Oracle® Identity Manager

Connector Guide for Novell GroupWise

Release 9.0.4

E10433-08

October 2015

Oracle Identity Manager Connector Guide for Novell GroupWise, Release 9.0.4

E10433-08

Primary Author: Gauhar Khan

Contributing Authors: Gowri.G.R, Alankrita Prakash, Deena Purushothaman

Contents

2 Deploying the Connector

3 Using the Connector

4 Testing and Troubleshooting

5 Known Issues

Index

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Novell GroupWise.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` 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 document is available in the Oracle Identity Manager Connector Pack documentation library:

`http://www.oracle.com/technology/documentation/oim.html`

Documentation Updates

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

`http://www.oracle.com/technology/documentation/index.html`

Conventions

This document uses the following text conventions:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	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 the Oracle Identity Manager Connector for Novell GroupWise?

This chapter provides an overview of the updates made to the software and documentation for the Novell GroupWise connector in release 9.0.4.12 of the Oracle Identity Manager connector pack.

> **Note:** Release 9.0.4.12 of the connector comes after release 9.0.4.2. Release numbers from 9.0.4.3 through 9.0.4.11 have not been used.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

See Also: *Oracle Identity Manager Release Notes*

Software Updates

The following sections discuss updates made from release 9.0.4 to the current release of the connector:

- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.1

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 11*g* 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 11*g* release 1 (11.1.1).

See Section 3.5.2, "Request-Based Provisioning" for more information.

Software Updates in Release 9.0.4.2

The following are the software updates in release 9.0.4.2:

- Using the Connector Installer
- Resolved Issues

Support for New Target System

From this release onward, the connector adds support for Novell GroupWise 7, 8 as target systems.

These target systems are mentioned in "Verifying Deployment Requirements".

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 "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.x" for more information.

Resolved Issues

The following table lists issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
5664763	While provisioning a mailbox to an OIM User, the values in the Visibility list on the process form were displayed in English when a non-English locale was selected for the Oracle Identity Manager deployment.	This issue has been resolved. For non-English locales, the values in the Visibility list on the process form are now being displayed in the respective locales instead of English.
5688673	While creating access policies in the Administrative and User Console, the values of the Participating Type list on the Create Access Policy page were displayed in English even when a non-English locale was selected for the Oracle Identity Manager deployment.	This issue has been resolved. The values of the Participation Type list are now being displayed in the respective locales instead of English.
7623037	Suppose an access policy for provisioning a mailbox to an OIM User was created. During the Create Mailbox provisioning operation for a large number of users, the Remote Manager stopped functioning as the native code for running this provisioning operation was not thread safe.	This issue has been resolved. The Remote Manager continues to function when mailboxes are simultaneously provisioned to multiple users that meet the criterion specified in the access policy. This is because, the native code has now been made thread safe.

Bug Number	Issue	Resolution
8451826	After a user reconciliation run, the user's distribution list membership information was not displayed on the distribution child form of the target system user's process form.	This issue has been resolved. After a user reconciliation run, the user's membership information is now being displayed.
8509388	When the Novell eDirectory and Novell GroupWise resources were provisioned to an OIM User, and the user and the corresponding mailbox were deleted from Novell eDirectory and Novell Groupwise respectively, the `GW_USER_DOES_NOT_EXIST` error message was displayed during a Move Post Office provisioning operation with Unknown response received as the detailed error message.	This issue has been resolved. If you perform a Move Post Office provisioning operation after you delete a user from Novell eDirectory and the corresponding mailbox from Novell GroupWise, then the Move PostOffice task displays the following error message: `User does not exist in eDirectory`
8521041	After a target resource reconciliation run, the Visibility list of the process form was blank.	This issue has been resolved. The values in the Visibility list of the process form are visible after a target resource reconciliation run.
8521163	During user reconciliation, user records that were not modified were fetched to Oracle Identity Manager and then disabled.	This issue has been resolved. During user reconciliation, user records that are not modified are not fetched in to Oracle Identity Manager.

Software Updates in Release 9.0.4.1

The following is the software update in release 9.0.4.1:

Changes in the Directory Structure of the Connector Files on the Installation Media

The `xliGroupWise65.jar` file has been split into two files, `xliGroupWise65.jar` and `xliGroupWiseRecon.jar`. Corresponding changes have been made in the following sections:

- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector
- Copying the Connector Files

Documentation-Specific Updates

The following documentation-specific updates have been made in the guide:

- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.2
- Documentation-Specific Updates in Release 9.0.4.1

Documentation-Specific Updates in Release 9.0.4.12

The following documentation-specific update has been made in revision "08" of release 9.0.4.12:

- A note has been removed from the "Target Systems" row of Table 1–1, " Certified Components".
- The description element of the "URL" row in Section 2.3.2.1.1, "GroupWise XRM" has been modified.

- Section 2.6, "Installation and Configuration on the Target System" has been added.
- The "Oracle Identity Manager" row in Table 1–1, " Certified Components" has been modified.

The following are documentation-specific updates in revision "7" of release 9.0.4.12:

- A note has been added to the "Target System" row of Table 1–1, " Certified Components".
- The path to locate and open the GroupwiseXLResourceObject.xml file has been updated in step 4 of Section 2.5.3, "Configuring Trusted Source Reconciliation."

The following are documentation-specific updates in revision "6" of release 9.0.4.12:

- The "Oracle Identity Manager" row in Table 1–1, " Certified Components" has been modified.
- A note has been added to the "Files in the DataSets directory" row of Table 2–1, " Files and Directories On the Connector Installation Media".
- The following sections have been added:
  - Section 2.5.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
  - Section 2.5.2, "Localizing Field Labels in UI Forms"
  - Section 3.6, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Section 2.3.1, "Running the Connector Installer"
  - Section 2.3.2, "Configuring IT Resources"
  - Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.x"
- In Table 1–1, " Certified Components", a note has been added in the target system row.

In earlier revisions of release 9.0.4.12, major changes have been made to the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of the information provided by the guide.

Documentation-Specific Updates in Release 9.0.4.2

The following are documentation-specific updates in release 9.0.4.2:

- Some of the sections in the "Deploying the Connector" chapter have been rearranged.
- The "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.x" section has been added.
- The "Configuring the Connector for Multiple Installations of the Target System" section has been removed from the "Using the Connector" chapter.
- The "Known Issues" chapter has been modified.
- From this release onward:
  - The minimum certified release of Oracle Identity Manager is release 9.1.0.1.
  - The minimum certified release of JDK is release 1.4.2.

See "Verifying Deployment Requirements" section for the complete listing of certified components.

Documentation-Specific Updates in Release 9.0.4.1

There are no documentation-specific updates in this release of the guide.

1 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 Novell GroupWise.

This chapter contains the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "Lookup Definitions Used During Reconciliation and Provisioning"
- Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning"
- Section 1.7, "Connector Objects Used During Trusted Source Reconciliation"
- Section 1.8, "Roadmap for Deploying and Using the Connector"

> **Note:** In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.
>
> At some places in this guide, Novell GroupWise has been referred to as the *target system.*

1.1 Certified Components

Table 1–1 lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.0.1 through 9.0.3.*x* ■ Oracle Identity Manager release 9.1.0.1 and any later BP in this release track **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 supports. ■ Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1) and future releases in this release track. ■ Oracle Identity Manager 11g release 1 PS1 (11.1.1.5.0) and any later BP in this release track ■ Oracle Identity Manager 11g release 1 PS2 (11.1.1.7.0) and any later BP in this release track ■ Oracle Identity Manager 11*g* release 2 BP04 (11.1.2.0.4) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.2** has been used to denote Oracle Identity Manager 11*g* release 2 BP04 (11.1.2) and future releases in this release track. ■ Oracle Identity Manager 11g release 2 PS1 (11.1.2.1.0) and any later BP in this release track ■ Oracle Identity Manager 11g release 2 PS2 (11.1.2.2.0) and any later BP in this release track The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at `http://www.oracle.com/technetwork/documentation/oim1014-097544.html`
Target systems	Novell GroupWise 6.5, 7, or 8.
Target system user account	Novell GroupWise user account to which the Supervisor right has been assigned You provide the credentials of this user account while performing the procedure in one of the following sections: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: Section 2.4.2, "Importing the Connector XML File" ■ For Oracle Identity Manager release 11.1.*x*: Section 2.3.2, "Configuring IT Resources" If this target system user account is not assigned the specified rights, then the following error message may be displayed during connector operations: `Transaction is not active (Transaction Manager error)`

Table 1–1 (Cont.) Certified Components

Item	Requirement
Other systems	Novell eDirectory 8.7.3
External code	tcGroupWise65.dll, ldap.jar, ldapbp.jar **Note:** The tcGroupWise65.dll is bundled with the rest of the connector installation files on the installation media.
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x*, use JDK 1.4.2 or a later release in the 1.4.2 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series. ■ For Oracle Identity Manager release 11.1.*x*, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

The connector supports the following languages:

- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

Note: Novell GroupWise does not support the entry of non-ASCII characters. See Chapter 5, "Known Issues" for more information about this limitation.

See Also: One of the following guides for information about supported special characters:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*:

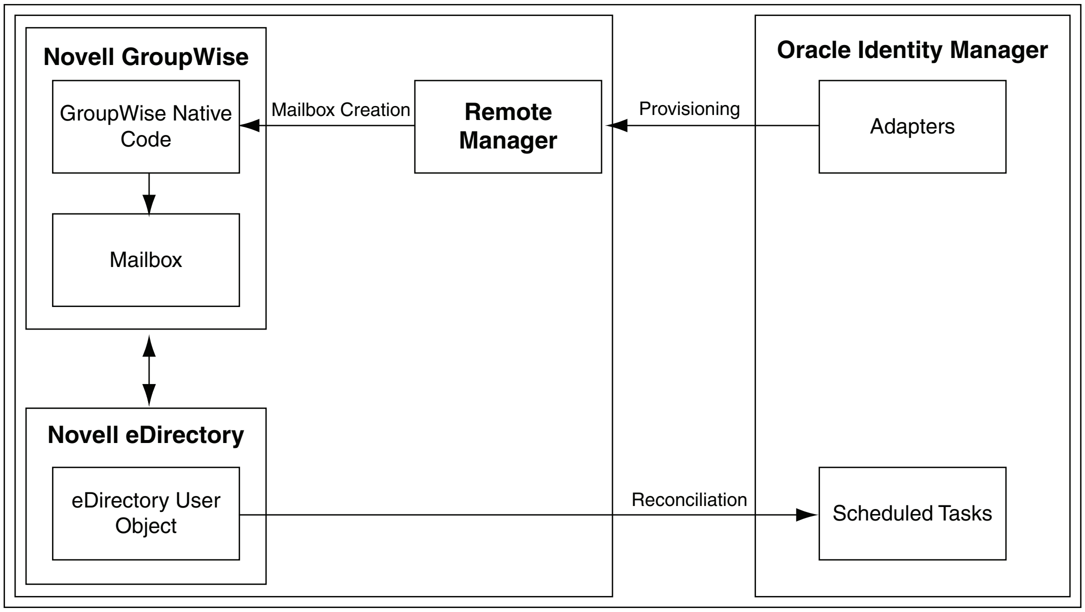
  Oracle Identity Manager Globalization Guide

- For Oracle Identity Manager release 11.1.*x*:

  Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager

1.3 Connector Architecture

Figure 1–1 Connector Architecture



Novell Groupwise uses Novell eDirectory as a user repository to store information about a user's mailbox.

During provisioning, adapters carry provisioning data submitted through the process form to the target system. The Remote Manager on the target system passes the provisioning data to the native GroupWise code. By using the information available in the user's eDirectory profile, the native GroupWise code creates the mailbox.

During reconciliation, scheduled tasks fetch user mailbox data from the target system into Oracle Identity Manager.

1.4 Features of the Connector

- Section 1.4.1, "Support for Both Target Resource and Trusted Source Reconciliation"
- Section 1.4.2, "Support for Limited Reconciliation"
- Section 1.4.3, "Support for Batched Reconciliation"
- Section 1.4.4, "Support for Both Full and Incremental Reconciliation"
- Section 1.4.5, "Support for Reconciliation of Deleted User Records"

1.4.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure Novell GroupWise as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3, "Configuring Reconciliation" for more information.

1.4.2 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the CustomizedReconQuery attribute of the GroupWise IT Resource. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See Section 3.3.2, "Limited Reconciliation" for more information.

1.4.3 Support for Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See Section 3.3.3, "Batched Reconciliation" for more information.

1.4.4 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time. See Section 3.3.1, "Full Reconciliation" for more information.

1.4.5 Support for Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records by setting the value of the XLDeleteUsersAllowed attribute of the scheduled task to `true.` In target resource mode, if a record is deleted on the target system, then the corresponding GroupWise resource is revoked from the OIM User. In trusted source mode, if a record is deleted on the target system, then the corresponding OIM User is deleted.

See Section 3.3.4, "User Reconciliation Scheduled Task" for more information about the XLDeleteUsersAllowed attribute.

1.5 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during connector operations can be divided into the following categories:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Other Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

The following lookup definitions are populated with values fetched from the target system by the scheduled tasks for lookup field synchronization:

> **See Also:** Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about these scheduled tasks

- For Distribution List: Lookup.NGW.DistributionLists
- For Post Office List: Lookup.NGW.PostOffices

1.5.2 Other Lookup Definitions

Table 1–2 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–2 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.NGW.Configuration	This lookup definition maps visibility levels of accounts fetched from the target system with corresponding visibility levels to be displayed in the Visibility field of the OIM User form.	This lookup definition is prepopulated with values. You cannot add or modify entries in this lookup definition.
AttrName.Recon.Map.GW	This lookup definition user attribute mappings between Novell GroupWise and Oracle Identity Manager.	This lookup definition is prepopulated with values, and it is used during reconciliation runs. **Note:** Fields in the AttrName.Recon.Map.GW lookup definition that do not begin with the ldap prefix cannot have duplicate values.
Lookup.NGW.ParticipationType	This lookup definition holds information about the participation type that you can select for the user being added to the distribution list.	This lookup definition is prepopulated with values. You cannot add or modify entries in this lookup definition.
Lookup.NGW.Visibility	This lookup definition holds information about the visibility levels that you can select for the target system account that you create through Oracle Identity Manager.	This lookup definition is prepopulated with values. You cannot add or modify entried in this lookup definition.

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

The following sections provide information about connector objects used during target resource reconciliation and provisioning:

> **See Also:** One of the following guides for conceptual information about reconciliation:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
> - For Oracle Identity Manager release 11.1.*x*: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following sections provide information about connector objects used during reconciliation:

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Distribution List Attributes for Target Resource Reconciliation and Provisioning"

- Section 1.6.3, "Nick Names Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.4, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.6, "Provisioning Functions"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 provides information about user attribute mappings for target resource reconciliation and provisioning.

Table 1–3 User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Field	Description
User ID	cn	User's login ID
Visibility	nGWVisibility	Visibility of user in GroupWise system
File ID	nGWFileID	GroupWise user's unique FileID
Exp Date	nGWMailboxExpirationTime	GroupWise Mailbox expiration date
Gateway Account ID	nGWAccountID	User's GateWay account ID
Gateway Access	nGWGatewayAccess	Restricts access to a GroupWise gateway

1.6.2 Distribution List Attributes for Target Resource Reconciliation and Provisioning

Table 1–4 provides information about distribution list attribute mappings for target resource reconciliation and provisioning.

Table 1–4 Distribution List Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Group Attribute	Description
Dist List	distlist	Public address list
Participant	participant	Recipient type (To, Cc, or Bcc) of the user for e-mail messages received from the distribution list.

1.6.3 Nick Names Attributes for Target Resource Reconciliation and Provisioning

Table 1–5 provides information about nick names attribute mappings for target resource reconciliation and provisioning.

Table 1–5 Nick Names Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Role Attribute	Description
Nick Name	nickname	Alternative address
NNVisibility	visibility	Determines the post office to which the object's information is distributed

1.6.4 Reconciliation Rule for Target Resource Reconciliation

> **See Also:** One of the following guides for generic information about reconciliation matching and action rules:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
> - For Oracle Identity Manager release 11.1.*x*: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process-matching rule:

Rule name: GroupWise Recon User

Rule element: User Login Equals User ID

In this rule:

- User Login is one of the following:
  - For Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*:

    User ID attribute on the Xellerate User form.
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.*x*:

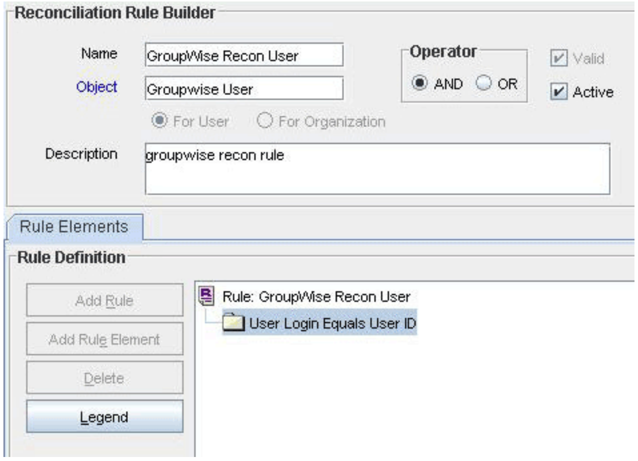
    User ID attribute on the OIM User form.
- User ID is the cn attribute of Novell Groupwise.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **GroupWise Recon User**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



Reconciliation Rule Builder

Name: GroupWise Recon User

Object: Groupwise User

● For User ○ For Organization

Description: groupwise recon rule

Operator: ● AND ○ OR

☑ Valid

☑ Active

Rule Definition

Rule: GroupWise Recon User

User Login Equals User ID

1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–6 lists the action rules for target resource reconciliation.

Table 1–6 Action Rules for Target Resource Reconciliation

Rule Condition	Action
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

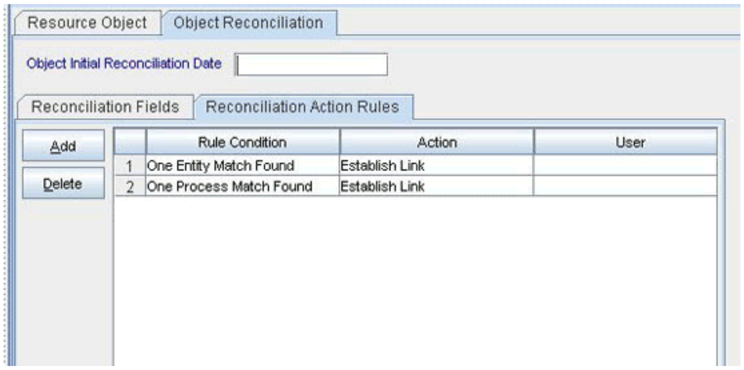
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.*x*: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **GroupwiseUser** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



	Rule Condition	Action	User
1	One Entity Match Found	Establish Link	
2	One Process Match Found	Establish Link	

1.6.6 Provisioning Functions

Table 1–7 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1–7 Provisioning Functions

Function	Adapter
Create a mailbox	NGW Create Mailbox
Delete a mailbox	NGW Delete Mailbox
Disable a mailbox	NGW Disable Mailbox
Enable a mailbox	NGW Enable Mailbox
Move a user from one post office to another	NGW Move User To PostOffice
Update a user	NGW Modify Mailbox
Add a user to a distribution list	NGW Add User to Distribution List
Remove a user from a distribution list	NGW Remove User from Distribution List
Add a nickname or alias for a user	NGW Add Nickname to User
Delete the nickname or alias of a user	NGW Delete Nickname of User
Reset user password	NGW Reset Password

1.7 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–8 lists user attributes for trusted source reconciliation.

Table 1–8 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Target System Attribute	Description
User ID	cn	User's logon name **Note:** The value reconciled into the User ID field is also reconciled into both the First Name and Last name fields.
First Name	cn	First name
Last Name	cn	Last name
Employee Type	NA	Default value: `Consultant`
User Type	NA	Default value: `End-User Administrator`
Organization	NA	Default value: `Xellerate Users`

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

> **See Also:** One of the following guides for generic information about reconciliation matching and action rules:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
> - For Oracle Identity Manager release 11.1.*x*: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process matching rule:

Rule name: Trusted Source recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is one of the following:
  - For Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*:

    User ID attribute on the Xellerate User form.
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.*x*:

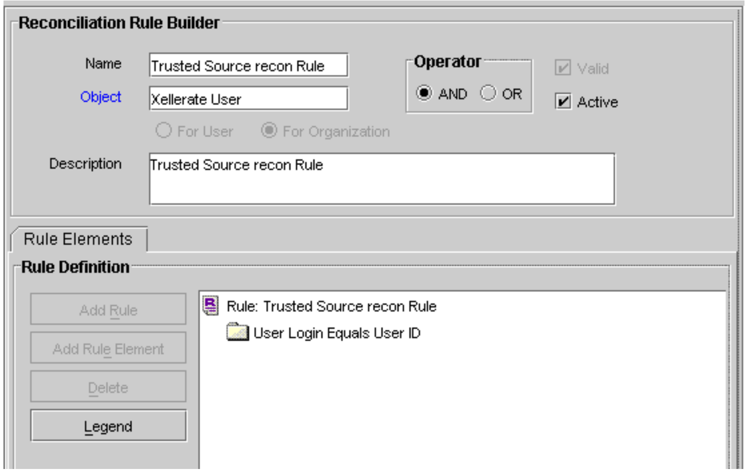
    User ID attribute on the OIM User form.
- User ID is the cn attribute of Novell GroupWise.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Trusted Source recon**. Figure 1–4 shows the reconciliation rule for trusted source reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation


Reconciliation Rule Builder

Name: Trusted Source recon Rule

Object: Xellerate User

Operator: ● AND ○ OR

☑ Valid

☑ Active

○ For User ● For Organization

Description: Trusted Source recon Rule

Rule Elements

Rule Definition

Rule: Trusted Source recon Rule

User Login Equals User ID

1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–9 lists the action rules for target resource reconciliation.

Table 1–9 Action Rules for Target Source Reconciliation

Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

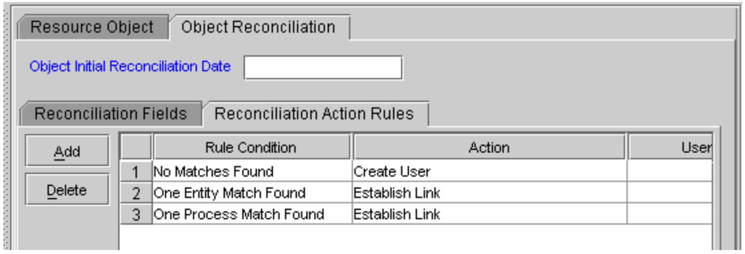
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.*x*: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rules for trusted source reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



Object Initial Reconciliation Date

	Rule Condition	Action	User
1	No Matches Found	Create User	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.8 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, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Testing and Troubleshooting" describes the procedure to use the connector testing utility for testing the connector.
- Chapter 5, "Known Issues" lists known issues associated with this release of the connector.

2 Deploying the Connector

Deploying the connector involves the following steps:

- Section 2.1, "Files and Directories on the Installation Media"
- Section 2.2, "Determining the Release Number of the Connector"
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Section 2.3, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.x"
  - Section 2.4, "Installing the Connector on Oracle Identity Manager Release 9.0.1 through 9.0.3.x"
- Section 2.5, "Configuring the Oracle Identity Manager Server"
- Section 2.6, "Installation and Configuration on the Target System"
- Section 2.7, "Configuring SSL"

2.1 Files and Directories on the Installation Media

Table 2–1 lists the files and directories on the installation media.

Table 2–1 Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
Files in the DataSets directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation. **Note:** These files are applicable to Oracle Identity Manager releases prior to 11.1.2.
lib/xliGroupWise65.jar	This JAR file contains the class files required for provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database
lib/xliGroupWiseRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database
lib/tcGroupWise65.dll	This DLL file contains the native code required to communicate with the Novell GroupWise client.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database **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.
test/troubleshoot/tcGroupWise65.dll	This file contains the native code required to interface with Novell GroupWise.
test/troubleshoot/tstGroupWise65.jar	This file contains the wrapper files and the test utility class.
test/troubleshoot/testcreate.bat test/troubleshoot/testmodify.bat test/troubleshoot/testdelete.bat	These batch files are used to run specific tests on the connector. They call the appropriate method in the test utility class.
test/troubleshoot/config.properties	In this configuration file, connection information about Novell eDirectory and Novell GroupWise and other related parameters are specified.

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

File in the Installation Media Directory	Description
test/troubleshoot/log4j.properties	This file is used to specify the directory in which the log file is to be created when you run the testing utility.
xml/xliGroupwiseResourceObject.xml	This file contains definitions for the following components of the connector: ▪ IT resource type ▪ Process form ▪ Process task and rule-generator adapters (along with their mappings) ▪ Resource object ▪ Provisioning process ▪ Pre-populate rules that are used with this connector
xml/ GroupwiseXLResourceObject.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.

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

2.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.*x,* 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/xliGroupWise65.jar

2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the xliGroupWise65.jar file.

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

2.3 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.x

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

Installing the connector on Oracle Identity Manager release 9.1.0.*x* or release 11.1.*x* involves the following procedure:

- Section 2.3.1, "Running the Connector Installer"
- Section 2.3.2, "Configuring IT Resources"

2.3.1 Running the Connector Installer

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, copy this JAR file to 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.*x*:
     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 the following guide:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide

   - For Oracle Identity Manager release 11.1.*x*:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

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, in the System Management region, click **Install Connector**.

   - For Oracle Identity Manager release 11.1.2:

     In the left pane, under System Management, click **Manage Connector.** In the Manage Connector page, click **Install.**

4. From the Connector List list, select **Novell GroupWise** ***RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in 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 **Novell GroupWise** ***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 Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see Section 2.5.3, "Configuring Trusted Source Reconciliation"or more information.

   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 Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.5.6, "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.

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 Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Section 2.1, "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.

2.3.2 Configuring IT Resources

You must specify values for the parameters of the GroupWise XRM, eDirectory IT Resource, and GroupWise IT Resource IT resource as follows:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.*x* or 11.1.1:

     Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2:

     Log in to Oracle Identity System Administration
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.*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.**
   - If you are using Oracle Identity Manager release 11.1.2, then in the left pane under Configuration, click **IT Resource**.
3. In the IT Resource Name field on the Manage IT Resource page, enter `GroupWise IT Resource` 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 GroupWise IT Resource IT resource. See Section 2.3.2.1, "Specifying Values for IT Resource Parameters" for information about the parameters of the IT resource and the values to be specified.
7. To save the values, click **Update.**
8. On the View IT Resource Details and Parameters page, click **Back to Search Results.**
9. Repeat Steps 3 through 8 for the GroupWise XRM and eDirectory IT Resource IT resources.

2.3.2.1 Specifying Values for IT Resource Parameters

This section provides information about the parameters for the following IT resources:

- GroupWise XRM
- eDirectory IT Resource
- GroupWise IT Resource

2.3.2.1.1 GroupWise XRM

You must specify values for the Groupwise XRM IT resource parameters listed in the following table.

Parameter	Description
Service Name	Name of the remote manager Default value: `RManager`
URL	Host name or IP address of the server hosting the remote manager Sample value: `rmi://10.0.0.1:12345`

After you specify values for these IT resource parameters, proceed to Step 7 of the procedure to configure IT resources.

2.3.2.1.2 eDirectory IT Resource You must specify values for the eDirectory IT Resource IT resource parameters listed in the following table.

Parameter	Description
Admin Id	DN of the user who has administrator rights on the target LDAP If this administrator has read/search rights, then that would be sufficient because this administrator is used only to search for existing users and no modification is done in Novell eDirectory. Sample value: `cn=Admin,ou=People, o=xyz`
Admin Password	Password of the administrator Sample value: `password`
Server Address	Host name or IP address of the server hosting Novell eDirectory
Root DN	Base DN from where the search for the user starts Sample value: `o=xyz`
Port	Port number of the Novell eDirectory server Sample value: `389`
SSL	Specifies whether or not SSL is to be used to secure communication between Oracle Identity Manager and Novell GroupWise The value can be `true` or `false.` If it is set to `true,` then you must import the certificate of the Novell eDirectory server into the Oracle Identity Manager server. **Note:** It is recommended that you enable SSL to secure communication with the target system.
Last Recon TimeStamp	For the first reconciliation run, the time stamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter. Sample value: `2006-06-02 12:08:06`
Prov Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning The value must be `AttrName.Prov.Map.EDIR.`
Recon Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for reconciliation The value must be `AttrName.Recon.Map.EDIR.`

Parameter	Description
Use XL Org Structure	If set to `true,` then the Oracle Identity Manager Organization structure is used during provisioning and reconciliation. If set to `false,` then the value of the Organization field in the process form is used for provisioning and the organization or container in the target Oracle Internet Directory is used for reconciliation.

After you specify values for these IT resource parameters, proceed to Step 7 of the procedure to configure IT resources.

2.3.2.1.3 GroupWise IT Resource You must specify values for the GroupWise IT Resource IT resource parameters listed in the following table.

Parameter	Description
GroupWise Domain DN or Path	See the "GroupWise Domain DN or Path" section for detailed information about this parameter.
Admin User ID	DN of the user who has administrator rights on the target Novell GroupWise server This administrator must have read/write access to the Novell GroupWise system/domain database. Ensure that this DN is entered in the dot format and not in the comma format. For example: `cn=admin.ou=admgrp` (Correct) `cn=admin,ou=admgrp` (Incorrect)
Admin Password	Password of the administrator
eDir Context	The Novell eDirectory context below which the administrator is present. The administrator ID plus this context should be the complete DN of the administrator. This context is usually one level below the eDirectory tree. For example: Suppose the DN of the administrator is as follows: `cn=admin.ou=admgrp.o=marketing` Then, the value of this parameter can be either `o=marketing` or `marketing`.
eDir Server Address	Host name or IP address of the server hosting Novell eDirectory
eDir Tree	Name of the Novell eDirectory tree under which the Novell GroupWise domain and the administrator are present This is the topmost level in Novell eDirectory. Sample value: `ExampleWidgets`
UseEDirAuth	Specifies whether the target Novell GroupWise uses the Novell eDirectory password or the Novell GroupWise password for authentication. If it is set to `true,` then the password is sent as an empty string when the Create Mailbox and Change User password/Reset Password functions are run. The password specified by the user is ignored. If it is set to `false,` then the password specified is set as the mailbox password.

Parameter	Description
Last Recon TimeStamp	The value is empty for the first reconciliation run. After that, the time at which the last reconciliation run was completed is stored in this parameter.
Recon Attribute Lookup Code	Contains the target attributes to be reconciled Sample lookup definition: `AttrName.Recon.Map.GW`
CustomizedReconQuery	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the `AND` (&) and `OR` (|) logical operators. Sample value: `givenname=John` For more information about this parameter, refer to the "Limited Reconciliation" section on page 3-4.

GroupWise Domain DN or Path

The complete DN of the Novell GroupWise domain or the path of the domain folder must be specified in one of the following ways:

- Local System Path

  The local system path can be specified in any one of the following ways:

  – By using the Domain DN path as follows:

  ```
  Domain DN: 'cn=GWdomain.ou=org_unit_name.dc=companyname.dc=com.o=org_name'
  ```

  For example:

  ```
  Domain DN: 'cn=MyGWdomain.ou=MyDomains.dc=ExampleWidgets.dc=com.o=EXAMPLE'
  ```

  Note: Use dots (not commas) to separate the object classes as shown in the preceding example.

  – By using the local directory path as follows:

  ```
  drive:\\domain_directory_path
  ```

  For example:

  ```
  f:\\groupwise\\testdomain
  ```

- UNC Path

  The UNC path can be specified in any one of the following ways:

  – By using the host name as follows

  ```
  \\hostname\share\\domainfolder
  ```

  For example

```
\\testsvr\\myshare\\testdomain
```

- By using the IP address as follows:

  \\IPaddress\\share_name\\domain_name

  For example:

  ```
  \\10.0.0.1\\myshare\\testdomain
  ```

The recommended method is to use the DN or the local directory path. If the domain is on a different computer, then map that folder locally and mention the local path. Use this method if you are not able to connect to the domain by using the DN.

After you specify values for these IT resource parameters, proceed to Step 7 of the procedure to configure IT resources.

2.4 Installing the Connector on Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*

Installing the connector on any Oracle Identity Manager release between release 8.5.3.1 through 9.0.3.*x* involves the following procedures:

- Section 2.4.1, "Copying the Connector Files"
- Section 2.4.2, "Importing the Connector XML File"
- Section 2.4.3, "Compiling Adapters"

2.4.1 Copying the Connector Files

The connector files to be copied and the directories to which you must copy them are given in the following table.

> **Note:** See Section 2.1, "Files and Directories on the Installation Media" for more information about these files.

File in the Installation Media Directory	Destination Directory
lib/xliGroupWise65.jar	*OIM_HOME*/xellerate/JavaTasks
lib/xliGroupWiseRecon.jar	*OIM_HOME*/xellerate/ScheduleTask
lib/tcGroupWise65.dll	Copy this DLL file into a directory that is included in the `PATH` environment variable on the remote manager server.
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources
Files in the test/troubleshoot directory	*OIM_HOME*/xellerate/groupwise/test/troubleshoot
Files in the xml directory	*OIM_HOME*/xellerate/groupwise/xml

To copy the ldap.jar file into the required directory:

1. Log on to the Novell Web site at

   `http://developer.novell.com/wiki/index.php/Special:Downloads/jldap/builds/netware_windows/`

2. Download the following file from the Novell Web site:

   ```
   novell-jldap-devel-2005.10.03-1netware_windows.zip
   ```

   The size of the file is 11.1 MB.

3. Extract the contents of the file that you downloaded in Step 2.

4. Copy the ldap.jar file from the novell-jldap-devel-2005.10.03-1netware_windows\jldap_2005.10.03\lib directory to the *OIM_HOME*\xellerate\ThirdParty directory on the Oracle Identity Manager server.

To copy the ldapbp.jar file into the required directory:

1. Log on the following Web site:

   `http://java.sun.com/products/jndi/downloads/index.html`

2. Click the **Download JNDI 1.2.1 & More** button.

3. From the table on the page that is displayed, select the **LDAP Service Provider 1.2.4** check box and download the ldap-1_2_4.zip file.

4. Extract the ldapbp.jar file from the ldap-1_2_4.zip file.

5. Copy the ldapbp.jar file into the *OIM_HOME*/xellerate/ThirdParty directory on the Oracle Identity Manager server.

> **Note:** While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the contents of the connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.

2.4.2 Importing the Connector XML File

Perform this procedure only if you are using Oracle Identity Manager release 9.*x*. As mentioned in Section 2.1, "Files and Directories on the Installation Media," the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.

3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.

4. Locate and open the xliGroupwiseResourceObject.xml file, which is in the *OIM_HOME*/xellerate/groupwise/xml directory. Details of this XML file are shown on the File Preview page.

5. Click **Add File**. The Substitutions page is displayed.

6. Click **Next**. The Confirmation page is displayed.

7. Click **Next**. The Provide IT Resource Instance Data page for the GroupWise XRM IT resource is displayed.

8. Specify values for the parameters of the GroupWise IT Resource IT resource. See Section 2.3.2.1, "Specifying Values for IT Resource Parameters" for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the Remote Manager resource type is displayed.
10. Repeat Steps 7, 8, and 9 for the GroupWise XRM and eDirectory IT Resource IT resources.
11. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

    See Also: If you want to define another IT resource, then see *Oracle Identity Manager Administrative and User Console Guide* for instructions.

12. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.

13. Click **Import**. The connector file is imported into Oracle Identity Manager.

2.4.3 Compiling Adapters

> **Note:** Perform the procedure described in this section *only* if you want to use the provisioning features of Oracle Identity Manager for this target system.

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

> **See Also:** Section 1.6.6, "Provisioning Functions" for a listing of the provisioning functions that are available with this connector

- NGW Create Mailbox
- NGW Delete Mailbox
- NGW Disable Mailbox
- NGW Enable Mailbox
- NGW Move User to PostOffice
- NGW Add User to Distribution List
- NGW Remove User from Distribution List
- NGW Add Nickname to User
- NGW Reset Password
- NGW Change User Password
- NGW PP String
- NGW Delete Nickname of User

You must compile these adapters before they can be used in provisioning operations.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you import into the current database, select **Compile All**.

   To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

   > **Note:** Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an `OK` compilation status.

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM_HOME*/xellerate/Adapter directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

If you want to compile one adapter at a time, then use the Adapter Factory form.

> **See Also:** For information about using the Adapter Factory and Adapter Manager forms, see one of the following guides:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:
>
>   Oracle Identity Manager Tools Reference Guide
>
> - For Oracle Identity Manager release 11.1.*x*:
>
>   *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

2.5 Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves performing the following procedures:

- Section 2.5.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
- Section 2.5.2, "Localizing Field Labels in UI Forms"
- Section 2.5.3, "Configuring Trusted Source Reconciliation"
- Section 2.5.4, "Configuring the Date Format"
- Section 2.5.5, "Changing to the Required Input Locale"

- Section 2.5.6, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.5.7, "Enabling Logging"
- Section 2.5.8, "Configuring Oracle Identity Manager for Request-Based Provisioning"

2.5.1 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- Section 2.5.1.1, "Tagging Form Fields"
- Section 2.5.1.2, "Creating and Activating a Sandbox"
- Section 2.5.1.3, "Creating a New UI Form"
- Section 2.5.1.4, "Creating an Application Instance"
- Section 2.5.1.5, "Publishing a Sandbox"
- Section 2.5.1.6, "Harvesting Entitlements and Sync Catalog"
- Section 2.5.1.7, "Updating an Existing Application Instance with a New Form"

2.5.1.1 Tagging Form Fields

You must add properties to certain form fields. To do so:

1. Log in to Oracle Identity Manager Design Console.
2. Open User Distribution Lists form (UD_NGW_DIST).
3. Create a new form version.
4. In the **Properties** tab, for the **Distribution List DN** field, add `Entitlement = true` property.
5. Click **Make Version Active.**
6. Open Groupwise parent form (UD_NGWS_USR).
7. Create a new form version.
8. In the **Properties** tab, add the following properties:

   For the **GroupWise Server** field, add `ITResource = true` property.

   For the **User ID** field, add `AccountName = true` property.

   For the **User ID** field, add `AccountId = true` property.
9. Click **Make Version Active.**

2.5.1.2 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see the "Managing Sandboxes" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes.** The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox.** The Create Sandbox dialog box is displayed.

3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
5. Click **Save and Close.** A message is displayed with the sandbox name and creation label.
6. Click **OK.** The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. Select the sandbox that you created.
8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
9. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

2.5.1.3 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see the "Managing Forms" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer.**
2. Under Search Results, click **Create.**
3. Select the resource type for which you want to create the form, for example, `GroupWise IT resource.`
4. Enter a form name and click **Create.**

2.5.1.4 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see the "Managing Application Instances" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances.**
2. Under Search Results, click **Create.**
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**
4. In the Form drop-down list, select the newly created form and click **Apply.**
5. Publish the application instance for a particular organization.

2.5.1.5 Publishing a Sandbox

To publish the sandbox that you created in Section 2.5.1.2, "Creating and Activating a Sandbox":

1. Close all the open tabs and pages.
2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Section 2.5.1.2, "Creating and Activating a Sandbox."

3. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.5.1.6 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Section 3.2, "Scheduled Task for Lookup Field Synchronization."
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.

2.5.1.7 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Section 2.5.1.2, "Creating and Activating a Sandbox."
2. Create a new UI form for the resource as described in Section 2.5.1.3, "Creating a New UI Form."
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in Section 2.5.1.5, "Publishing a Sandbox."

> **Note:** If you are using Oracle Identity Manager 11*g* Release 2 (11.1.2.0.4) or later, then you must perform the steps mentioned in MetaLink note 1535369.1 to ensure provisioning operations work as expected.
>
> See the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for the procedure to display the user-defined fields (UDFs), such as eDirectory Connector Version, GroupWise Connector Version, and GUID, on the user interface (UI).

2.5.2 Localizing Field Labels in UI Forms

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2 or later and you want to localize UI form field labels.

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:

   a. Search for the following text:

   ```
   <file source-language="en"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   b. Replace with the following text:

   ```
   <file source-language="en" target-language="LANG_CODE"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   In this text, replace LANG_CODE with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

   ```
   <file source-language="en" target-language="ja"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   c. Search for the application instance code. This procedure shows a sample edit for Novell GroupWise application instance. The original code is:

   ```
   <trans-unit
   id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
   ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
   rEO.UD_NGWS_USR_GATEWAY_ACCESS__c_description']}">
   <source>Gateway Access</source>
   <target/>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.GRPFORM.entity.GRPFORMEO.UD
   _NGWS_USR_GATEWAY_ACCESS__c_LABEL">
   <source>Gateway Access</source>
   <target/>
   </trans-unit>
   ```

   d. Open the resource file from the connector package, for example GroupWise_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_NGWS_USR_GATEWAY_ACCESS=\u30B2\u30FC\u30C8\u30A6\u30A7\u30A4\u30FB\u30A2\u30AF\u30BB\u30B9.

   e. Replace the original code shown in Step 6.c with the following:

   ```
   <trans-unit
   id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
   ```

```
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_NGWS_USR_GATEWAY_ACCESS__c_description']}">
<source>Gateway Access</source>
<target>\u30B2\u30FC\u30C8\u30A6\u30A7\u30A4\u30FB\u30A2\u30AF\u30BB\u30B9<
/target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.GRPFORM.entity.GRPFORMEO.UD
_NGWS_USR_GATEWAY_ACCESS__c_LABEL">
<source>Gateway Access</source>
<target>\u30B2\u30FC\u30C8\u30A6\u30A7\u30A4\u30FB\u30A2\u30AF\u30BB\u30B9<
/target>
</trans-unit>
```

f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace LANG_CODE with the code of the language to which you are localizing.

   Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

   See Also: The "Deploying and Undeploying Customizations" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager,* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Identity Manager.

2.5.3 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

Note: You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, GroupwiseXLResourceObject.xml, by using the Deployment Manager. This section describes the procedure to import the XML file.

   Note: Only one target system can be designated as a trusted source. If you import the GroupwiseXLResourceObject.xml file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Set the TrustedSource scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation bar.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.*x,* then:
   a. On the Welcome page, click **Advanced** in the upper-right corner.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File.** A dialog box for opening files is displayed.
4. Locate and open the GroupwiseXLResourceObject.xml file, which is in the following directory:
   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x:*

     OIM_HOME/xellerate/ConnectorDefaultDirectory/GroupWise_904120/xml
   - For Oracle Identity Manager release 11.1.*x:*

     OIM_HOME/server/ConnectorDefaultDirectory/GroupWise_904120/xml
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

After you import the XML file for trusted source reconciliation, you must set the value of the TrustedSource reconciliation scheduled task attribute to `True`. This procedure is described in Section 3.4, "Configuring Scheduled Tasks."

2.5.4 Configuring the Date Format

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

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

- Section 2.5.4.1, "Configuring the Date Format on Oracle Identity Manager release 9.0.1 through 9.0.3.x or Release 9.1.0.x"
- Section 2.5.4.2, "Configuring the Date Format on Oracle Identity Manager Release 11.1.x"

2.5.4.1 Configuring the Date Format on Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or Release 9.1.0.*x*

To configure the date format on Oracle Identity Manager:

1. Open the Oracle Identity Manager Design Console.

2. Expand **Administration,** and the double-click **System Configuration.**
3. Add a new entry in the `Server` category. The following are the details:

   Name: `Default date format`

   Keyword: `XL.DefaultDateFormat`

   Value: `yyyy/MM/dd hh:mm:ss z`
4. Click **Save.**

2.5.4.2 Configuring the Date Format on Oracle Identity Manager Release 11.1.x

To configure the date format on Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner.
3. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search System Properties.** Alternatively, you can click the **System Management** tab, and then click **System Configuration.**
4. On the left pane, search and open for the **Default date format** system property.
5. On the System Property Detail page, enter values for the following fields:
   - **Property Name:** `Default Date Format`
   - **Keyword:** `XL.DefaultDateFormat`
   - **Value:** `yyyy/MM/dd hh : mm : ss z`
6. Click **Save** to save the changes made.

   A message confirming that the system property has been modified is displayed.

2.5.5 Changing to the Required Input Locale

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

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.

2.5.6 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 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.*x*. 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 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.*x,* 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 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

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

   For Oracle Identity Manager release 11.1.*x*:

   ```
   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 9.0.1 through 9.0.3.*x* or 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.*x*:

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.

2.5.7 Enabling Logging

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

- Section 2.5.7.1, "Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.x or Release 9.1.0.x"
- Section 2.5.7.2, "Enabling Logging on Oracle Identity Manager Release 11.1.x"

2.5.7.1 Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.*x* or 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 and reconciliation 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.XELLERATE=log_level
     log4j.logger.XL_INTG.GROUPWISE=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.XL_INTG.GROUPWISE=INFO
     ```

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

  `WebLogic_home/user_projects/domains/domain_name/server_name/server_name.log`

- **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.XL_INTG.GROUPWISE=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.XL_INTG.GROUPWISE=INFO
     ```

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

  `WebSphere_home/AppServer/logs/server_name/startServer.log`

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, locate or add the following lines:

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>
     ```

```
<category name="XL_INTG.GROUPWISE">
   <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="XELLERATE">
      <priority value="INFO"/>
   </category>

   <category name="XL_INTG.GROUPWISE">
      <priority value="INFO"/>
   </category>
   ```

After you enable logging, the 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.XL_INTG.GROUPWISE=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.XL_INTG.GROUPWISE=INFO
     ```

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

  `OC4J_home/opmn/logs/default_group~home~default_group~1.log`

2.5.7.2 Enabling Logging on Oracle Identity Manager Release 11.1.x

> **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.*x* 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 2–2.

Table 2–2 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='groupwise-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="XL_INTG.GROUPWISE" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="groupwise-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 2–2 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='groupwise-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="XL_INTG.GROUPWISE" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="groupwise-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.

2.5.8 Configuring Oracle Identity Manager for 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.

> **Note:** Direct provisioning allows the provisioning of multiple target system accounts 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 2.5.8.1, "Copying Predefined Request Datasets"
- Section 2.5.8.2, "Importing Request Datasets into MDS"
- Section 2.5.8.3, "Enabling the Auto Save Form Feature"
- Section 2.5.8.4, "Running the PurgeCache Utility"

2.5.8.1 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 DataSets directory on the installation media:

- ProvisionResourceGroupwise User.xml
- ModifyResourceGroupwise User.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\GrpWise

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

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 on modifying request datasets.

2.5.8.2 Importing Request Datasets into MDS

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.

   > **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.5.8.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\GrpWise directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

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.

2.5.8.3 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 **Groupwise User** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.5.8.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.5.6, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.6 Installation and Configuration on the Target System

This section discusses the following topics:

- Section 2.6.1, "Installing the Remote Manager"
- Section 2.6.2, "Enabling Client-Side Authentication for the Remote Manager"
- Section 2.6.3, "Deploying the Remote Manager"
- Section 2.6.4, "Installing Novell GroupWise Client"

2.6.1 Installing the Remote Manager

The Remote Manager enables mailbox provisioning operations on Novell GroupWise.

> **Note:** In this guide, the directory in which you install the Remote Manager is referred to as *RM_HOME*.

The following are the prerequisites for installing the Remote Manager:

- For Oracle Identity Manager release 9.1.0.*x*

  If Novell GroupWise is running on 64-bit Microsoft Windows Server, then you must install the 64-bit version of JDK 1.5 or later before you install the Remote Manager.

- For Oracle Identity Manager release 11.1.*x*

  If Novell GroupWise is running on 64-bit Microsoft Windows Server, then before you install the Remote Manager, you must install Oracle WebLogic Application Server on the Remote Manager host computer. While installing the application server, do not select the JDK bundled with the application server. Instead, select an installed instance of a 64-bit version of JDK.

  > **Note:** During the mailbox provisioning operations on Novell GroupWise, the Remote Manager may throw the following type of error:
  >
  > ```
  > Get-ItemProperty: Cannot find path
  > ```
  >
  > To prevent such errors, you must ensure that the Remote Manager uses an installed instance of a 64-bit version of JDK.

2.6.2 Enabling Client-Side Authentication for the Remote Manager

To enable client-side authentication for the Remote Manager:

1. Open one of the following files in a text editor:
   - For Oracle Identity Manager release 9.1.0.*x:*

     RM_HOME/xlremote/config/xlconfig.xml
   - For Oracle Identity Manager release 11.1.*x:*

     OIM_HOME/remote_manager/config/xlconfig.xml
2. Set the ClientAuth property to true as follows:

   ```
   <ClientAuth>true</ClientAuth>
   ```
3. If you are using Oracle Identity Manager release 9.1.0.*x*, then ensure that the RMIOverSSL property is set to true as follows:

   ```
   <RMIOverSSL>true</RMIOverSSL>
   ```
4. Save and close the file.
5. If you are using Oracle Identity Manager release 9.1.0.*x*, then perform Steps 2 through 4 in the OIM_HOME/config/xlconfig.xml file.

2.6.3 Deploying the Remote Manager

The Remote Manager installation files are shipped along with the Oracle Identity Manager installation files. You can install the Remote Manager on any computer that is a part of the domain.

If you are using Oracle Identity Manager release 11.1.*x*, then see the Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager guide for instructions of installing the Remote Manager.

If you are using Oracle Identity Manager release 9.1.0.*x*, then depending on the application server that you use, perform the procedure to install the Remote Manager by following the instructions given in one of the following guides:

- Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server
- Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server
- Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server
- Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server

If you are using Oracle Identity Manager release 9.1.0.*x*, then copy the following JAR files into the *RM_HOME*\xlremote\JavaTasks directory:

- *OIM_HOME*/xellerate/lib/xlVO.jar
- *OIM_HOME*/xellerate/lib/xlScheduler.jar
- *OIM_HOME*/xellerate/lib/xlAPI.jar
- *INSTALL_MEDIA*/lib/tcGroupWise65.dll
- *INSTALL_MEDIA*/lib/xliGroupWiseRecon.jar
- *INSTALL_MEDIA*/lib/xliGroupWise65.jar

If you are using Oracle Identity Manager release 11.1.*x*, then copy the following JAR files into the *RM_HOME*\xlremote\JavaTasks directory:

- *OIM_HOME*/server/lib/xlVO.jar
- *OIM_HOME*/server/lib/xlScheduler.jar
- *OIM_HOME*/server/lib/xlAPI.jar
- *OIM_HOME*/server/lib/xlUtils.jar
- *OIM_HOME*/server/lib/xlRemoteManager.jar
- *OIM_HOME*/server/lib/xlLogger.jar

Note: In this guide, the connector installation media is referred to as *INSTALL_MEDIA*:

- *INSTALL_MEDIA*/lib/xliGroupWise65.jar
- *INSTALL_MEDIA*/lib/xliGroupWiseRecon.jar
- *INSTALL_MEDIA*/lib/tcGroupWise65.dll

Note: To enable logging in the Remote Manager, create a log directory and file inside the *RM_HOME* directory. For example:

RM_HOME/Log/Report.log

Specify the name of the Remote Manager as the value of the Remote Manager IT resource parameter. This parameter is described in Section 2.3.2.1, "Specifying Values for IT Resource Parameters."

See one of the following guides for information about modifying the value of an IT resource parameter:

- For Oracle Identity Manager release 9.1.0.*x:*

  Oracle Identity Manager Administrative and User Console Guide

- For Oracle Identity Manager release 11.1.*x:*

  Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

2.6.4 Installing Novell GroupWise Client

You must install the Novell GroupWise Client for provisioning to work as per the troubleshooting step "GW_FAILED_TO_CREATE_INSTANCE".

2.7 Configuring SSL

To set up SSL connectivity between Oracle Identity Manager and the Novell GroupWise server:

1. Import the certificate from the target system into the JSDK (the JSDK that is used during installation of Oracle Identity Manager) `cacerts` keystore as follows:

   ```
   keytool -import -alias alias_name -file
   certificate_file_name_with_complete_path -keystore
   JAVA_HOME/jre/lib/security/cacerts
   ```

Here, *JAVA_HOME* is the JDK directory used for Oracle Identity Manager.

2. Restart Oracle Identity Manager.
3. In the eDirectory IT Resource IT resource:
   - Set the SSL parameter value to `true.`
   - Set the Port parameter value to the SSL port number. Typically, this number is `636.`

3 Using the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

> **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, "Performing First-Time Reconciliation"
- Section 3.2, "Scheduled Task for Lookup Field Synchronization"
- Section 3.3, "Configuring Reconciliation"
- Section 3.4, "Configuring Scheduled Tasks"
- Section 3.5, "Performing Provisioning Operations"
- Section 3.6, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"

3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing user records:

> **Note:** In Oracle Identity Manager release 11.1.*x*, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.*x*.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

1. Perform lookup field synchronization by running the scheduled tasks provided for this operation.

See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about the attributes of the scheduled tasks for lookup field synchronization.

See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

2. Perform user reconciliation by running the scheduled task for user reconciliation.

   See Section 3.3.4, "User Reconciliation Scheduled Task" for information about the attributes of this scheduled task.

   See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

After first-time reconciliation, depending on the mode in which you configure the connector, the Last Recon TimeStamp parameter of the GroupWise IT Resource IT resource is automatically set to the time stamp at which the reconciliation run began.

> **See Also:** Section 2.3.2, "Configuring IT Resources" for information about the parameters of the IT resource

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the IT resource are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled task.

3.2 Scheduled Task for Lookup Field Synchronization

The following scheduled tasks are used for lookup fields reconciliation:

- Groupwise DistributionList Lookup Recon Task

  This scheduled task is used to synchronize the Distribution List lookup field in Oracle Identity Manager with distribution list-related data in the target system.

- Groupwise PostOffice List Lookup Recon Task

  This scheduled task is used to synchronize the Post Office List lookup field in Oracle Identity Manager with post office-related data in the target system.

Table 3–1 describes the attributes of both scheduled tasks. See Section 3.4, "Configuring Scheduled Tasks" for information about configuring scheduled tasks.

> **Note:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Table 3–1 Attributes of the Scheduled Tasks for Lookup Field Synchronization

Attribute	Description
LookupCodeName	This attribute holds the name of the lookup definition that contains mappings between the lookup fields of the target system and corresponding lookup definitions created in Oracle Identity Manager. The default value is one of the following: ■ For distribution list lookup synchronization: `Lookup.NGW.DistributionLists` ■ For post office list lookup sycnhronization: `Lookup.NGW.PostOffices`
ITResourceName	Enter the name of the Novell eDirectory IT resource. Default value: `eDirectory IT Resource`
SearchContext	Enter the Novell Groupwise search context to be used for fetching lookup field values from the target system. Default value: `O=glob`
ObjectClass	Enter the name of the object class. The default value is: ■ For distribution lists: `groupWiseDistributionList` ■ For post office list: `groupWisePostOffice`
ReconMode	Enter `Refresh` if you want to completely refresh the existing lookup. Existing values in the lookup definition are deleted and then new values are added. Enter `update` if you want to update the lookup definition with new values. Existing values in the lookup definition are left untouched. The default value of this attribute in the Groupwise DistributionList Lookup Recon Task scheduled task is `update`. The default value of this attribute in the Groupwise PostOffice List Lookup Recon Task scheduled task is `Refresh`.

3.3 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Section 3.3.1, "Full Reconciliation"
- Section 3.3.2, "Limited Reconciliation"
- Section 3.3.3, "Batched Reconciliation"
- Section 3.3.4, "User Reconciliation Scheduled Task"

3.3.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

To perform a full reconciliation run:

- Ensure that the Last Recon TimeStamp parameter of the GroupWise IT Resource IT resource does not contain a value.

- Specify `All Available` as the value of the NumberOfBatches attribute of the user reconciliation scheduled task.

At the end of the reconciliation run, the Last Recon TimeStamp parameter of the GroupWise IT Resource IT resource is automatically set to the time stamp at which the run started. From the next reconciliation run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

3.3.2 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

For this connector, you create a filter by specifying values for the CustomizedReconQuery parameter of the GroupWise IT Resource IT resource while performing the procedure described in one of the following sections:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x*:

  Section 2.4.2, "Importing the Connector XML File"

- For Oracle Identity Manager release 9.1.0.*x* or release 11.1.*x*:

  Section 2.3.2, "Configuring IT Resources"

The following table lists the Novell GroupWise attributes, and the corresponding Oracle Identity Manager attributes, that you can use to build the query condition. You specify this query condition as the value of the CustomizedReconQuery parameter.

Oracle Identity Manager Attribute	Novell GroupWise Attribute
User ID	cn
File ID	nGWFileID
Account ID	nGWAccountID
Gateway Access	nGWGatewayAccess

The following are sample query conditions:

- Value assigned to the CustomizedReconQuery parameter: `cn=JOHN|cn=JANE`

  The user with user ID `JOHN` and `JANE` are reconciled.

- Value assigned to the CustomizedReconQuery parameter: nGWFileID=f06|nGWFileID=s1z

  The users with File ID `f06` and `s1z` are reconciled.

If you do not specify values for the CustomizedReconQuery parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

The following are guidelines to be followed while specifying a value for the CustomizedReconQuery parameter:

- For the target system attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.

- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

  ```
  cn=John
  ```

  ```
  cn= John
  ```

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

> **Note:** An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

- The query condition must be an expression without any braces.
- Searching users based on more than three user attributes is not supported. For example, if the query condition is `cn=JOHN&nGWFileID=f06&nGWGatewayAccess=Sublm|nGWAccountID=23`, then the query generates an error.

3.3.3 Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete. You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- StartRecord: Use this attribute to specify the record number from which batched reconciliation must begin.
- BatchSize: Use this attribute to specify the number of records that must be included in each batch.
- NumberOfBatches: Use this attribute to specify the total number of batches that must be reconciled. If you do not want to use batched reconciliation, specify `All Available` as the value of this attribute.

> **Note:** If you specify `All Available` as the value of this attribute, then the values of the `StartRecord` and `BatchSize` attributes are ignored.

You specify values for these attributes by following the instructions described in Section 3.3.4, "User Reconciliation Scheduled Task."

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then refer to the log file for information about the batch at which reconciliation has failed. The log file provides the following information about batched reconciliation:

- Serial numbers of the batches that have been successfully reconciled
- User IDs associated with the records with each batch that has been successfully reconciled
- If the batched reconciliation run fails, then the serial number of the batch that has failed

3.3.4 User Reconciliation Scheduled Task

When you run the Connector Installer or import the connector XML file, the Groupwise User Recon Task reconciliation scheduled task is automatically created in Oracle Identity Manager. This scheduled task is used to reconcile user data from the target system.

You must specify values for the following attributes of the Groupwise User Recon Task scheduled task. Table 3–2 describes the attributes of this scheduled task.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Table 3–2 Attributes of the User Reconciliation Scheduled Task

Attribute	Description
ITResourceName	Enter the name of the IT resource for the Novell GroupWise installation from which you want to reconcile user records. Default value: `GroupWise IT Resource`
eDirITResourceName	Enter the name of the Novell eDirectory IT resource. Default value: `eDirectory IT Resource`
RemoteResourceName	Enter the name of the IT resource in which the remote service name and URL are specified. Default value: `GroupWise XRM`
ResourceObjectName	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `Groupwise User`
XLDeleteUsersAllowed	If this attribute is set to `true,` then the Delete reconciliation event is started. Users who are deleted from the target system are removed from Oracle Identity Manager. This requires all the users on the target system to be compared with all the users in Oracle Identity Manager. If this attribute is set to `false`, then the users are not deleted. Default value: `true` **Note:** This process affects performance.

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Task

Attribute	Description
TrustedSource	Enter `true` if you want to configure the connector for trusted source reconciliation. Enter `false` if you want to configure the connector for target resource reconciliation. Default value: `true`
Xellerate Type	Enter the role that must be set for OIM Users created through reconciliation. You can enter one of the following values: ■ `End-User` ■ `End-User Administrator` Default value: `End-User Administrator`
Organization	Enter the name of the Oracle Identity Manager organization in which reconciled users must be created. Default value: `Xellerate Users`
Role	Enter the employee type that must be set for OIM Users created through reconciliation. You can enter one of the following values: ■ `Full-Time Employee` ■ `Part-Time Employee` ■ `Temp` ■ `Intern` ■ `Consultant` Default value: `Consultant`
StartRecord	Enter the number of the target system record from which a batched reconciliation run must begin. Default value: `1` This attribute is used in conjunction with the BatchSize and NumberOfBatches attributes. All three attributes are discussed in Section 3.3.3, "Batched Reconciliation."
BatchSize	Enter the number of records that must be included in each batch fetched from the target system. Default value: `3` This attribute is used in conjunction with the NumberOfBatches and StartRecord attributes. All three attributes are discussed in Section 3.3.3, "Batched Reconciliation."
NumberOfBatches	Enter the number of batches that must be reconciled. Default value: `All Available` Sample value: `50` This attribute is used in conjunction with the BatchSize and StartRecord attributes. All three attributes are discussed in detail in Section 3.3.3, "Batched Reconciliation." If you accept the default value (`All Available`), then batched reconciliation is not performed.

3.4 Configuring Scheduled Tasks

You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–3 lists the scheduled tasks that form part of the connector.

Table 3–3 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
Groupwise DistributionList Lookup Recon Task	This scheduled task is used to synchronize the values of distribution list lookup fields between Oracle Identity Manager and the target system. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task.
Groupwise PostOffice List Lookup Recon Task	This scheduled task is used to synchronize the values of post office list lookup fields between Oracle Identity Manager and the target system. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task.
Groupwise User Recon Task	This scheduled task is used for user reconciliation. See Section 3.3.4, "User Reconciliation Scheduled Task" for information about this scheduled task.

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

- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.x"
- Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.x"

3.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*

To configure a scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler**.
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option. If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task.
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.

Stopping Reconciliation

Suppose the user reconciliation scheduled task for the connector is running and user records are being reconciled. If you want to stop the reconciliation process:

1. Perform Steps 1 through 4 of the procedure to configure reconciliation scheduled tasks.
2. Select the **Stop Execution** check box in the task scheduler.
3. Click **Save**.

3.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.x

To configure a scheduled task:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.*x* or 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   - For Oracle Identity Manager release 11.1.2:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click **Scheduler.**
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.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   - 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. Click the **System Management** tab, and then click **Scheduler.**
     c. On the left pane, click **Advanced Search**.
3. On the page that is displayed, you can use any combination of the search options provided to locate a scheduled task. Click **Search** after you specify the search criteria.

   The list of scheduled tasks that match your search criteria is displayed in the search results table.
4. 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*, then in the search results table, click the Edit icon in the Edit column for the scheduled task.
   - If you are using Oracle Identity Manager release 11.1.*x*, then select the link for the scheduled task from the list of scheduled tasks displayed in the search results table.
5. Modify the details of the scheduled task. To do so:

a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

   - **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
   - **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.
   - **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
   - **Frequency:** Specify the frequency at which you want the task to run.

b. If you are using Oracle Identity Manager release 11.1.*x*, then on the Job Details tab, you can modify the following parameters:

   - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

> **Note:** See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

6. Specify values for the attributes of the scheduled task. To do so:

> **Note:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - Attributes of the scheduled task are discussed in Section 3.3.4, "User Reconciliation Scheduled Task."

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
   - If you are using Oracle Identity Manager release 11.1.*x,* then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

7. After specifying the attributes, perform one of the following:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

Note: The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

- If you are using Oracle Identity Manager release 11.1.*x*, then click **Apply** to save the changes.

Note: The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.5 Performing Provisioning Operations

See Also: Section 3.6, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

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 3.5.3, "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
- Provisioning triggered by policy changes

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

This section discusses the following topics:

- Section 3.5.1, "Direct Provisioning"
- Section 3.5.2, "Request-Based Provisioning"
- Section 3.5.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"

3.5.1 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 8.5.3.1 through 9.0.3.*x* or 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 8.5.3.1 through 9.0.3.*x* or release 9.1.0.*x*, then:

     a. From the Users menu, select **Manage**.

     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.

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

     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.

     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - If you are using Oracle Identity Manager release 8.5.3.1 through 9.0.3.*x* or release 9.1.0.*x*, then:

     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.

     b. On the Resource Profile page, click **Provision New Resource**.

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

     a. On the user details page, click the **Resources** tab.

     b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **Groupwise User** from the list and then click **Continue**.

6. On the Step 2: Verify Resource Selection page, click **Continue**.

7. On the Step 5: Provide Process Data for GroupWise User page, enter the details of the account that you want to create on the target system and then click **Continue**.

8. On the Step 5: Provide Process Data for User Nicknames page, if required, enter details of the nicknames and then click **Continue**.

9. On the Step 5: Provide Process Data for User Distribution Lists page, if required, enter details of the distribution list, and then click **Continue.**
10. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
11. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
    - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
    - If you are using Oracle Identity Manager release 11.1.1, then:
        a. Close the window displaying the "Provisioning has been initiated" message.
        b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.2 Request-Based Provisioning

> **Note:** The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The 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 3.5.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.5.2.2, "Approver's Role in Request-Based Provisioning"

3.5.2.1 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 **iPlanet User**, 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.

3.5.2.2 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.

3.5.3 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 2.5.8, "Configuring Oracle Identity Manager for 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 **Groupwise User** 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 **Groupwise User** 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 back 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 **Groupwise User** 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 **Groupwise User** resource object.
   c. Select the **Self Request Allowed** check box.
   d. Click the Save icon.

3.6 Configuring Provisioning in Oracle Identity Manager Release 11.1.2

To configure provisioning operations in Oracle Identity Manager release 11.1.2:

> **Note:** The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See the "Managing Users" chapter in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance, and then click **Checkout.**
5. Specify values for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If you want to provision a resource to an existing OIM User, then:
    1. On the Users page, search for the required user.
    2. On the user details page, click **Accounts.**
    3. Click the **Request Accounts** button.
    4. Search for the Novell GroupWise application instance in the catalog search box and select it.
    5. Click **Add to Cart.**
    6. Click **Checkout.**
    7. Specify values for fields in the application form and then click **Ready to Submit.**
    8. Click **Submit.**

4

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Section 4.1, "Running Test Cases"
- Section 4.2, "Troubleshooting"

4.1 Running Test Cases

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the testing utility:

1. Specify the required values in the config.properties file. This file is located in one of the following directories:

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

     OIM_HOME/xellerate/groupwise/test/troubleshoot

   - For Oracle Identity Manager release 11.1.*x*:

     OIM_HOME/server/groupwise/test/troubleshoot

   The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Novell eDirectory Connection Parameters	Connection parameters required to connect to the Novell eDirectory system See Section 2.3.2, "Configuring IT Resources" for information about the values that you must provide.
Novell GroupWise Connection Parameters	Connection parameters required to connect to the Novell GroupWise system See Section 2.3.2, "Configuring IT Resources" for information about the values that you must provide.
Create Mailbox Parameters	Values required to create a mailbox
Modify Mailbox Parameters	Values required to modify a mailbox
Delete Mailbox Parameters	Values required to delete a mailbox

2. Use a text editor to open each of the BAT files in one of the following directories:

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

OIM_HOME/xellerate/groupwise/test/troubleshoot

- For Oracle Identity Manager release 11.1.*x*:

  OIM_HOME/server/groupwise/test/troubleshoot

The names of the JAR files that must be added to the `CLASSPATH` environment variable are given in these BAT files. Copy these JAR files into the same directory as the BAT files and then add them to the CLASSPATH environment variable.

3. Run the appropriate BAT file to test the creation, modification, and deletion of users in Novell GroupWise:

   - Create a user by running the testcreate.bat file.

     After you run the BAT file, check if the user is created in Novell GroupWise according to the details given in the config.properties file. If you run this BAT file from a command window, then the `User_Creation_Successful` message is displayed.

   - Modify the user by running the testmodify.bat file.

     After you run the BAT file, check if the user is modified in Novell GroupWise according to the details given in the config.properties file. If you run this BAT file from a command window, then the `User_Modification_Successful` message is displayed.

   - Delete the user by running the testdelete.bat file.

     After you run the BAT file, check if the user is deleted from Novell GroupWise. If you run this BAT file from a command window, then the `User_Deletion_Successful` message is displayed.

When you run testing utility, the debugGW.log file is created in the *OIM_HOME*/xellerate/groupwise/test/troubleshoot directory.

4.1.1 Testing Limited Reconciliation

To test query-based reconciliation, you can specify the following types of query conditions as values for the `CustomizedReconQuery` parameter:

- Queries with user attributes
  - Value assigned to the `CustomizedReconQuery` parameter: `cn=JOHN|cn=JANE`

    The user with user ID `JOHN` and `JANE` are reconciled.

  - Value assigned to the `CustomizedReconQuery` parameter: nGWFileID=f06|nGWFileID=s1z

    The users with File ID `f06` and `s1z` are reconciled.

  - Value assigned to the CustomizedReconQuery parameter: `nGWFileID=f06&nGWAccountID=s1z`

    The users with File ID f06 and Account ID s1z are reconciled.

  - Value assigned to the CustomizedReconQuery parameter: `nGWGatewayAccess=jkl12`

    The users with the Gateway Access value `jkl12` are reconciled.

4.1.2 Testing Batch-Based Reconciliation

You can test reconciliation based on batching and data paging of user records by specifying values for the following user reconciliation scheduled task attributes:

- If you set the value of `StartRecord` to `1`, `BatchSize` to `0`, and `NumberOfBatches` to `All Available`, then all the users are reconciled.
- If you set the value of `StartRecord` to `1`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then all the users starting from record 1 are reconciled in 50 batches, with 5 records in each batch.
- If you set the value of `StartRecord` to `200`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then all the users starting from record 200 are reconciled in 50 batches, with 5 records in each batch.

The results of batching are displayed in the logger file, which is located in the following path:

```
JBOSS_HOME/server/default/log/server.log
```

In this file, you can view the batch numbers, the user ids of the users that are reconciled, and whether the reconciliation is successful or not.

4.2 Troubleshooting

This section provides solutions to the following commonly encountered errors associated with the connector:

- Section 4.2.1, "Remote Method Invocation Errors"
- Section 4.2.2, "Novell GroupWise Connector Errors"

4.2.1 Remote Method Invocation Errors

The following are steps to resolve remote method invocation errors:

- Verify that the URL has been correctly specified in the `GroupWise XRM` IT resource definition.
- In the remote manager form, ensure that the **Running** check box is selected for the `GroupWise XRM` IT resource. If it is not selected, then the remote manager may not be running.

4.2.2 Novell GroupWise Connector Errors

Errors discussed in this section are divided on the basis of response codes:

- Section 4.2.2.1, "Common Response Codes for All Use Cases"
- Section 4.2.2.2, "Use Case-Specific Response Codes"

4.2.2.1 Common Response Codes for All Use Cases

The errors discussed in the following table correspond to common response codes for all use cases.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with Novell eDirectory. **Returned Error Message:** Unable to communicate with the eDirectory server **Returned Error Code:** `GW_EDIR_COMMUNICATION_ERROR`	■ Ensure that the Novell eDirectory server is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the IP address, admin ID, and admin password are correct. ■ Check if the `SSL` IT resource parameter is set to `false`. It must be set to `true` if the Novell eDirectory server is accepting only SSL connections. ■ Check if the specified eDirectory connection values (in the Novell eDirectory IT resource) are correct.
Target not available. **Returned Error Message:** eDirectory server may not be available **Returned Error Code:** `GW_EDIR_TARGET_UNAVAILABLE_ERROR`	■ Check if Novell eDirectory is running. ■ Check if the Novell eDirectory connection values specified in the eDirectory IT resource definition are correct. ■ Check if the server IP address in the Novell eDirectory/GroupWise connection information is correct.
Authentication error **Returned Error Message:** Unable to authenticate to the eDirectory server **Returned Error Code:** `GW_EDIR_AUTHENTICATION_ERROR`	■ Check if the Novell eDirectory connection values, especially the admin credentials, specified in the IT resource definition are correct. ■ Check if the `SSL` IT resource parameter is set to `false`. It must be set to `true` if SSL has been enabled on the Novell eDirectory server.
Naming error **Returned Error Message:** Naming exception encountered while trying to connect to the eDirectory server **Returned Error Code:** `GW_EDIR_INVALID_NAMING_ERROR`	Check if the Novell eDirectory connection values specified in the IT resource definition are correct.
Oracle Identity Manager cannot establish a connection to Novell Directory Services (NDS). **Returned Error Message:** NDS connection failed **Returned Error Code:** `GW_NDS_CONNECTION_FAILED`	■ Ensure that Novell eDirectory is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the IP address, admin ID, and admin password are correct. ■ Check if the Novell GroupWise connection values specified in the IT resource definition are correct. ■ Check if some other user is connected to the NDS server through Novell Client. If yes, then close that connection.
Oracle Identity Manager cannot establish a connection to Novell Directory Services (NDS). **Returned Error Message:** Invalid credentials **Returned Error Code:** `GW_NDS_INVALID_CREDENTIALS`	■ Check if the Novell GroupWise connection values, especially the admin credentials, specified in the IT resource definition are correct. ■ Check if some other user is connected to the NDS server through Novell Client. If yes, then close that connection.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to Novell GroupWise. **Returned Error Message:** Could not create instance of GroupWise class **Returned Error Code:** `GW_FAILED_TO_CREATE_INSTANCE`	■ Check if Novell Client has been installed on the computer on which the remote manager is installed. ■ Check if the Novell GroupWise client has been installed on the computer on which the remote manager is installed.
Oracle Identity Manager cannot establish a connection to Novell Directory Services (NDS) or Novell GroupWise. **Returned Error Message:** Invalid eDirectory Tree **Returned Error Code:** `GW_INVALID_TREE`	Check if the Novell GroupWise connection values, especially the eDirectory tree, specified in the IT resource definition are correct.
Oracle Identity Manager cannot establish a connection to Novell GroupWise. **Returned Error Message:** Invalid domain DN or path **Returned Error Code:** `GW_INVALID_DOMAIN_DN_OR_PATH`	■ Check if the Novell GroupWise connection values specified in the IT resource definition, especially the GroupWise domain DN or path, are correct. ■ Check if the connection values have been specified in the format given in this document. ■ Check if the Novell GroupWise domain database is corrupted.
JNI out of memory **Returned Error Message:** JNI out of memory error encountered **Returned Error Code:** `GW_JNI_OUT_OF_MEMORY_ERROR`	JNI has run out of memory. Increase JVM memory on the server on which the remote manager is installed.
Internal error has occurred **Returned Error Message:** Internal error encountered in Groupwise **Returned Error Code:** `GW_INTERNAL_ERROR`	Review the log file to determine the exact error.
Invalid argument **Returned Error Message:** Invalid arguments passed to method **Returned Error Code:** `GW_INVALID_ARGUMENTS`	Check if the Novell GroupWise connection values specified in the IT resource definition are correct.

Problem Description	Solution
Required information missing **Returned Error Message:** Empty or null arguments were passed for mandatory fields or for connection information **Returned Error Code:** `GW_INSUFFICIENT_INFO_PROVIDED`	■ Ensure that the IP address, admin ID, and admin password are correct. ■ Ensure that the following connection information has been provided IT resource definition: **Information about the Novell eDirectory connection:** - Novell eDirectory server name - Novell eDirectory port number - Novell eDirectory root context - Admin user DN - Admin user password - Whether or not SSL is to be used **Information about the Novell GroupWise connection:** - Novell eDirectory tree - Novell eDirectory context - Novell admin user DN - Novell admin password - Novell GroupWise domain DN or path The required information also includes other process data, such as the user ID.
User not present **Returned Error Message:** User does not exist **Returned Error Code:** `GW_USER_DOES_NOT_EXIST`	The specified user ID does not exist in Novell eDirectory.
Mailbox not present **Returned Error Message:** Mailbox does not exist **Returned Error Code:** `GW_MAILBOX_DOES_NOT_EXIST`	The specified mailbox does not exist in Novell GroupWise.
Mailbox already present **Returned Error Message:** Mailbox already exists for the specified user **Returned Error Code:** `GW_MAILBOX_ALREADY_EXISTS`	The specified mailbox already exists in Novell GroupWise.
Post office not present **Returned Error Message:** PostOffice does not exist **Returned Error Code:** `GW_POSTOFFICE_DOES_NOT_EXIST`	The specified post office does not exist in Novell GroupWise.

Problem Description	Solution
Distribution list not present **Returned Error Message:** Distribution list does not exist **Returned Error Code:** `GW_DISTLIST_DOES_NOT_EXIST`	The specified distribution list does not exist in Novell GroupWise.
Nickname not present **Returned Error Message:** Nickname does not exist **Returned Error Code:** `GW_NICKNAME_DOES_NOT_EXIST`	The specified nickname does not exist in Novell GroupWise.

4.2.2.2 Use Case-Specific Response Codes

The errors discussed in the following table correspond to response codes that are specific to use cases. For all the errors listed in the table, you must review the log file to determine the exact error.

Problem Description	Solutions
Oracle Identity Manager cannot create a user or mailbox in Novell GroupWise. **Returned Error Message:** Could not create mailbox **Returned Error Code:** `GW_MAILBOX_CREATE_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot delete a user or mailbox in Novell GroupWise. **Returned Error Message:** Could not delete mailbox **Returned Error Code:** `GW_MAILBOX_DELETE_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot disable a user or mailbox in Novell GroupWise. **Returned Error Message:** Mailbox could not be disabled **Returned Error Code:** `GW_MAILBOX_DISABLE_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot add a nickname to the user. **Returned Error Message:** Nickname add failed **Returned Error Code:** `GW_NICKNAME_ADD_FAILED`	A nickname already exists for the specified user. Review the log file to determine the exact error.

Problem Description	Solutions
Oracle Identity Manager cannot remove the nickname of a user. **Returned Error Message:** Nickname remove failed **Returned Error Code:** `GW_NICKNAME_REMOVE_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot add a user to a distribution list. **Returned Error Message:** Could not add user to distribution list **Returned Error Code:** `GW_DISTLIST_USERADD_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot remove a user from a distribution list. **Returned Error Message:** Could not remove user from distribution list **Returned Error Code:** `GW_DISTLIST_USERREMOVE_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot reset the password of a user. **Returned Error Message:** Password reset failed **Returned Error Code:** `GW_PASSWORD_RESET_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot move a user to the specified post office. **Returned Error Message:** Could not move mailbox **Returned Error Code:** `GW_POSTOFFICE_MOVEUSER_FAILED`	Review the log file to determine the exact error.
Oracle Identity Manager cannot modify an attribute of a user. **Returned Error Message:** Could not modify mailbox **Returned Error Code:** `GW_USER_ATTRIBUTE_SET_FAILED`	The specified attribute name may be invalid. Review the log file to determine the exact error.

5 Known Issues

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

- **Bug 7656117**

  The following issue is observed if you are using version 6.5 of Novell GroupWise as the target system:

  While performing the Add User To Distribution List provisioning operation, Remote Manager stops functioning if the length of the distinguished name of the distribution list is more than 97 characters.

  If the length of the Distribution List DN process form field is more than 64 characters, then you cannot create the distribution list.

  To overcome this issue, use version 7.0 of Novell GroupWise with SP3 as the target system.

- **Bug 8547806**

  During the Add User To Distribution List provisioning operation, the `Add User to Distribution List` task is completed successfully. If you perform the Add User To Distribution List provisioning operation again for the same target system user, then the status of the `Add User To Distribution List` task is rejected. However, the child form displays the name of the distribution list twice.

  Now, if you perform the Remove User From Distribution List provisioning operation, then the target system user is successfully removed from the distribution list. However, the child form still displays the name of the distribution list. If you perform the Remove User From Distribution List provisioning operation again, then (although the user was successfully removed from the distribution list) the `Remove User from Distribution List` task is completed successfully.

  This issue is because of a GroupWise API. The same issue has been mentioned in the administrative Web site of Novell:

  `http://developer.novell.com/wiki/index.php/GroupWise_Administrative_Object_API_Defect_Fixes`

- **Bug 8575556**

  If the distribution list or nickname list is empty, then reconciliation is performed with the `[None]` string value as the Distribution List and Nick Name List values in Oracle Identity Manager.

The following is a limitation of the target system:

Versions 6.5 and 7 of Novell GroupWise do not support the entry of non-ASCII characters. Therefore, you cannot transfer non-ASCII data through the connector.

However, error messages and response codes would be displayed in Oracle Identity Manager in the language corresponding to the language that you select.

Index