HTTP Server, A-2
 - Oracle Internet Directory, A-4
 - Oracle Mobile Collaboration, A-3
 - Oracle Process Manager and Notification Server (OPMN), A-2
 - Oracle Real-Time Collaboration, A-7
 - Process Manager, A-7
 - Redirector server listening point, A-7
 - Redirector to Oracle Presence Server, A-7
 - Redirector to Oracle Presence Server SSL, A-7
 - Voice Conversion Server, A-7
 - Voice Proxy Server, A-7
 - Oracle Ultra Search, A-3
 - OracleAS Portal, A-3
 - OracleAS Web Cache, A-2
 - OracleAS Wireless, A-3
- port tunneling, A-3
 - updating, 14-13, 14-17
 - viewing, 14-2
- port tunneling
 - ports, A-3
 - changing, 14-21
- PORTAL schema
 - changing password, 6-44
- PORTAL_APP schema

- changing password, 6-44
- PORTAL_DEMO schema
 - changing password, 6-44
- PORTAL_PUBLIC schema
 - changing password, 6-44
- portconfig command, 14-6
- portlist.ini, 1-7
- ports
 - changing
 - Applications tier, 14-2
 - Distributed Configuration Management (DCM), 14-18
 - infrastructure, 14-22
 - Java object cache, 14-19
 - log loader, 14-19
 - logical site, 14-11
 - OPMN, 14-19
 - Oracle Application Server Containers for J2EE (OC4J), 14-4
 - Oracle Enterprise Manager, 14-3
 - Oracle HTTP Server, 14-6, 14-30
 - Oracle HTTP Server diagnostic, 14-20
 - Oracle Internet Directory, 14-27
 - Oracle Management Agent, 14-3
 - Oracle Mobile Collaboration, 14-21
 - OracleAS Metadata Repository, 14-22
 - OracleAS Portal, 14-21
 - OracleAS Web Cache administration, 14-16
 - OracleAS Web Cache HTTP listen, 14-10
 - OracleAS Web Cache HTTPS listen, 14-11
 - OracleAS Web Cache invalidation, 14-17
 - OracleAS Web Cache statistics, 14-18
 - OracleAS Wireless, 14-21
 - port tunneling, 14-21
- changing on a tier hosting Oracle Collaborative Portlets, 5-43
- checking after installation, 1-7
- less than 1024, 14-10, 14-32
- managing, 14-1
- updating
 - Oracle Internet Directory, 14-25
 - Oracle Mobile Collaboration, 14-15
 - OracleAS Certificate Authority, 14-25, 14-34
 - OracleAS Portal, 14-13, 14-17
 - OracleAS Single Sign-On, 14-25, 14-33
 - OracleAS Wireless, 14-15
- Web Providers, 14-17
- preferred credentials, 6-11
 - setting, 6-11
- printlogs command, 8-15
- privileges
 - assigning to users, 4-13
 - RESTRICTED SESSION system privilege, 6-18
- process or system outages, 11-3
- process outages, 11-3
- processes
 - increasing server and listening processes, 10-12
 - monitoring for Oracle Real-Time Collaboration, 10-12
- Provisioning

- managing Identity Management Realms, 4-37
- provisioning, 4-4
 - API
 - creating a user, C-14
 - debugging, C-16
 - deleting a user, C-15
 - looking up a user, C-15
 - modifying a user, C-15
 - sample code, C-16
 - application configuration, C-1
 - application configuration classes, C-13
 - application registration, C-1
 - components, 4-4
 - configuration, C-3
 - configuring user account creation, 4-25
 - for applications, 4-4
 - interfaces, C-7
 - introduction, 4-1
 - Java API, C-1
 - Java plug-ins, C-17
 - data access plug-in, C-21
 - data entry plug-in, C-18
 - plug-in return status, C-22
 - post-data-entry plug-in, C-21
 - pre-data-entry plug-in, C-20
 - requirements, C-18
 - sample code, C-24
 - template, C-23
 - types, C-17
 - Oracle Calendar, 4-4
 - Oracle Content Services, 4-5
 - Oracle Mail, 4-5
 - Oracle Real-Time Collaboration, 4-5
 - Oracle Voicemail & Fax, 4-5
 - plugin, C-13
 - policies, 4-28
 - privileged groups, C-3
 - profiles, 4-29
 - user management, C-13
- Provisioning Console
 - customizing look and feel, 15-6
- provisioning policies, 4-2
- provisioning subscription tool, 4-30

R

RAC

- adding a node
 - overview, 13-1
- adding a node on a shared Oracle home, 13-13
- Adding an Instance page, 13-11
- adding and removing nodes, 13-1
- adding database instances to new nodes, 13-10
- adding nodes at the database layer, 13-8
- Adding nodes that already have
 - clusterware, 13-12
- adding or deleting nodes from a database, 13-17
- Cluster Node Addition Progress page, 13-5, 13-9
- clusters
 - adding new nodes, 13-2
 - extending clusterware to new nodes, 13-3

- Database Configuration Assistant (DBCA), 13-10, 13-13
- deleting instances from a database, 13-13
- deleting nodes from Oracle Clusters, 13-14, 13-16
- Instance Storage page, 13-11
- List of Cluster Databases page, 13-10
- modifying database connect string in Oracle Internet Directory, 13-17
- Node Addition Summary page, 13-4, 13-8
- preparing storage on new nodes, 13-6
- removing nodes from load-balanced applications, 13-19
- Services page, 13-11
- Virtual IP Configuration Assistant (VIPCA), 13-9
- racgons utility, 13-6
- read-only database
 - opening, 6-20
- Real Application Clusters. *See* RAC.
- realms
 - about, 9-7
 - access control policies in, 9-9
 - configuring in Active Directory integration, 9-16
 - default, 9-8
 - Identity Management Realms, 4-37
 - multiple, 9-8
- re-association
 - Infrastructure, 12-1
- RECOVER, 11-6
- RECOVER clause
 - STARTUP command, 6-19
- Recovery
 - types, 11-5
- recovery
 - types
 - cancel-based recovery, 11-6
 - change-based recovery, 11-6
 - complete recovery, 11-5
 - crash recovery, 11-5
 - data loss, 11-2
 - host failure, 11-2
 - incomplete recovery, 11-6
 - instance recovery, 11-5
 - media failure, 11-2
 - media recovery, 11-5
 - PITR, 11-6
 - point-in-time recovery, 11-6
 - process outages, 11-3
 - system outages, 11-3
 - tablespace point-in-time recovery, 11-6
 - time-based recovery, 11-6
 - TSPITR, 11-6
- Recovery Manager
 - starting a database, 6-15, 6-22
 - starting a database instance, 6-15
- redo log files
 - description, 6-26
 - multiplexing, 6-26
 - unavailable when database is opened, 6-17
- registration
 - log files, 8-18

- replication, 12-25
- repository.jar file, C-1
- RESETLOGS option, 11-6
- resource usage, 3-12
- resources
 - viewing, 3-13
- RESTORE, 11-6
- RESTRICT clause
 - STARTUP command, 6-18
- RESTRICTED SESSION system privilege
 - restricted mode and, 6-18
- RMAN, 11-3, 11-6
 - BACKUP AS COPY command, 11-6
 - BACKUP command, 11-6
 - in control file backup, 11-5
 - RECOVER command, 11-6
 - RESTORE command, 11-6
- RMAN. *See* Recovery Manager.
- rollback segments
 - description, 6-27
- rootaddnode.sh script, 13-5
- rtctctl utility, 5-4

S

- sample code
 - provisioning
 - Java plug-ins, C-24
 - provisioning API, C-16
- schema passwords
 - changing
 - Oracle Calendar, 6-50
 - changing for Oracle Content Services, 6-50
 - changing for Oracle Mail, 6-51
 - changing for Oracle Real-Time Collaboration, 6-52
 - viewing for OracleAS Metadata Repository, 6-41
- schemas
 - for OracleAS Metadata Repository
 - deleting, 6-41
- SCN
 - in change-based recovery, 11-6
 - in offline database backup, 11-4
 - in online database backup, 11-4
- SCOTT schema
 - changing password, 6-44
- scripted starting and stopping, 2-3
- search filter, customizing in Active Directory
 - integration, 9-22
- search. *See*
- searching
 - for user accounts using the Provisioning Console, 4-36
- searchlet, 5-11
- Segment Advisor
 - description, 10-29
 - using, 6-31
- server parameter file
 - STARTUP command behavior, 6-15
- Service Registry, 7-7
 - editing, 7-10

- introduction, 7-7
- stored URIs, 7-8
- setupinfo.txt, 3-8
- Shared Pool Advisor
 - description, 10-29
- SHLIB_PATH environment variable, 1-2
- SHUTDOWN ABORT
 - in crash recovery, 11-5
- SHUTDOWN command
 - ABORT clause, 6-23
 - IMMEDIATE clause, 6-23
 - NORMAL clause, 6-22
 - shutting down a database, 6-22
 - TRANSACTIONAL clause, 6-23
- SHUTDOWN IMMEDIATE, 2-22
- shutting down a database
 - SQL*Plus, 6-22
- shutting down a database instance
 - SQL*Plus, 6-22
- Simple and Protected GSS-API Negotiation Mechanism (SPNEGO), 9-4
- single Active Directory domain controller, integration with, 9-10
- single sign-on server
 - configuring for Windows native authentication, 9-39 to ??
- Sites, Oracle Content Services, 1-3
- spfile
 - in configuration file backup, 11-5
- SPFILE initialization parameter
 - specifying from client machine, 6-16
- SPNEGO protocol, 9-4
- SQL Access Advisor
 - description, 10-29
 - using, 10-30
- SQL statements
 - about, 6-12
- SQL Tuning Advisor
 - description, 10-29
 - using, 10-29
- SQL*Plus
 - shutting down a database, 6-22
 - shutting down a database instance, 6-22
 - starting, 6-15
 - starting a database instance, 6-15
- sqlplus
 - starting, 6-12
- SSL
 - and Active Directory integration, 9-26
- SSL Mode, 12-3
- ssl.conf file
 - port directive and, 14-11, 14-32
- starting
 - databases, 6-15
- starting a database
 - forcing, 6-19
 - Oracle Enterprise Manager, 2-5, 2-10
 - recovery and, 6-19
 - Recovery Manager, 6-15, 6-22
 - restricted mode, 6-18
 - STARTUP command, 6-15
 - when control files unavailable, 6-17
 - when redo logs unavailable, 6-17
- starting a database instance
 - automatically at system startup, 6-19
 - CONNECT command, 6-15
 - database closed and mounted, 6-18
 - Database Control, 6-14, 6-21
 - forcing, 6-19
 - Grid Control, 6-14, 6-21
 - mounting and opening the database, 6-17
 - normally, 6-17
 - recovery and, 6-19
 - Recovery Manager, 6-15
 - remote instance startup, 6-19
 - restricted mode, 6-18
 - SQL*Plus, 6-15
 - when control files unavailable, 6-17
 - when redo logs unavailable, 6-17
 - without mounting a database, 6-17
- starting an instance
 - Oracle Enterprise Manager, 2-5, 2-10
- starting and stopping
 - components, 2-12
 - using opmnctl, 2-13
 - using Oracle Collaboration Suite Control, 2-13
 - in High-Availability environments, 13-19
 - log loader, 2-21, 8-12
 - manually
 - Applications, 2-7, 2-10
 - stopping Infrastructure, 2-6
 - Oracle Calendar, 2-14
 - Oracle Collaboration Suite, 2-1
 - overview, 2-2
 - scripted, 2-3
 - Oracle Collaboration Suite Database, 2-11
 - shutting down with the IMMEDIATE option, 2-22
 - Oracle Collaboration Suite Search, 2-19
 - Oracle Content Services, 2-15
 - node processes across multiple Applications tiers, 2-15
 - node processes on a single Applications tier, 2-15
 - sub-processes, 2-16
 - Oracle Discussions, 2-16
 - Oracle Mail, 2-17
 - Oracle Mobile Collaboration, 2-17
 - Oracle Real-Time Collaboration, 2-18
 - Oracle Voicemail & Fax, 2-19
 - Oracle Web Conferencing, 2-18
 - Oracle Workspaces, 2-19
 - scripted
 - Applications, 2-9, 2-11
 - Infrastructure, 2-5, 2-7
- starting Applications tiers, 2-7
 - manually, 2-7
 - scripted, 2-9
- starting Infrastructure tiers, 2-4
 - manually, 2-4

- scripted, 2-5
- stopping Applications tiers, 2-10
 - manually, 2-10
 - scripted, 2-11
- stopping Infrastructure tiers, 2-6
 - manually, 2-6
 - scripted, 2-7
- tiers, 2-3
- using `opmnctl` instead of other command line tools, 2-20
- STARTUP command
 - MOUNT clause, 6-18
 - NOMOUNT clause, 6-18
 - RECOVER clause, 6-19
 - RESTRICT clause, 6-18
 - starting a database, 6-15
- `staticports.ini` file, A-1
- synchronization
 - Active Directory passwords with Oracle Internet Directory, 9-23
 - between Microsoft Active Directory and Oracle Internet Directory, 9-38
 - decisions to make before, 9-9
 - deletions from Active Directory, 9-23
 - DirSync control-based, 9-5
 - Oracle Internet Directory passwords with Active Directory, 9-24
 - USNChange-based, 9-5
- synchronization profiles
 - ActiveChgImp, 9-17
 - ActiveImport, 9-17
 - configuring, 9-17
 - creating, 9-18
 - samples for synchronizing with Active Directory, 9-17
- SYS schema
 - changing password, 6-44
- SYSAUX tablespace, 6-28
- System Components table, 3-10
- system outages, 11-3
- SYSTEM schema
 - changing password, 6-44
- SYSTEM tablespace, 6-28

T

- tablespace backup, 11-5
- tablespace point-in-time recovery, 11-6
- tablespaces
 - data block, 6-27
 - description, 6-27
 - EXAMPLE, 6-28
 - modifying, 6-30
 - Segment Advisor, 6-30
- segments
 - extents, 6-27
- SYSAUX, 6-28
- SYSTEM, 6-28
- TEMP, 6-28
- UNDOTBS1, 6-28
- USERS, 6-28

- `targets.xml` file
 - ports and, 14-12, 14-13, 14-26, 14-32
- TEMP environment variable, 1-2
- TEMP tablespace, 6-28
- temporary tablespace groups, 6-29
- time-based recovery, 11-6
- TMP environment variable, 1-2
- `tnsnames.ora` file, 12-24
- topologies
 - displaying, 3-11
- Topology Viewer, 3-11
- transitive trust relationships in Active Directory, 9-12
- TSPITR, 11-6

U

- UDDISYS schema
 - changing password, 6-44
- `ulimit` command, using to increase Oracle Real-Time Collaboration connections, 10-13
- undo
 - advisor, 6-35
 - automatic undo management, 6-33
 - database
 - description, 6-33
 - managing, 6-32
 - managing
 - recommendations, 6-35
 - with Database Control, 6-34
- Undo Advisor
 - description, 10-29
- undo tablespace, 6-33
 - extending, 6-35
- UNDOTBS1 tablespace, 6-28
- `unistatus` command, 2-14
- unlocking user accounts, 4-15
- user attributes
 - component-specific, 4-18
- user name limitations, 4-8, 4-12
- `usercreatebase`
 - configuring in integration with Active Directory, 9-16
- UserFactory object, C-14
- UserFactoryBuilder class, C-13
- UserFactoryControl object, C-14
- users
 - assigning privileges, 4-13
 - bulk management, 4-11
 - component-specific attributes, 4-18
 - configuring user account creation, 4-25
 - creating, 4-8
 - database
 - administering, 6-5
 - creating, 6-6
 - editing, 6-8
 - deleting, 4-17
 - de-provisioning, 4-15
 - enabling and disabling, 4-15
 - modifying, 4-12
 - password policies, 4-32

- passwords, 4-14
 - unlocking accounts, 4-15
- users and groups
 - managing, 4-1
- USERS tablespace, 6-28
- usersearchbase
 - configuring in integration with Active Directory, 9-16
- USNChange-based synchronization, 9-5

V

- Vendor Cluster File Systems, 13-6
- Verifying the current configuration, 1-7
- Virtual IP Configuration Assistant (VIPCA), 13-9
- Voice Conversion server
 - starting, 2-18

W

- WCRSYS schema
 - changing password, 6-45
- Web Providers
 - ports and, 14-17
- WebDAV URL, 1-10
- Welcome Page, 3-8
- Welcome page, 1-5
 - accessing, 1-6
- whole database backup, 11-5
- Windows native authentication, 9-4
 - authentication dynamics, 9-5
 - browser settings, 9-41, 9-42
 - configuring, 9-38 to 9-42
 - fallback authentication, 9-42, 9-43
 - how it works, 9-4
 - login scenarios, 9-43
 - system requirements, 9-38
- WIRELESS schema
 - changing password, 6-45
- WK_TEST schema
 - changing password, 6-45
- WKPROXY schema
 - changing password, 6-45
- WKSYS schema
 - changing password, 6-45