

Oracle® Identity Manager
Connector Guide for Microsoft Windows
Release 9.0.4
E10431-09

March 2011

Oracle Identity Manager Connector Guide for Microsoft Windows, Release 9.0.4

E10431-09

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Prakash Hulikere, Devanshi Mohan

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. 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, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vi
Conventions	vi
What's New in Oracle Identity Manager Connector for Microsoft Windows?	vii
Software Updates	vii
Documentation-Specific Updates.....	x
1 About the Connector	
1.1 Certified Components	1-1
1.2 Certified Languages.....	1-2
1.3 Connector Architecture.....	1-3
1.4 Lookup Definitions Used During Connector Operations.....	1-4
1.5 User Attributes for Provisioning	1-4
1.6 Provisioning Functions	1-4
1.7 Roadmap for Deploying and Using the Connector	1-5
2 Deploying the Connector	
2.1 Preinstallation.....	2-1
2.1.1 Preinstallation on Oracle Identity Manager.....	2-1
2.1.1.1 Files and Directories on the Installation Media	2-1
2.1.1.2 Installing Oracle Identity Manager Connector for Microsoft Active Directory User Management	2-2
2.1.1.3 Determining the Release Number of the Connector	2-3
2.1.2 Preinstallation on the Target System	2-3
2.2 Installation	2-3
2.2.1 Running the Connector Installer	2-3
2.2.2 Configuring the IT Resource	2-6
2.3 Postinstallation	2-8
2.3.1 Setting Up the Lookup.Windows.Configuration Lookup Definition.....	2-8
2.3.2 Setting a Value for the PATH Environment Variable	2-9
2.3.3 Changing to the Required Input Locale	2-9

2.3.4	Clearing Content Related to Connector Resource Bundles from the Server Cache...	2-9
2.3.5	Enabling Logging.....	2-11
2.3.5.1	Enabling Logging on Oracle Identity Manager Release 9.1.0.x.....	2-11
2.3.5.2	Enabling Logging on Oracle Identity Manager Release 11.1.1	2-13
2.3.6	Enabling Request-Based Provisioning.....	2-15
2.3.6.1	Copying Predefined Request Datasets	2-16
2.3.6.2	Importing Request Datasets into MDS.....	2-16
2.3.6.3	Enabling the Auto Save Form Feature	2-17
2.3.6.4	Running the PurgeCache Utility	2-17

3 Configuring the Connector

3.1	Configuring the Connector for Multiple Installations of the Target System	3-1
3.2	Performing Provisioning Operations.....	3-2
3.2.1	Direct Provisioning.....	3-2
3.2.2	Request-Based Provisioning.....	3-3
3.2.2.1	End User's Role in Request-Based Provisioning.....	3-4
3.2.2.2	Approver's Role in Request-Based Provisioning.....	3-5
3.3	Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1	3-5

4 Testing and Troubleshooting

5 Known Issues

Index

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Microsoft Windows.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/support/contact.html> or visit <http://www.oracle.com/accessibility/support.html> if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

<http://www.oracle.com/technetwork/documentation/oim1014-097544.html>

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

<http://www.oracle.com/technetwork/documentation/oim1014-097544.html>

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.
monospace	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 Identity Manager Connector for Microsoft Windows?

This chapter provides an overview of the updates made to the software and documentation for the Microsoft Windows connector in release 9.0.4.12.

The updates discussed in this chapter are divided into the following categories:

- [Software Updates](#)
This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.
- [Documentation-Specific Updates](#)
This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss software updates:

- [Software Updates in Release 9.0.4.1](#)
- [Software Updates in Release 9.0.4.2](#)
- [Software Updates in Release 9.0.4.3](#)
- [Software Updates in Release 9.0.4.11](#)
- [Software Updates in Release 9.0.4.12](#)

Software Updates in Release 9.0.4.1

In release 9.0.4.1, changes have been made in the names and directory structure of the connector installation files.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- [Using the Connector Installer](#)
- [Resolved Issues in Release 9.0.4.2](#)

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See "[Running the Connector Installer](#)" on page 2-3 for details.

Resolved Issues in Release 9.0.4.2

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
5180725 and 5180704	The share name set for a user's directory on the target system could not be updated through the Update User provisioning operation.	This issue has been resolved. You can update the share name through the Update User provisioning operation.
5573882	On the Administrative and User Console, the Provisioned status was displayed for a user even when the user's directory could not be created through the Create User provisioning operation.	This issue has been resolved. The Provisioning status is displayed for a user if the directory cannot be created during the Create User provisioning operation.
7597465	The Microsoft Windows connector could not be used with the Microsoft Active Directory connector release 9.0.4.10 or later.	This issue has been resolved. The Microsoft Windows connector can now be used with any release of the Microsoft Active Directory connector.

Software Updates in Release 9.0.4.3

The following are software updates in release 9.0.4.3:

- [Change in the Requirement for Microsoft Active Directory User Management Connector and Oracle Identity Manager](#)
- [Support for Creating Hidden Shares and Removing Shares](#)
- [New IT Resource Parameters Added](#)
- [Support for New Target System](#)
- [Resolved Issues in Release 9.0.4.3](#)

Change in the Requirement for Microsoft Active Directory User Management Connector and Oracle Identity Manager

From this release onward, Microsoft Active Directory User Management connector release 9.1.1 is the minimum supported Microsoft Active Directory User Management connector release. To install the Microsoft Active Directory User Management connector release 9.1.1, you require Oracle Identity Manager release 9.1.0.1 or later. Therefore, the minimum Oracle Identity Manager requirement for the current release of the Microsoft Windows connector is Oracle Identity Manager release 9.1.0.1.

This requirement is mentioned in "[Certified Components](#)" section.

Support for Creating Hidden Shares and Removing Shares

From this release onward, the connector enables you to:

- Create hidden shares on a folder
- Stop sharing a folder

The Create hidden folder for a user and Delete share attribute functions have been listed in the "[Provisioning Functions](#)" section.

New IT Resource Parameters Added

The `Invert Display Name` and `isLookupDN` parameters have been added to the Windows AD Server IT Resource to enable this connector to successfully connect to Microsoft Active Directory. See the "[Configuring the IT Resource](#)" section for more information about these parameters.

Support for New Target System

From this release onward, the connector adds support for Microsoft Windows Server 2008 as the target system.

This target system is mentioned in "[Certified Components](#)" section of the connector guide.

Resolved Issues in Release 9.0.4.3

The following are issues resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
5180972	All error and exception messages that occurred during the course of provisioning operations were displayed on a console on the Oracle Identity Manager host computer. These messages were not written to a log file.	This issue has been resolved. All error and exception messages are displayed on the console and written to the log file of the application server.
8558641	When a provisioning operation was performed several times, the JVM stopped functioning. This caused Oracle Identity Manager to stop responding and the following error message was displayed on the application server console: An unexpected error has been detected by HotSpot Virtual Machine: EXCEPTION_ACCESS_VIOLATION	This issue has been resolved. The <code>EXCEPTION_ACCESS_VIOLATION</code> error message is no longer encountered when a provisioning operation is performed several times. Therefore, Oracle Identity Manager does not stop responding.
8569946	The <code>java.lang.NoSuchMethodException</code> exception was encountered when you tried to perform the Add User to Folder provisioning operation while using release 9.0.4.2 of the Microsoft Windows connector along with release 9.1.1 of the Microsoft Active Directory connector.	This issue has been resolved. You can perform add users to folders through provisioning.

Software Updates in Release 9.0.4.11

The following are software updates in release 9.0.4.11:

- [Dependency on a Specific Release of the Microsoft Active Directory Connector Has Been Removed](#)
- [Resolved Issues in Release 9.0.4.11](#)

Dependency on a Specific Release of the Microsoft Active Directory Connector Has Been Removed

The earlier release of the connector required you to install release 9.1.1 of the Microsoft Active Directory connector. From this release onward, you can use any release of the Microsoft Active Directory connector that provides the GUID user attribute. The `Lookup.Windows.Configuration` lookup definition has been introduced to store details

of the Microsoft Active Directory User Management connector used by the Microsoft Windows connector.

See the ["Setting Up the Lookup.Windows.Configuration Lookup Definition"](#) section for more information.

Resolved Issues in Release 9.0.4.11

The following are issues resolved in release 9.0.4.11:

Bug Number	Issue	Resolution
9172138	NoSuchMethodException was encountered on the target system when you performed the Remove User from Folder provisioning operation from Oracle Identity Manager.	This issue has been resolved. You can now perform the Remove User from Folder provisioning operation.
9303613	The Revoke Share provisioning operation did not work.	This issue has been resolved. The Revoke Share provisioning operation now works as expected.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- [Support for New Oracle Identity Manager Release](#)
- [Support for Request-Based Provisioning](#)

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11g release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See [Section 1.1, "Certified Components"](#) for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11g release 1 (11.1.1).

See [Section 3.2.2, "Request-Based Provisioning"](#) for more information.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- [Documentation-Specific Updates in Release 9.0.4.1](#)
- [Documentation-Specific Updates in Release 9.0.4.2](#)
- [Documentation-Specific Updates in Release 9.0.4.3](#)
- [Documentation-Specific Updates in Release 9.0.4.11](#)
- [Documentation-Specific Updates in Release 9.0.4.12](#)

Documentation-Specific Updates in Release 9.0.4.1

The following documentation-specific updates have been made in release 9.0.4.3:

- In ["Certified Components"](#) section, the Oracle Identity Manager host platform names have been added.

Documentation-Specific Updates in Release 9.0.4.2

The following documentation-specific updates have been made in release 9.0.4.2:

- In "[Provisioning Functions](#)" section, the Add New Share Path provisioning function has been added to the list of supported functions.
- In the "[Known Issues](#)" chapter:
 - The following point has been removed:

The locale of the server on which Oracle Identity Manager is installed must be set to the language that is used to enable folders to be created on the target system. For example, if Japanese is in use on the target system, then Oracle Identity Manager must be installed on a server running the Japanese language locale.
 - The following points have been added:

Bug 5691610: The connector does not support deployment scenarios in which Oracle Identity Manager is installed on an operating system other than Microsoft Windows.

Bug 7490324: For a provisioning operation, the file server, Oracle Identity Manager, and the target system account used by Oracle Identity Manager to perform provisioning operations must be on the same domain.
 - Microsoft Windows 2000 is no longer a supported host for the target system. All occurrences of "Microsoft Windows 2000" have been removed from this guide.
 - In "[Certified Components](#)" section, changes have been made in the "Target systems" and "Target system host platform" rows.

Documentation-Specific Updates in Release 9.0.4.3

The following documentation-specific updates have been made in release 9.0.4.3:

- In "Provisioning Module" section, the Hidden field has been added to the list of fields that are provisioned.
- In "[Provisioning Functions](#)" section, the descriptions of the functions have been modified.
- The "Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.1" section has been removed from the "[Deploying the Connector](#)" chapter.
- In the "Postinstallation on the Target System" section, the following point has been added:

"Ensure that a value for the TEMP or TMP system environment variable has been set."
- In "[Certified Components](#)" section, minor changes have been made.

Documentation-Specific Updates in Release 9.0.4.11

The following is a documentation-specific update in release 9.0.4.11:

- In "[Certified Components](#)" section, the minimum JDK requirement of release 1.4.2 has been added.
- In "[Provisioning Functions](#)" section, a Note has been added for the Create folder for a user function.

Documentation-Specific Updates in Release 9.0.4.12

There are no documentation-specific updates in this release.

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with Microsoft Windows.

This chapter contains the following sections:

Note: In this guide, the term **Oracle Identity Manager host computer** refers to the computer on which Oracle Identity Manager is installed.

At some places in this guide, Microsoft Windows has been referred to as the **target system**.

- [Section 1.1, "Certified Components"](#)
- [Section 1.2, "Certified Languages"](#)
- [Section 1.3, "Connector Architecture"](#)
- [Section 1.4, "Lookup Definitions Used During Connector Operations"](#)
- [Section 1.5, "User Attributes for Provisioning"](#)
- [Section 1.6, "Provisioning Functions"](#)
- [Section 1.7, "Roadmap for Deploying and Using the Connector"](#)

1.1 Certified Components

[Table 1-1](#) lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	<p>You can use one of the following releases of Oracle Identity Manager:</p> <ul style="list-style-type: none"> ■ Oracle Identity Manager release 9.1.0.1 or later <p>Note: In this guide, Oracle Identity Manager release 9.1.0.x has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.x series that the connector will support.</p> <p>To use this release of the connector, you must install a release of the Microsoft Active Directory User Management connector that provides the GUID user attribute.</p> <ul style="list-style-type: none"> ■ Oracle Identity Manager 11g release 1 (11.1.1) <p>Note: In this guide, Oracle Identity Manager release 11.1.1 has been used to denote Oracle Identity Manager 11g release 1 (11.1.1).</p>
JDK	<p>The JDK version can be one of the following:</p> <ul style="list-style-type: none"> ■ For Oracle Identity Manager release 9.1.0.x, use JDK 1.6 update 5 or later. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.
Target systems	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2003 ■ Microsoft Windows Server 2008
Oracle Identity Manager host platform	<p>The Oracle Identity Manager host platform can be any one of the following:</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2003 ■ Microsoft Windows Server 2008
Infrastructure requirements	<p>An additional computer running any one of the following:</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2003 Active Directory installed on Microsoft Windows Server 2003 ■ Microsoft Windows Server 2008 Active Directory installed on Microsoft Windows Server 2008 <p>This computer is meant for use as a file server.</p>
Other applications	<p>A release of the Microsoft Active Directory User Management connector that supports the GUID user attribute</p>
Target system user account	<p>The target system user account can be any one of the following:</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2003 File Server administrator ■ Microsoft Windows Server 2008 File Server administrator <p>You provide the credentials of this user account while configuring the IT resource. The procedure is described later in this guide.</p>

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French

- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

See Also: For information about supported special characters

- On Oracle Identity Manager release 9.1.0.x, see *Oracle Identity Manager Globalization Guide*.
- On Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

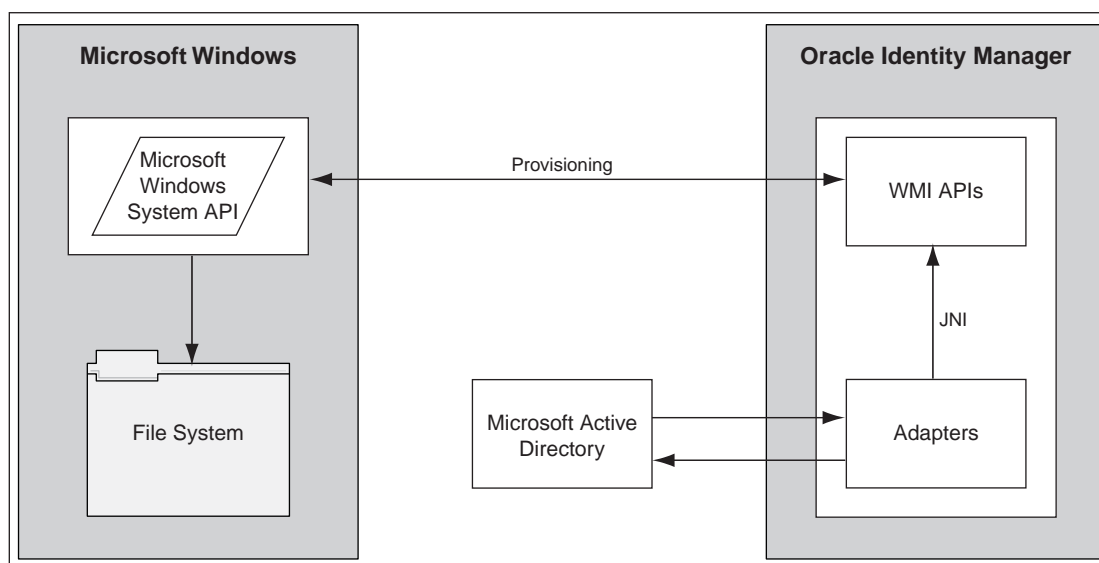
1.3 Connector Architecture

The connector enables the creation of shared folders on Microsoft Windows Server through a provisioning operation on Oracle Identity Manager. This provisioning operation consists of the following steps:

1. For the specified OIM User, the connector fetches the GUID from the Microsoft Active Directory resource records stored in Oracle Identity Manager.
2. From the GUID, the connector determines the user name in the Microsoft Active Directory resource record.
3. The connector uses the Microsoft Windows System APIs on the target system to create the shared folder. The user name obtained from Microsoft Active Directory is set as the owner of the shared folder.

Figure 1–1 shows the basic architecture of the connector.

Figure 1–1 Connector Architecture



After you create a shared folder, you can also perform the following additional provisioning operations:

- Set and modify permissions assigned to the user on the folder.
- Set a new share path for the folder.
- Hide the folder.

1.4 Lookup Definitions Used During Connector Operations

The Lookup.Windows.Configuration lookup definition is automatically created when you install the connector. This lookup definition holds the following entries:

- ADGUIDColumnName
- ADROName

[Section 2.3.1, "Setting Up the Lookup.Windows.Configuration Lookup Definition"](#) provides information about setting values in this lookup definition.

1.5 User Attributes for Provisioning

[Table 1–2](#) provides information about user attribute mappings for provisioning.

Table 1–2 *User Attributes for Provisioning*

Process Form Field	Target System Attribute	Description
Share Path	Folder Path	This attribute is used to specify the path of the shared folder.
Hidden	Hidden	This attribute is used to specify that the shared folder must be hidden.
New Share Path	New Share Name	This attribute is used to assign a new share name to an existing shared folder.
Full Control	Full Control	This attribute is used to grant full control of the folder to the user.
Change	Modify	This attribute is used to grant the user permission to modify the contents of the folder.
Read	Read	This attribute is used to grant the user permission to view the contents of the folder.
Write	Write	This attribute is used to grant the user permission to add contents to the folder.
None	On the target system, the check boxes in the Deny column are selected. Alternatively, the check boxes in the Allow column are not selected.	This attribute is used to deny the user access to the folder.

1.6 Provisioning Functions

[Table 1–3](#) lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when each function is performed.

Table 1–3 Provisioning Functions

Function	Description	Adapter
Create folder for a user	<p>Creates a folder, shares it for the user, and adds the user to the shared folder.</p> <p>Note:</p> <p>The folder that the connector creates is <i>not</i> the home folder for the user. When the user is added to the shared folder, only the permissions selected on the process form are granted.</p> <p>When you create a share for a user, the share name assigned is the user ID. Therefore, you cannot directly create another share for the user. As a workaround, you can specify a new share name for the first share and then create another share for the user. The second share is assigned the user ID as its name. You can follow this approach to create multiple shares for a user.</p>	<p>Win2K Create Directory</p> <p>Win2K Create Share</p> <p>Win2K Add User To Folder</p>
Create hidden folder for a user	<p>Creates a hidden folder, shares it for the user, and adds the user to the shared hidden folder.</p> <p>Note: The folder that the connector creates is <i>not</i> the home folder for the user. When the user is added to the shared folder, only the permissions selected on the process form are granted.</p>	Win2K Create Hide Option
Delete share attribute	Stops sharing a folder.	Win2K Delete Share
Update access permissions for user	Updates the permissions granted to a user on the shared folder.	Win2K Add User To Folder
Revoke access permissions from user	Revokes the permissions granted to a user on a shared folder.	Win2K Remove User From Folder
Add new share name	Assigns a new share name to an existing shared folder.	Win2K Update Share Path

1.7 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- [Chapter 2, "Deploying the Connector"](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Chapter 3, "Configuring the Connector"](#) describes guidelines on using the connector.
- [Chapter 4, "Testing and Troubleshooting"](#) describes the procedure to test the connector.
- [Chapter 5, "Known Issues"](#) lists known issues associated with this release of the connector.

Deploying the Connector

To deploy the connector, perform the procedures described in the following sections:

- [Section 2.1, "Preinstallation"](#)
- [Section 2.2, "Installation"](#)
- [Section 2.3, "Postinstallation"](#)

2.1 Preinstallation

This section is divided into the following topics:

- [Section 2.1.1, "Preinstallation on Oracle Identity Manager"](#)
- [Section 2.1.2, "Preinstallation on the Target System"](#)

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- [Section 2.1.1.1, "Files and Directories on the Installation Media"](#)
- [Section 2.1.1.2, "Installing Oracle Identity Manager Connector for Microsoft Active Directory User Management"](#)
- [Section 2.1.1.3, "Determining the Release Number of the Connector"](#)

2.1.1.1 Files and Directories on the Installation Media

[Table 2-1](#) describes the files and directories on the installation media.

Table 2-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
dataset\ProvisionResourceWindows.xml dataset\ModifyResourceWindows.xml	These request dataset XML files are used to enable request-based provisioning. Section 2.3.6, "Enabling Request-Based Provisioning" provides more information.
configuration\MS Windows-CI.xml	This XML file contains configuration information that is used during connector installation.
config\debug.properties	This file contains the debug parameter that you use to specify whether or not the connector must run in debug mode.
lib\tcWindowsNT40.dll	This DLL file contains the native code required for provisioning directories on a Microsoft Windows 2003 server.

Table 2–1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
lib\xliWindows2000.jar	<p>This JAR file contains the class files required for provisioning. During connector deployment, this file is copied to the following location:</p> <ul style="list-style-type: none"> ■ For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/JavaTasks</i> ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
Files in the resources directory	<p>Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied to the following location:</p> <ul style="list-style-type: none"> ■ For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/connectorResources</i> ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database <p>Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.</p>
test\config\config.properties	This file contains the connection attributes required for Oracle Identity Manager to connect to the target system and perform test provisioning operations.
test\scripts\runWindowsTest.bat	This file is used to start the testing utility.
xml\Windows2000Object_DM.xml	<p>This XML file contains definitions for the following components of the connector:</p> <ul style="list-style-type: none"> ■ IT resource type ■ Process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules ■ Lookup definitions

Note: The files in the test directory are used only to run tests on the connector.

2.1.1.2 Installing Oracle Identity Manager Connector for Microsoft Active Directory User Management

The connector uses records stored in Oracle Identity Manager by Oracle Identity Manager Connector for Microsoft Active Directory User Management. Shared folders can be created on the target system only for OIM Users who already have a Microsoft Active Directory account in Oracle Identity Manager. Therefore, you must ensure that the Microsoft Active Directory User Management connector is installed before you start using the Microsoft Windows connector.

Note: The release of the Microsoft Active Directory User Management connector that you install must support the GUID attribute. To verify whether the connector supports the GUID attribute, check the documentation for that release.

2.1.1.3 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.1.0.x, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1, then skip this section.

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:
`OIM_HOME/xellerate/JavaTasks/xliWindows2000.jar`
2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the xliWindows2000.jar file.

In the manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.1.2 Preinstallation on the Target System

Configure the file server and the target system in the domain in which you install Microsoft Active Directory. In addition, ensure that a value has been set for the TEMP or TMP environment variable.

2.2 Installation

Installation on Oracle Identity Manager consists of the following procedures:

- [Section 2.2.1, "Running the Connector Installer"](#)
- [Section 2.2.2, "Configuring the IT Resource"](#)

2.2.1 Running the Connector Installer

Note: In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Administrative and User Console.

Direct provisioning is automatically enabled after you run the Connector Installer. If required, you can enable request-based provisioning in the connector. Direct provisioning is automatically disabled when you enable request-based provisioning. See [Section 2.3.6, "Enabling Request-Based Provisioning"](#) if you want to use the request-based provisioning feature for this target system.

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

Note: In an Oracle Identity Manager cluster, perform this step on each node of the cluster.

- For Oracle Identity Manager release 9.1.0.x:
OIM_HOME/xellerate/ConnectorDefaultDirectory
 - For Oracle Identity Manager release 11.1.1:
OIM_HOME/server/ConnectorDefaultDirectory
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console Guide*.
 3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - For Oracle Identity Manager release 9.1.0.x:
Click **Deployment Management**, and then click **Install Connector**.
 - For Oracle Identity Manager release 11.1.1:
On the Welcome to Identity Manager Advanced Administration page, under the System Management section, click **Install Connector**.
 4. From the Connector List list, select **Microsoft Windows *RELEASE_NUMBER*** This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory specified Step 1.
If you have copied the installation files into a different directory, then:
 - a. In the **Alternative Directory** field, enter the full path and name of that directory.
 - b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
 - c. From the Connector List list, select **Microsoft Windows *RELEASE_NUMBER***
 5. Click **Load**.
 6. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector XML files (by using the Deployment Manager)
- c. Compilation of adapters

On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

- Retry the installation by clicking **Retry**.
- Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:
 - a. Ensuring that the prerequisites for using the connector are addressed

Note: At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See [Section 2.3.4, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#) for information about running the PurgeCache utility.

There are no prerequisites for some predefined connectors.

- b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.
 - c. Configuring the scheduled tasks that are created when you installed the connector

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.
8. Copy the files listed in the first column of the following table to the destination directories specified in the second column:

Table 2–2 Files Copied to the Oracle Identity Manager Host Computer

File in the Installation Media Directory	Destination for Oracle Identity Manager Release 9.1.0.x	Destination for Oracle Identity Manager Release 11.1.1
config\debug.properties	<i>OIM_HOME</i> \xellerate\XLIntegration\s\Windows2000\config	Oracle Identity Manager database
lib\tcWindowsNT40.dll	<i>OIM_HOME</i> \xellerate\XLIntegration\s\Windows2000\dl <ul style="list-style-type: none"> ■ For Oracle Application Server, you must also copy this file into the following directory: <i>ORACLE_HOME</i>\bin ■ For Oracle WebLogic Server, you must also copy this file into the following directory: <i>WEBLOGIC_HOME</i>\server\bin 	For Oracle WebLogic Server, you must also copy this file into the following directory: <i>WEBLOGIC_HOME</i> \server\bin
test\config directory	<i>OIM_HOME</i> \xellerate\XLIntegration\s\Windows2000\config	<i>OIM_HOME</i> \server\XLIntegration\Windows2000\config
test\scripts directory	<i>OIM_HOME</i> \xellerate\XLIntegration\s\Windows2000\scripts	<i>OIM_HOME</i> \server\XLIntegration\Windows2000\scripts

Note: When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in [Table 2–1](#).

Installing the Connector in an Oracle Identity Manager Cluster

While installing the connector in a cluster, you must copy all the JAR files and the contents of the resources directory into the destination directories on each node of the cluster. Then, restart each node. See [Section 2.1.1.1, "Files and Directories on the Installation Media"](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.2.2 Configuring the IT Resource

You must specify values for the parameters of the IT resource as follows:

1. Log in to the Administrative and User Console.
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - If you are using Oracle Identity Manager release 9.1.0.x, expand **Resource Management**, and then click **Manage IT Resource**.
 - If you are using Oracle Identity Manager release 11.1.1, then:
 - a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.
 - b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the **Configuration** region, click **Manage IT Resource**.
3. On the Manage IT Resource page, enter `W2K File Server` in the IT Resource Type field and then click **Search**.
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource. The following table describes each parameter:

Parameter	Parameter Description
AdminName	Enter the user ID of the admin user on the Microsoft Windows computer that is used as the file server.
AdminPassword	Enter the password of the admin user on the Microsoft Windows computer that is used as the file server.
ComputerName	Enter the host name or IP address of the Microsoft Windows computer that is used as the file server.
DomainName	Enter the domain of the Microsoft Windows computer that is used as the file server.

7. To save the values, click **Update**.
8. On the Manage IT Resource page, enter `Windows AD Server` in the IT Resource Name list and then click **Search**.

Note: This IT resource is used to connect to Microsoft Active Directory.

9. Click the edit icon for the IT resource.
10. From the list at the top of the page, select **Details and Parameters**.

11. Specify values for the parameters of the IT resource. The following table describes each parameter:

Parameter	Parameter Description
Admin FQDN	<p>Enter the fully qualified domain name of the admin user account whose user ID you enter as the value of the AdminName parameter of the W2K File Server IT resource.</p> <p>You can use any one of the following formats to enter the domain name:</p> <ul style="list-style-type: none"> ■ <code>user_login@domain.com</code> ■ <code>cn=user_login,cn=Users,dc=domain,dc=com</code> <p>Sample values:</p> <p><code>john_doe@example.com</code></p> <p><code>cn=OIMadmin,cn=Users,dc=domain,dc=com</code></p>
Admin Login	<p>Enter the user ID that you specify as the value of the AdminName parameter of the W2K File Server IT resource.</p>
Admin Password	<p>Enter the password that you specify as the value of the AdminPassword parameter of the W2K File Server IT resource.</p>
Root Context	<p>Enter the fully qualified domain name of the parent or root organization.</p> <p>For example, the root suffix.</p> <p>Format: <code>ou=ORGANIZATION_NAME,dc=DOMAIN</code></p> <p>Sample value: <code>ou=Adapters,dc=adomain</code></p>
Server Address	<p>Enter the host name or IP address of the Microsoft Windows computer on which Microsoft Active Directory is installed.</p> <p>Sample values:</p> <p><code>w2khost</code></p> <p><code>172.20.55.120</code></p>
Use SSL	<p>Use this parameter to specify whether or not SSL has been used to secure communication between Oracle Identity Manager and Microsoft Active Directory.</p> <p>Default value: <code>true</code></p> <p>Note: It is recommended that you enable SSL to secure communication with the target system.</p>
SSL Port Number	<p>Enter the number of the port at which SSL is running on the target system host computer.</p> <p>Sample values:</p> <ul style="list-style-type: none"> ■ 636, if the Use SSL parameter is set to <code>yes</code> ■ 389, if the Use SSL parameter is set to <code>no</code>
Target Locale: Country	<p>Enter the country code.</p> <p>Default value: <code>US</code></p> <p>Note: You must specify the value in uppercase.</p>
Target Locale: Language	<p>Enter the language code.</p> <p>Default value: <code>en</code></p> <p>Note: You must specify the value in lowercase.</p>

Parameter	Parameter Description
Invert Display Name	<p>Enter the value that you had entered for the Invert Display Name parameter of the ADITResource IT Resource.</p> <p>If you enter <code>yes</code>, then the Display Name field will be in the <code>LAST_NAME FIRST_NAME</code> format. If you enter <code>no</code>, then Display Name field will be in the <code>FIRST_NAME LAST_NAME</code> format.</p> <p>For example, if you enter <code>yes</code>, then the Display Name field for user John Doe would show Doe John.</p> <p>Default value: <code>no</code></p> <p>Note: If you want to set this parameter to <code>yes</code>, then note that it works only with the ADITResource IT resource. It will not work if the IT resource for the target system has a different name.</p>
isLookupDN	This parameter has been deprecated. It will be removed from the IT resource definition in a future release. Do not change the default value of this parameter.

12. To save the values, click **Update**.

2.3 Postinstallation

The following sections describe postinstallation steps:

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster.

- [Section 2.3.1, "Setting Up the Lookup.Windows.Configuration Lookup Definition"](#)
- [Section 2.3.2, "Setting a Value for the PATH Environment Variable"](#)
- [Section 2.3.3, "Changing to the Required Input Locale"](#)
- [Section 2.3.4, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#)
- [Section 2.3.5, "Enabling Logging"](#)
- [Section 2.3.6, "Enabling Request-Based Provisioning"](#)

2.3.1 Setting Up the Lookup.Windows.Configuration Lookup Definition

The Microsoft Active Directory User Management connector stores the GUID of users that you manage through the Microsoft Windows connector. You use the Lookup.Windows.Configuration lookup definition to store details of the Microsoft Active Directory User Management connector used by the Microsoft Windows connector. To enter these details in the lookup definition:

1. On the Design Console, determine the column name for the GUID attribute on the process form of the Microsoft Active Directory User Management connector.
2. On the Design Console, determine the name of the resource object of the Microsoft Active Directory User Management connector.
3. On the Design Console, expand **Administration** and double-click **Lookup Definition**.
4. Search for and open the **Lookup.Windows.Configuration** lookup definition.

5. In the **Decode** column for the ADGUIDColumnName entry, enter the name of the process form field (column) that stores the GUID, which you determined in Step 1.
6. In the **Decode** column for the ADROName entry, enter the name of the resource object, which you determined in Step 2.
7. Click the Save icon.

2.3.2 Setting a Value for the PATH Environment Variable

To set a value for the PATH environment variable:

1. Use a text editor to open the following file:
 - If you are using Oracle Identity Manager 9.1.0.x, then:
`OIM_HOME\xellerate\bin\xlStartServer.bat`
 - If you are using Oracle Identity Manager 11.1.1, then:
`OIM_HOME\server\bin\StartManagedWeblogic.bat`
2. Add the following line at the start of this file:
 - If you are using Oracle Identity Manager 9.1.0.x, then:
`SET PATH=OIM_HOME\xellerate\XLIntegrations\Windows2000\dll`
 - If you are using Oracle Identity Manager 11.1.1, then:
`SET PATH=OIM_HOME\server\XLIntegrations\Windows2000\dll`
3. Save and close the file.

2.3.3 Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

You may require the assistance of the system administrator to change to the required input locale.

2.3.4 Clearing Content Related to Connector Resource Bundles from the Server Cache

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the `OIM_HOME/xellerate/connectorResources` directory for Oracle Identity Manager release 9.1.0.x and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, perform one of the following steps:
 - If you are using Oracle Identity Manager release 9.1.0.x, then switch to the `OIM_HOME/xellerate/bin` directory.

- If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME/server/bin* directory.

Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

For Oracle Identity Manager release 9.1.0.x:

```
OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME
```

For Oracle Identity Manager release 11.1.1:

```
OIM_HOME/server/bin/SCRIPT_FILE_NAME
```

2. Enter one of the following commands:

Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat CATEGORY_NAME` on Microsoft Windows or `PurgeCache.sh CATEGORY_NAME` on UNIX. The *CATEGORY_NAME* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

- For Oracle Identity Manager release 9.1.0.x:
On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`
On UNIX: `PurgeCache.sh ConnectorResourceBundle`

Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

In this command, `ConnectorResourceBundle` is one of the content categories that you can delete from the server cache. See the following file for information about the other content categories:

```
OIM_HOME/xellerate/config/xlconfig.xml
```

- For Oracle Identity Manager release 11.1.1:
On Microsoft Windows: `PurgeCache.bat All`
On UNIX: `PurgeCache.sh All`

When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

```
t3://OIM_HOST_NAME:OIM_PORT_NUMBER
```

In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.3.5 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform the procedure described in one of the following sections:

- [Section 2.3.5.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"](#)
- [Section 2.3.5.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"](#)

2.3.5.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.x

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL
This level enables logging for all events.
- DEBUG
This level enables logging of information about fine-grained events that are useful for debugging.
- INFO
This level enables logging of messages that highlight the progress of the application at a coarse-grained level.
- WARN
This level enables logging of information about potentially harmful situations.
- ERROR
This level enables logging of information about error events that might allow the application to continue running.
- FATAL
This level enables logging of information about very severe error events that could cause the application to stop functioning.
- OFF
This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **Oracle WebLogic Server**

To enable logging:

1. Add the following lines in the *OIM_HOME/xellerate/config/log.properties* file:

```
log4j.logger.OIMCP.WINDOWS=log_level
```

2. In these lines, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.OIMCP.WINDOWS=INFO
```

After you enable logging, log information is displayed on the server console.

- **IBM WebSphere Application Server**

To enable logging:

1. Add the following lines in the *OIM_HOME/xellerate/config/log.properties* file:

```
log4j.logger.XELLERATE=log_level  
log4j.logger.OIMCP.WINDOWS=log_level
```

2. In these lines, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO  
log4j.logger.OIMCP.WINDOWS=INFO
```

After you enable logging, log information is written to the following file:

WEBSPHERE_HOME/AppServer/logs/SERVER_NAME/SystemOut.log

- **JBoss Application Server**

To enable logging:

1. In the *JBOSS_HOME/server/default/conf/log4j.xml* file, add the following lines if they are not already present in the file:

```
<category name="OIMCP.WINDOWS">  
  <priority value="log_level"/>  
</category>  
  
<category name="XL_INTG.LOTUSNOTES">  
  <priority value="log_level"/>  
</category>
```

2. In the second XML code line of each set, replace *log_level* with the log level that you want to set. For example:

```
<category name="OIMCP.WINDOWS">  
  <priority value="INFO"/>  
</category>  
  
<category name="XL_INTG.LOTUSNOTES">  
  <priority value="INFO"/>  
</category>
```

After you enable logging, log information is written to the following file:

JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

To enable logging:

1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

```
log4j.logger.XELLERATE=log_level
log4j.logger.OIMCP.WINDOWS=log_level
```

2. In these lines, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.OIMCP.WINDOWS=INFO
```

After you enable logging, log information is written to the following file:

ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

2.3.5.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on `java.util.logger`. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- `SEVERE.intValue()+100`
This level enables logging of information about fatal errors.
- `SEVERE`
This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.
- `WARNING`
This level enables logging of information about potentially harmful situations.
- `INFO`
This level enables logging of messages that highlight the progress of the application.
- `CONFIG`
This level enables logging of information about fine-grained events that are useful for debugging.
- `FINE`, `FINER`, `FINEST`
These levels enable logging of information about fine-grained events, where `FINEST` logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in [Table 2-3](#).

Table 2–3 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
 - a. Add the following blocks in the file:

```
<log_handler name='windows-handler' level=' [LOG_LEVEL] '
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off' />
  <property name='path' value=' [FILE_NAME] ' />
  <property name='format' value='ODL-Text' />
  <property name='useThreadName' value='true' />
  <property name='locale' value='en' />
  <property name='maxFileSize' value='5242880' />
  <property name='maxLogSize' value='52428800' />
  <property name='encoding' value='UTF-8' />
</log_handler>

<logger name="OIMCP.WINDOWS" level=" [LOG_LEVEL] " useParentHandlers="false">
  <handler name="windows-handler" />
  <handler name="console-handler" />
</logger>
```

- b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. [Table 2–3](#) lists the supported message type and level combinations.

Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

```
<log_handler name='windows-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off' />
  <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log' />
```

```

    <property name='format' value='ODL-Text' />
    <property name='useThreadName' value='true' />
    <property name='locale' value='en' />
    <property name='maxFileSize' value='5242880' />
    <property name='maxLogSize' value='52428800' />
    <property name='encoding' value='UTF-8' />
  </log_handler>

  <logger name="OIMCP.WINDOWS" level="NOTIFICATION:1"
  useParentHandlers="false">
    <handler name="windows-handler" />
    <handler name="console-handler" />
  </logger>

```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

Replace **FILENAME** with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.3.6 Enabling Request-Based Provisioning

Note: Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.
- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- [Section 2.3.6.1, "Copying Predefined Request Datasets"](#)
- [Section 2.3.6.2, "Importing Request Datasets into MDS"](#)
- [Section 2.3.6.3, "Enabling the Auto Save Form Feature"](#)
- [Section 2.3.6.4, "Running the PurgeCache Utility"](#)

2.3.6.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following are the predefined request datasets available in the dataset directory on the installation media:

- `ModifyResourceWindows.xml`
- `ProvisionResourceWindows.xml`

Copy the file from the dataset directory on the installation media to the `OIM_HOME/DataSet/file` directory.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about modifying request datasets.

2.3.6.2 Importing Request Datasets into MDS

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster.

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.
2. In a command window, change to the `OIM_HOME\server\bin` directory.
3. Run one of the following commands:
 - On Microsoft Windows
`weblogicImportMetadata.bat`
 - On UNIX
`weblogicImportMetadata.sh`
4. When prompted, enter the following values:
 - Please enter your username [weblogic]
Enter the username used to log in to the WebLogic server
Sample value: `WL_User`
 - Please enter your password [weblogic]
Enter the password used to log in to the WebLogic server.
 - Please enter your server URL [t3://localhost:7001]
Enter the URL of the application server in the following format:
`t3://HOST_NAME_IP_ADDRESS:PORT`

In this format, replace:

- *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.
- *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS.

2.3.6.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management**, and then double-click **Process Definition**.
3. Search for and open the **Windows 2000** process definition.
4. Select the **Auto Pre-populate** and **Auto Save Form** check boxes.
5. Click the Save icon.

2.3.6.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See [Section 2.3.4, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#) for instructions.

The procedure to configure request-based provisioning ends with this step.

Configuring the Connector

This chapter is divided into the following sections:

Note: These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- [Section 3.1, "Configuring the Connector for Multiple Installations of the Target System"](#)
- [Section 3.2, "Performing Provisioning Operations"](#)
- [Section 3.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"](#)

3.1 Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of Microsoft Windows.

You may want to configure the connector for multiple installations of Microsoft Windows. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Example Multinational Inc. have their own installations of Microsoft Windows. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of Microsoft Windows.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of Microsoft Windows.

To configure the connector for multiple installations of the target system, create and configure one IT resource for each target system installation

The IT Resources form is in the Resource Management folder. An IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing this procedure

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the Microsoft Windows installation to which you want to provision the user.

3.2 Performing Provisioning Operations

Provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in [Section 3.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."](#)

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

See Also: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- [Section 3.2.1, "Direct Provisioning"](#)
- [Section 3.2.2, "Request-Based Provisioning"](#)

3.2.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
 - If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. From the Users menu, select **Create**.
 - b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
 - If you are using Oracle Identity Manager release 11.1.1, then:
 - a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
 - b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
 - If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. From the Users menu, select **Manage**.

following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

Note: The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- [Section 3.2.2.1, "End User's Role in Request-Based Provisioning"](#)
- [Section 3.2.2.2, "Approver's Role in Request-Based Provisioning"](#)

3.2.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.
The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **Windows 2000**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
 - Effective Date
 - Justification

On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.2.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

A message confirming that the task was approved is displayed.

3.3 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

Note: It is assumed that you have performed the procedure described in [Section 2.3.6, "Enabling Request-Based Provisioning."](#)

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **Windows 2000** process definition.
 - c. Deselect the Auto Save Form check box.
 - d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the **Windows 2000** resource object.
 - c. Deselect the Self Request Allowed check box.
 - d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning to request-based provisioning, then:

1. Log in to the Design Console.

2. Enable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **Windows 2000** process definition.
 - c. Select the **Auto Save Form** check box.
 - d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the **Windows 2000** resource object.
 - c. Select the Self Request Allowed check box.
 - d. Click the Save icon.

Testing and Troubleshooting

You can use the testing utility to directly use the connector for identifying the cause of problems associated with connecting to the target system server and performing basic operations on the target system.

To use the testing utility:

1. Copy the contents of the test directory on the installation media, to one of the following directories:

- If you are using Oracle Identity Manager release 9.1.0.x, then:

Copy files from the test/config directory on the installation media to the *OIM_HOME/xellerate/XLIntegrations/Windows2000/config* directory.

Copy files from the test/scripts directory on the installation media to the *OIM_HOME/xellerate/XLIntegrations/Windows2000/scripts* directory.

- If you are using Oracle Identity Manager release 11.1.1, then:

Copy files from the test/config directory on the installation media to the *OIM_HOME/server/XLIntegrations/Windows2000/config* directory.

Copy files from the test/scripts directory on the installation media to the *OIM_HOME/server/XLIntegrations/Windows2000/scripts* directory.

Note: You must create the destination directories on the Oracle Identity Manager host computer if they are not present.

2. Open the following file:

- If you are using Oracle Identity Manager release 9.1.0.x, then:

OIM_HOME/xellerate/XLIntegrations/Windows2000/config/config.properties

- If you are using Oracle Identity Manager release 11.1.1, then:

OIM_HOME/server/XLIntegrations/Windows2000/config/config.properties

3. Specify values for the attributes in this file. These attributes are described in the following table.

Attribute	Description	Sample Value
Action	Specifies the provisioning action to be performed by the testing utility	CREATE_DIRECTORY CREATE_SHARE DELETE_SHARE
Admin_ID	Specifies the user ID of the Microsoft Windows 2003 server administrator	dmsadmin
Domain_Name	Specifies the domain name of the Microsoft Windows 2003 server	sagemdms
Computer_Name	Specifies the IP address or computer name of the Microsoft Windows 2003 server	172.21.106.90
Share_Path	Specifies the share path Note: The path separator must be '\\\' and not '\\\'.	c:\\temp
Share_Name	Specifies the name of the share	testshare

4. After you specify values in the config.properties file, run the runWindowsTest.bat or runWindowsTest.sh file. This file is located in the scripts directory on the installation media.
5. If the script runs without any error, then verify that the required provisioning action has been carried out on the target system.

Known Issues

The following are known issues associated with this release of the connector:

- **Bug 5691610**
The connector does not support deployment scenarios in which Oracle Identity Manager is installed on an operating system other than Microsoft Windows.
- **Bug 7490324**
For a provisioning operation, the file server, Oracle Identity Manager, and the target system account used by Oracle Identity Manager to perform provisioning operations must be on the same domain.

Index

A

adapters, compiling, 3-2

C

certified components, 1-1
changing input locale, 2-9
clearing server cache, 2-9
compiling adapters, 3-2
configuring
 connector for multiple installations of the target system, 3-1
configuring connector, 3-1
configuring provisioning, 3-2
connector configuration, 3-1
connector files and directories
 description, 2-1
connector installer, 2-3
connector testing, 4-1
connector version number, determining, 2-3

D

defining
 IT resources, 2-6
determining version number of connector, 2-3

E

enabling logging, 2-11

F

files and directories of the connector
 See connector files and directories

G

globalization features, 1-2

I

input locale, changing, 2-9
installing connector, 2-3
issues, 5-1
IT resources

defining, 2-6
parameters, 2-6

L

logging enabling, 2-11

M

multilanguage support, 1-2

P

parameters of IT resources, 2-6
problems, 5-1
provisioning
 direct provisioning, 3-2
 request-based provisioning, 3-2
provisioning functions, 1-4

S

server cache, clearing, 2-9
supported
 languages, 1-2
 releases of Oracle Identity Manager, 1-2
 target systems, 1-2

T

target system, multiple installations, 3-1
target systems
 supported, 1-2
testing the connector, 4-1

V

version number of connector, determining, 2-3

X

XML files
 description, 2-2

