Oracle® Identity Manager

Connector Guide for Microsoft Exchange

Release 9.1.1

E11198-06

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for Microsoft Exchange, Release 9.1.1

E11198-06

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

3 Using the Connector

4 Extending the Functionality of the Connector

List of Figures

List of Tables

Preface

This guide discusses the connector that is used to integrate Oracle Identity Manager with Microsoft Exchange.

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For generic information about connectors, see *Oracle Identity Manager Connector Concepts* in the Oracle Identity Manager Connectors documentation library.

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network. The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

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

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

This chapter provides an overview of the updates made to the software and documentation of the Microsoft Exchange connector in release 9.1.1.

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  These include major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

The following sections discuss software updates:

- Software Updates in Release 9.1.0
- Software Updates in Release 9.1.0.1
- Software Updates in Release 9.1.1

Software Updates in Release 9.1.0

The following are issues resolved in release 9.1.0:

- Support for Microsoft Exchange 2007
- Introduction of the Connector Installer
- Support for Specifying the Exchange Server and Mail Store for Provisioning Operations
- Support for Reconciliation of Mailbox Data from Specific Mail Store and Distribution Group
- Support for the Application of Native LDAP Queries During Reconciliation
- Support for Full and Incremental Reconciliation
- Introduction of Scheduled Task for Reconciliation of Deleted Mailboxes

Support for Microsoft Exchange 2007

The connector can be used to integrate Microsoft Exchange 2000, 2003, or 2007 with Oracle Identity Manager. In addition, the connector also supports mixed mode operation in which a single connector is used to integrate more than one version of the target system with Oracle Identity Manager.

Information specific to the Microsoft Exchange 2007 has been provided at various places in this guide.

Introduction of the Connector Installer

You can now install the connector by using the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

See "Running the Connector Installer" on page 2-4 for more information.

Support for Specifying the Exchange Server and Mail Store for Provisioning Operations

The MailStore Name field has been added to the process form for provisioning operations. You can use this field to specify the Exchange server and mail store in which provisioning operations must be performed.

Support for Reconciliation of Mailbox Data from Specific Mail Store and Distribution Group

By using the Mail Store Name and Distribution Group Name attributes of the Exchange Reconciliation Task scheduled task, you can specify the mail store or distribution group from which mailbox data must be reconciled.

See "Types of Reconciliation Enabled by the Connector" on page 1-6 for more information.

Support for the Application of Native LDAP Queries During Reconciliation

In the earlier release, you specify the query condition for limited reconciliation by using operators that are not native to the target system. You can now specify the query condition using either non-native or native operators.

See "Limited Reconciliation vs. Regular Reconciliation" on page 3-5 for more information.

Support for Full and Incremental Reconciliation

You can use the MEXC Timestamp attribute of the reconciliation scheduled task to specify whether you want to configure full reconciliation or incremental reconciliation.

See "Full Reconciliation vs. Incremental Reconciliation" on page 3-6 for more information.

Introduction of Scheduled Task for Reconciliation of Deleted Mailboxes

The connector can be configured to reconcile deleted mailbox data. The Exchange Delete Recon Task scheduled task has been introduced to automate this process.

See "Exchange Delete Recon Task" on page 3-9 for more information about this scheduled task.

Software Updates in Release 9.1.0.1

There are no software updates in release 9.1.0.1.

Software Updates in Release 9.1.1

The following are issues resolved in release 9.1.1:

Microsoft Windows Server 2008 Added to the List of Certified Target System Host Platforms

From this release onward, Microsoft Windows Server 2008 has been added to the list of certified target system host platforms. This has been mentioned in the "Certified Deployment Configurations" section.

Change in the Oracle Identity Manager Requirement

From this release onward, Oracle Identity Manager release 9.1.0.1 is the minimum supported Oracle Identity Manager release. This is mentioned in the "Certified Deployment Configurations" section.

Support for Creating Copies of the Connector

The Parameters.Exchange lookup definition has been renamed to "Lookup.Exchange.Configuration." In addition, new entries that hold the names of process form fields used for matching user records have been added in this lookup definition. If you create a copy of the process form, then you can specify details of the new process form in the copy of the Lookup.Exchange.Configuration lookup definition. This feature enables you to create multiple copies of the connector without making code-level changes.

See the following sections for more information:

- Configuring the Lookup.Exchange.Configuration Lookup Definition
- Creating Copies of the Connector

Introduction of the Lookup.Exchange.Constants Lookup Definition

The Lookup.Exchange.Constants lookup definition stores the constants and variables defined in the Java classes that constitute the connector.

Caution: You must not change any entry in the Lookup.Exchange.Constants lookup definition. If you change any entry, then the connector will not function correctly.

The name of this lookup definition is specified as the value of the Exchange Constants Lookup Code Key in the Lookup.Exchange.Configuration lookup definition.

No Support for Native Queries

You use the Query attribute of the user reconciliation scheduled tasks to specify the query condition that must be applied during reconciliation. In earlier releases, you used the Use Native Query attribute to specify that the query condition was in native

LDAP format. From this release onward, you can use only native LDAP queries. The Use Native Query attribute has been removed from the scheduled tasks.

Issues Resolved in Release 9.1.1

The following are issues resolved in release 9.1.1:

Bug Number	Issue	Resolution
7157839, 7676069, and 7507908	If the target system was Microsoft Exchange 2007, then the connector did not respond correctly to the RMTimeOut setting in the Lookup.Exchange.Configuration lookup definition.	This issue has been resolved. The RMTimeOut attribute of the Lookup.Exchange.Configuration lookup definition has been removed. This feature is now handled internally by the connector.
7157996	When you enabled a mailbox, you were not required to set an incoming or outgoing message size. This is not the same as the behavior on the target system.	This issue has been resolved. The DefaultInComingMsgSize and DefaultOutGoingMsgSize parameters have been added in the Lookup.Exchange.Configuration lookup definition. See "Configuring the Lookup.Exchange.Configuration Lookup Definition" for more information.
8276367	Earlier the mail store name was extracted from the mail store DN and displayed in the lookup field on the Administrative and User Console.	This issue has been resolved. From this release onward, the full mail store DN is displayed in the lookup field.
7577059	An exception is encountered on running a scheduled task for which an attribute's value is not specified. In earlier releases, the message displayed did not provide sufficient details to identify the cause of the exception.	This issue has been resolved. The stack trace is displayed on the Java console and is also recorded in the log file.
7145460	Suppose an OIM User was provisioned a Microsoft Active Directory resource and a Microsoft Exchange mailbox. After the next target resource reconciliation run, suppose the user was deleted on the target system and the scheduled task for reconciliation of deleted users was then run. At this point, the Microsoft Active Directory resource was revoked but the mailbox was not revoked.	This issue has been resolved. The mailbox is revoked along with the Microsoft Active Directory resource.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

Documentation-Specific Updates in Release 9.1.0

Major changes have been made in 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 information provided by the guide.

See "Roadmap for Deploying and Using the Connector" on page 1-15 for detailed information about the organization of content in this guide.

Documentation-Specific Updates in Release 9.1.0.1

Information specific to installing the Remote Manager for Microsoft Exchange 2007 has been added in the following sections:

- "Creating the IT Resource" on page 2-6
- "Installing the Remote Manager" on page 2-10
- "Guidelines on Configuring Reconciliation Runs" on page 3-1
- "Guidelines on Performing Provisioning Operations" on page 3-2

Documentation-Specific Updates in Release 9.1.1

The following is a documentation-specific update in release 9.1.1:

- In the "Mailbox Provisioning Functions Supported by the Connector" section, the following functions have been added:

  Disable Mail box

  Enable Mail box

- In the "Mailbox Fields for Target Resource Reconciliation" section, the following fields have been added to the list of target system fields that are reconciled:
  - userPrincipalName
  - homeMDB
  - mDBUseDefaults
- In the "Known Issues" chapter, a description for Bug 7207232 has been added.
- Microsoft Windows 2000 is no longer a supported host for the target system. All occurrences of "Microsoft Windows 2000" have been removed from this guide.
- Information about JDK requirement for installing Remote Manager has been added in the following sections:
  - "Certified Deployment Configurations" on page 1-1
  - "Installing the Remote Manager" on page 2-10
- In the "Certified Deployment Configurations" section, changes have been made in the "Target Systems" row.

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 external, identity-aware applications. This guide discusses the connector that enables you to use Microsoft Exchange as a managed (target) resource of Oracle Identity Manager.

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

In the account management mode of the connector, information about mailboxes created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform mailbox provisioning operations on the target system.

This chapter contains the following sections:

1.1 Certified Deployment Configurations

Table 1–1 lists the certified deployment configurations.

Table 1–1 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0.1 or later
Target systems	The target system can be any one or a combination of the following: ■ Microsoft Exchange 2003 ■ Microsoft Exchange 2007
Target system host platforms	The target system host platform can be any one of the following: ■ Microsoft Windows Server 2003 ■ Microsoft Windows Server 2008

Table 1–1 (Cont.) Certified Deployment Configurations

Item	Requirement
JDK	If you are installing Remote Manager for Microsoft Exchange 2007 that is running on 64-bit Microsoft Windows Server, then you must install the 64-bit version of JDK 1.4.2_15 or JDK 1.5.
Other systems	Microsoft Active Directory Microsoft Active Directory User Management connector You must deploy the Microsoft Active Directory User Management connector before you can deploy and use the Microsoft Exchange connector. In addition, you must ensure that SSL is configured for the Microsoft Active Directory User Management connector. See *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for instructions to deploy the Microsoft Active Directory connector.

1.2 Certified Languages

The connector supports the following languages:

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

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

1.3 Features of the Connector

This section discusses the following topics:

- The "Connector Architecture" on page 1-3 describes the architecture of the connector.
- The following sections describe the features of the managed resource mode of the connector:
  - Lookup Field Synchronization
  - Target Resource Reconciliation
  - Provisioning

1.3.1 Connector Architecture

This section discusses the following topics:

- Architecture of the Connector for Microsoft Exchange 2000 and Microsoft Exchange 2003
- Architecture of the Connector for Microsoft Exchange 2007

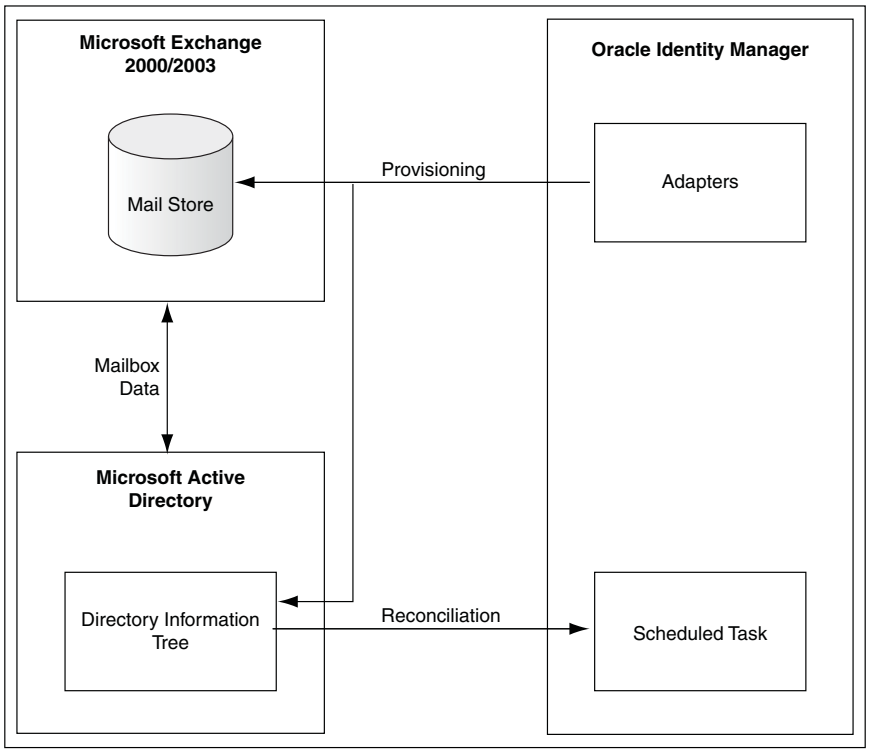
Note: The connector requires the deployment of a Microsoft Active Directory User Management connector. The user account data is stored in Microsoft Active Directory. Before you can provision a Microsoft Exchange mailbox for a user, you must create an account for the user in Microsoft Active Directory. The Microsoft Exchange connector uses the data in Microsoft Active Directory during the mailbox provisioning operation. This means that the connector can be configured only in the account management mode, which involves target resource reconciliation and provisioning with Microsoft Exchange.

1.3.1.1 Architecture of the Connector for Microsoft Exchange 2000 and Microsoft Exchange 2003

Microsoft Exchange uses Microsoft Active Directory as a user repository to store information about a user's mailbox, mail stores, and storage groups.

Figure 1–1 shows the architecture of the connector for Microsoft Exchange 2000 and Microsoft Exchange 2003.

Figure 1–1 Architecture of the Connector for Microsoft Exchange 2000 and Microsoft Exchange 2003



During a provisioning operation, the adapters create a mailbox for a user by setting the Exchange-specific attributes in the user's Active Directory profile. This information is used by the Recipient Update Service (RUS), a component in the Exchange 2000 and Exchange 2003, to generate the SMTP and other e-mail addresses required to allow users to log in to their mailboxes. For more information about the RUS, visit the Microsoft Help and Support Web site at

http://support.microsoft.com

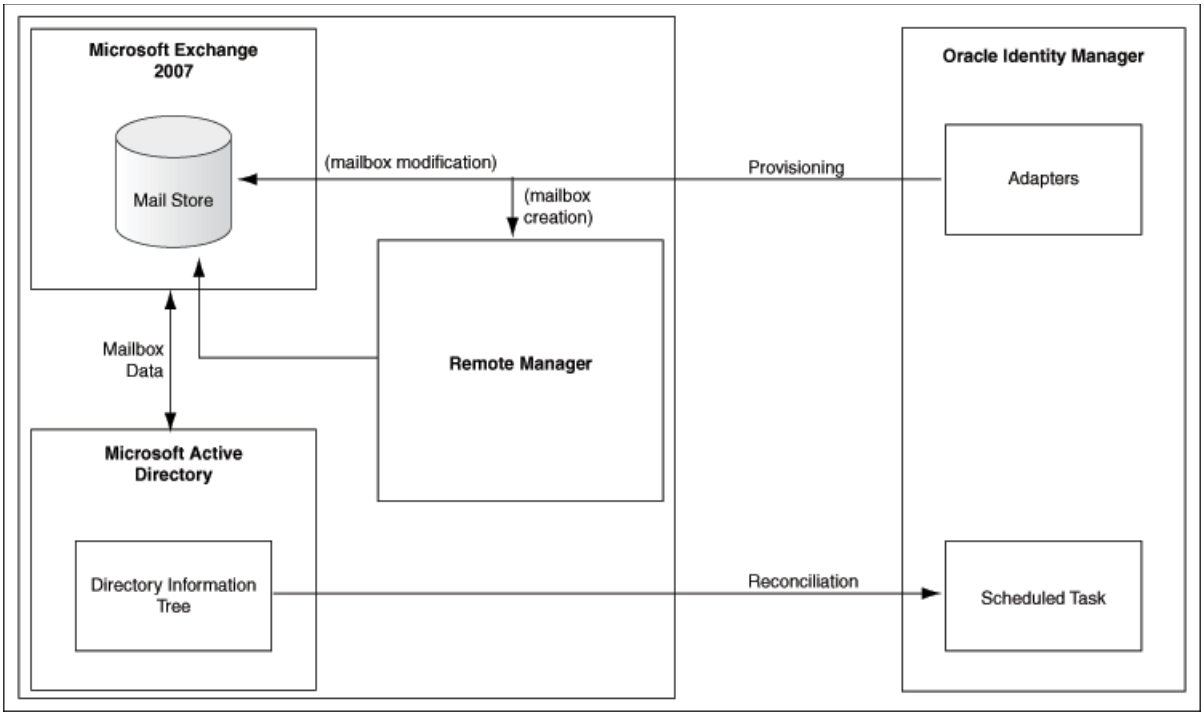
During reconciliation, scheduled tasks fetch user mailbox and mail store data from the target system into Oracle Identity Manager.

1.3.1.2 Architecture of the Connector for Microsoft Exchange 2007

Microsoft Exchange 2007 uses Microsoft Active Directory to store information about user mailboxes, mail stores, and Microsoft Exchange servers. Unlike Microsoft Exchange 2000 and 2003, Microsoft Exchange 2007 does not contain the RUS. Microsoft Exchange 2007 uses the Exchange Management Shell to carry out Exchange administration activities including mailbox management.

Figure 1–2 shows the architecture of the connector for Microsoft Exchange 2007.

Figure 1–2 Architecture of the Connector for Microsoft Exchange 2007



Microsoft Exchange 2007 requires the Exchange Management Shell (based on Windows Power Shell) to create mailboxes. Oracle Identity Manager uses a Remote Manager to communicate with the Exchange Management Shell. During provisioning operations, the adapters execute a Power Shell script through the Remote Manager to create or modify mailboxes.

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

See Also: For more information about Remote Managers, refer to:

- The "Remote Manager Form" section in the *Oracle Identity Manager Design Console Guide*
- The "Back-End System Integration Tier" section in *Oracle Identity Manager Concepts*

1.3.2 Lookup Field Synchronization

During a provisioning operation, you use a lookup field to specify a single value from a set of values. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system mail store data into the lookup definitions in Oracle Identity Manager.

Note: As an implementation best practice, lookup fields should be synchronized before you perform reconciliation or provisioning operations.

Table 1–2 lists the lookup fields that are synchronized with their corresponding lookup definitions in Oracle Identity Manager.

Table 1–2 Lookup Definitions Created in Oracle Identity Manager

Lookup Definition	Target System Field	Method to Specify Values for the Lookup Definition
AtMap.Exchange	All the fields used during provisioning	You manually add or update entries in this lookup definition. If the value in this lookup does not work on the target system, then you must update the lookup with the correct value. This lookup definition contains mappings between the LDAP attributes of the target system and their corresponding process form fields in Oracle Identity Manager.
Lookup.Exchange.Configuration	Values of parameters used during provisioning and reconciliation	You use this lookup definition to specify parameters that are used during both reconciliation and provisioning. This lookup definition is discussed in "Configuring the Lookup.Exchange.Configuration Lookup Definition" on page 3-3.
Lookup.ExchangeReconciliation.MailStore	All mail stores of the target system	You use the Exchange Mail Store Lookup Reconciliation scheduled task to synchronize this lookup definition. This scheduled task is discussed in "Scheduled Task for Lookup Field Synchronization" on page 3-4.
Lookup.Deleted Item Manager	The deletedItemFlags field of the users	You manually add or update entries in this lookup definition. You use this lookup definition to modify attributes in the Deleted item retention section of the target system.

Table 1–2 (Cont.) Lookup Definitions Created in Oracle Identity Manager

Lookup Definition	Target System Field	Method to Specify Values for the Lookup Definition
Lookup.Hide From Address list	The msExchHideFromAddressLists field of the users	You manually add or update entries in this lookup definition. You use this lookup definition to specify if the user data is displayed in the Address list of the target system.
Lookup.Use Default Storage	The mDBUseDefaults field of the users	You manually add or update entries in this lookup definition. You use this lookup definition to specify whether or not the default storage values of mailboxes are used.
Lookup.Exchange.Constants	NA	This lookup definition stores constants and variables defined in the Java classes that constitute the connector. **Caution:** You must not change any entry in this lookup definition. If you change any entry, then the connector will not function correctly.

1.3.3 Target Resource Reconciliation

In the managed account mode, the connector can be used to perform target resource reconciliation and provisioning.

Target resource reconciliation involves fetching data about newly created or modified mailboxes on the target system and using this data to create or modify mailbox resources assigned to OIM Users. The Exchange Reconciliation Task scheduled task is used to start target resource reconciliation runs. This scheduled task is discussed in "Reconciliation Scheduled Tasks" on page 3-7.

> **See Also:** The "Target Resource Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about target resource reconciliation

This section discusses the following topics:

- Types of Reconciliation Enabled by the Connector
- Mailbox Fields for Target Resource Reconciliation
- Reconciliation Rule
- Reconciliation Action Rules

1.3.3.1 Types of Reconciliation Enabled by the Connector

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

- Reconciliation of Mailbox Data from Mail Stores
- Reconciliation of Mailbox Data from Distribution Groups

1.3.3.1.1 Reconciliation of Mailbox Data from Mail Stores During this type of reconciliation, mailbox data is fetched either from all mail stores configured with the Microsoft Active Directory server on which Microsoft Exchange is enabled, or from mail stores specified in the Exchange Reconciliation Task scheduled task.

You can reconcile mail store data individually from Microsoft Exchange 2000, 2003, or 2007. Alternatively, you can use the connector to integrate Oracle Identity Manager with a combination of different Microsoft Exchange versions, such as Exchange 2003 and 2007. This is known as the **mixed mode setup**.

In a mixed mode scenario, Microsoft Active Directory user objects are stored on Microsoft Active Directory and mailboxes of Microsoft Active Directory users are stored on different Microsoft Exchange installations. For example, user1 and user2 can belong to the same Microsoft Active Directory instance while having a mailbox in Microsoft Exchange 2003 and Microsoft Exchange 2007, respectively.

1.3.3.1.2 Reconciliation of Mailbox Data from Distribution Groups During this type of reconciliation, mailbox data is fetched from all or specific distribution groups specified in the Exchange Reconciliation Task scheduled task. If you want to fetch mailbox data from a specific distribution group, then you can perform query-based reconciliation of mailbox data from distribution groups.

You can also perform distribution group reconciliation and query-based distribution group reconciliation for Microsoft Exchange 2000 and 2003, or you can perform distribution group reconciliation and dynamic distribution group reconciliation for Exchange 2007 a mixed mode setup.

1.3.3.2 Mailbox Fields for Target Resource Reconciliation

Table 1–3 lists the mailbox fields from which values are fetched during a target resource reconciliation run.

Table 1–3 Mailbox Fields for Target Resource Reconciliation

Process Form Field	Target System Field	Description
Deleted Item Manager	deletedItemFlags	Number of items in the Deleted Items folder
Display Name	displayName	Name of a user as displayed in the address book This is usually a combination of the user's first name, middle initial, and last name.
Email Alias **Note:** This is a mandatory field.	mailNickname	Mailbox alias, which is generally the same as sAMAccountName **Note:** sAMAccountName is the user login for Microsoft Active Directory.
Garbage Collection Period	garbageCollPeriod	Time interval, in days, between garbage collection runs This field corresponds to the "Keep deleted items for (days)" field value on the target system.
Hide From Address Lists	msExchHideFromAddressLists	Specifies if the user appears in address lists
Mailbox Size Receipt Quota	mDBOverHardQuotaLimit	Maximum mailbox size, in KB, over which sending and receiving e-mail is disabled This field corresponds to the *Prohibit send and receive at (KB)* field on the target system.
Mailbox Size Transmit Quota	mDBOverQuotaLimit	Mailbox quota overdraft limit, in KB This field corresponds to the *Prohibit send at (KB)* field on the target system.
Mailbox Warning Size	mDBStorageQuota	Message database quota, in KB This field corresponds to the *Issue warning at (KB)* field on the target system.
Major Business Number	telephonenumber	Primary office phone number
Max Incoming Message Size	delivContLength	Maximum incoming message size, in KB
Max Outgoing Message Size	submissionContLength	Maximum outgoing message size, in KB
Max Recipients Per Message	msExchRecipLimit	Maximum number of recipients of a single e-mail

Table 1–3 (Cont.) Mailbox Fields for Target Resource Reconciliation

Process Form Field	Target System Field	Description
Mobile Number	mobile	Primary mobile phone number
Object GUID	objectGUID	GUID based on the current time stamp assigned to an object
Other Business Number	otherTelephone	Alternative office phone number
Pager Number	pager	Primary pager number
Use Storage Defaults	mDBUseDefaults	Specifies whether or not the mailbox store must use the default quota, instead of the per-mailbox quota This field corresponds to the *Use mailbox store defaults* field on the target system.
Email	proxyAddresses	Primary e-mail address
Log On Name	userPrincipalName	User Principal name
Mail Store Name	homeMDB	Mail store database name of the user
DB User Defaults	mDBUseDefaults	User database size defaults

1.3.3.3 Reconciliation Rule

The following is the default reconciliation rule for this connector:

Rule Name: Exchange Recon

Rule Element: User Login Equals sAMAccountName

In this rule:

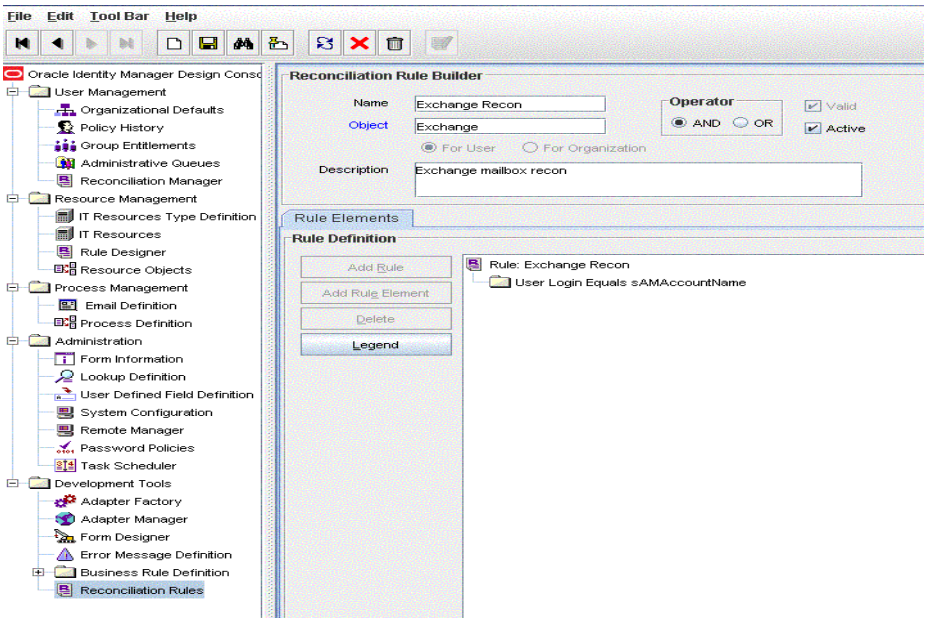
- User Login is the User ID field on the OIM User form.
- sAMAccountName is the User ID field of Microsoft Active Directory. Microsoft Exchange uses the same User ID during reconciliation.

After you deploy the connector, you can view the reconciliation rule for the connector 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 **Exchange Recon**. Figure 1–3 shows the reconciliation rule for the connector.

Figure 1–3 Reconciliation Rule for the Exchange Connector



1.3.3.4 Reconciliation Action Rules

Table 1–4 lists the action rules for target resource reconciliation.

Table 1–4 Action Rules for Target Resource Reconciliation

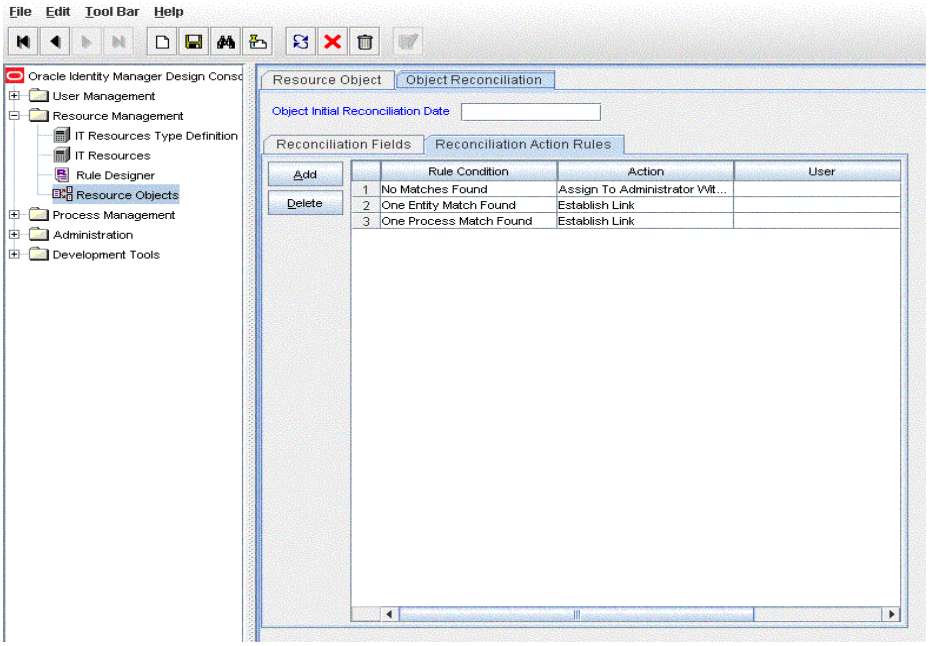
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

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

> **Note:** For any rule condition that is not predefined for this connector, Oracle Identity Manager will neither perform any action nor log an error.

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 **Exchange** resource object.
5. Click the **Object Reconciliation** tab, and then 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 the connector.

Figure 1–4 Reconciliation Action Rules for the Connector



1.3.4 Provisioning

Provisioning involves creating or modifying mailbox data on the target system through Oracle Identity Manager.

> **See Also:** The "Provisioning" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

This section discusses the following topics:

- Mailbox Provisioning Functions Supported by the Connector
- Mailbox Fields for Provisioning

1.3.4.1 Mailbox Provisioning Functions Supported by the Connector

Table 1–5 lists the supported mailbox provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

> **See Also:** *Oracle Identity Manager Connector Concepts* for generic information about adapters

Table 1–5 Mailbox Provisioning Functions Supported by the Connector

Function	Adapter
Create a mailbox	MEXC Create Mailbox. The following adapters are triggered before the MEXC Create Mailbox adapter is triggered: ■ Check User Process Ordered ■ Chk Value Set ■ Get Value Form User Process If the mailbox is successfully created, then the following adapters are triggered: ■ MEXC Set Primary Email ■ MEXC Set User Properties
Delete a mailbox	MEXC Delete Mailbox
Update the Deleted Item Manager	MEXC Update User Property
Update a display name	MEXC Update User Property
Update an e-mail alias	MEXC Update User Property
Update the garbage collection period (Days)	MEXC Update User Property
Update the "hide from address lists" field	MEXC Update User Property
Update the mailbox size receipt quota (KB)	MEXC Update User Property
Update the mailbox size transmit quota (KB)	MEXC Update User Property
Update the mailbox warning size (KB)	MEXC Update User Property
Update a major business number	MEXC Update User Property
Update the maximum incoming message size (KB)	MEXC Update User Property
Update the maximum outgoing message size (KB)	MEXC Update User Property
Update the maximum recipients per message	MEXC Update User Property
Set Exchange-related properties	MEXC Update User Property
Update the use storage defaults	MEXC Update User Property
Get ObjectGUID from Process	MEXC Get Value From User Process
Update a mobile number	MEXC Update User Property
Update any other business number	MEXC Update User Property
Update a pager number	MEXC Update User Property
Update a primary e-mail address	MEXC Set Primary Email
Disable Mail box	MEXCDisableMailBox
Enable Mail box	MEXCEnableMailBox

1.3.4.2 Mailbox Fields for Provisioning

Table 1–6 lists the mailbox fields used for provisioning. These fields are used in provisioning operations performed on Microsoft Exchange 2000, Microsoft Exchange 2003, and Microsoft Exchange 2007.

Table 1–6 Mailbox Fields Used in Provisioning

Process Form Field	Microsoft Exchange Field	Description	Adapter
Deleted Item Manager	deletedItemFlags	Number of items in the Deleted Items folder If this field is not available or if its value is 0 (zero), then the "Use mailbox store defaults" check box on the target system is automatically selected. If this field is available and its value is non zero, then the "Use mailbox store defaults" check box on the target system is automatically deselected. If the value of this field is 3, then the "Do not permanently delete items until the store has been backed up" check box is automatically selected on the target system. If the value is other than 3, then the "Do not permanently delete items until the store has been backed up" check box is automatically deselected. **Note:** The non zero value can be configured in the Lookup.Deleted Item Manager lookup definition. This depends on the value of the field on the target system.	MEXC Update User Property
Display Name	displayName	Name of a user as displayed in the address book This is usually a combination of the user's first name, middle initial, and last name.	MEXC Update User Property
Garbage Collection Period (Days)	garbageCollPeriod	Time interval, in days, between garbage collection runs. This field corresponds to the Keep deleted items for (days) field value on the target system. The value of the Keep deleted items for (days) field takes effect only when the Deleted Item Manager field value is non zero.	MEXC Update User Property
Email Alias **Note:** This is a mandatory field.	mailNickname	Mailbox alias, which is generally the same as sAMAccountName	MEXC Update User Property
Hide From Address Lists	msExchHideFromAddressLists	Specifies if the user appears in address lists Default value: `false` **Note:** This field is not used during mailbox creation. It can be used only during a mailbox update.	MEXC Update User Property

Table 1–6 (Cont.) Mailbox Fields Used in Provisioning

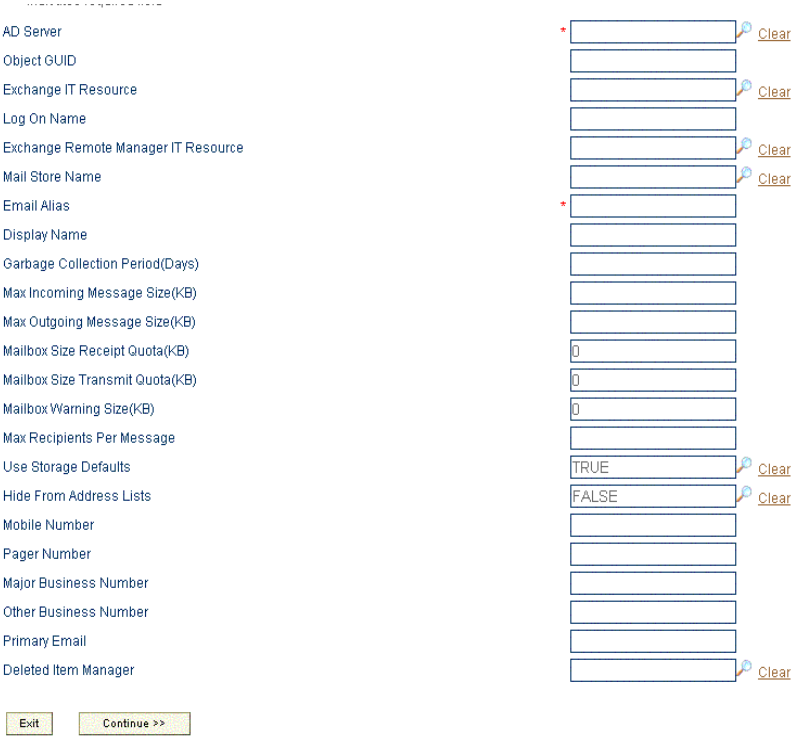
Process Form Field	Microsoft Exchange Field	Description	Adapter
Mailbox Size Receipt Quota (KB)	mDBOverHardQuotaLimit	Maximum mailbox size, in KB, over which sending and receiving e-mail is disabled This field corresponds to the Prohibit send and receive at (KB) field on the target system. Default value: 0 **Note:** If you want to specify a mailbox size receipt quota, then set the value of the Use Storage Defaults field as `false` and specify a value for this field.	MEXC Update User Property
Mailbox Size Transmit Quota (KB)	mDBOverQuotaLimit	Mailbox quota overdraft limit, in KB This field corresponds to the Prohibit send at (KB) field on the target system. Default value: 0 **Note:** If you want to specify a mailbox size receipt quota, then set the value of the Use Storage Defaults field as `false` and specify a value for this field.	MEXC Update User Property
Mailbox Warning Size (KB)	mDBStorageQuota	Message database quota, in KB This field corresponds to the Issue warning at (KB) field on the target system. Default value: 0 **Note:** If you want to specify a mailbox size receipt quota, then set the value of the Use Storage Defaults field as `false` and specify a value for this field.	MEXC Update User Property
Major Business Number	telephonenumber	Primary office phone number	MEXC Update User Property
Max Incoming Message Size (KB)	delivContLength	Maximum incoming message size, in KB	MEXC Update User Property
Max Outgoing Message Size (KB)	submissionContLength	Maximum outgoing message size, in KB	MEXC Update User Property
Max Recipients Per Message	msExchRecipLimit	Maximum number of recipients of a single e-mail	MEXC Update User Property
Use Storage Defaults	mDBUseDefaults	Storage Defaults configuration Default value: true	MEXC Update User Property
Mobile Number	mobile	Primary mobile phone number	MEXC Update User Property
Object GUID	objectGUID	GUID based on the current time stamp assigned to an object	MEXC Get Value From User Process
Other Business Number	otherTelephone	Alternative office phone number	MEXC Update User Property
Pager Number	pager	Primary pager number	MEXC Update User Property

Table 1–6 (Cont.) Mailbox Fields Used in Provisioning

Process Form Field	Microsoft Exchange Field	Description	Adapter
Primary Email	proxyAddresses	Primary e-mail address	MEXC Set Primary Email
Mail Store Name **Note:** This is a mandatory field for provisioning.	homeMDB	Indicates the mail store and the server name to which the mailbox must be provisioned. This lookup definition is populated after successful reconciliation of mail stores. **Note:** Although this is a mandatory field, it is not marked as mandatory in the process form. This is done so that the accounts of mail users who do not have a mail store can be reconciled in Microsoft Exchange 2007.	MEXC Create Mailbox.
Log On Name This is a mandatory field for provisioning in Microsoft Exchange 2007.	userPrincipalName	userPrincipalName of an AD object. During a provisioning operation, you must enter the logon name in the following format: `user1@domain name.com` **Note:** The domain name in the specified format corresponds to the Microsoft Active Directory domain name.	MEXC Create Mailbox.

Figure 1–5 shows the process form fields for this connector.

Figure 1–5 Process Form Fields of the Connector



1.4 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of the 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 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to perform provisioning operations and configure reconciliation runs.
- Chapter 5, "Known Issues" lists the known issues associated with this release of the connector.
- Appendix A, "Special Characters Supported for Alias Name" lists special characters that you can use in the Alias Name field on the target system and Oracle Identity Manager.

2

Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- Preinstallation
- Installation
- Postinstallation

> **Note:** Some of the procedures described in this chapter are meant to be performed on the target system. The minimum permissions required to perform the target system procedure are those assigned to members of the Domain Admins group. To perform the target system-specific procedures, you can use the same user account that you create for deploying the Microsoft Active Directory User Management connector.
>
> See the "Deploying the Connector" chapter of *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for information about creating that user account.

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Preinstallation on Oracle Identity Manager
- Preinstallation on the Target System

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Files and Directories On the Connector Installation Media
- Determining the Release Number of the Connector

2.1.1.1 Files and Directories On the Connector Installation Media

The contents of the connector installation media directory are described in Table 2–1.

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

File in the Installation Media Directory	Description
configuration/Exchange-CI.xml	This XML file contains configuration information that is used during the connector installation process.
lib/xliExchange.jar	This JAR file contains the class files required for provisioning.
lib/xliExchangeRecon.jar	This JAR file contains the class files required for reconciliation.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. **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.
script/CreateMailboxExchange2007.vbs	This VBScript file is used by the Remote Manager to provision mailboxes in Exchange 2007. This script is called by the Remote Manager.
xml/MicrosoftExchange-ConnectorConfig.xml	This XML file contains definitions for the connector components. These components include the following: ■ IT resource type ■ Process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Prepopulate rules ■ Lookup definitions ■ Scheduled tasks

2.1.1.2 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the current 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/xliExchange.jar

2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the xliExchange.jar file and the xliExchangeRecon.jar file.

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

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves creating a target system user account with appropriate permissions for connector operations. Oracle Identity Manager requires this account to connect to the target system during reconciliation and provisioning operations.

You can use a Microsoft Windows 2003 Server (Domain Controller) administrator account as a target system user account. Alternatively, you can create a user account

and assign the minimum required rights to that user account, if Microsoft Active Directory and Microsoft Exchange are not installed on the same system.

The procedure to create a target system user account is provided in the following section.

2.1.2.1 Creating a Target System User Account for Connector Operations

To create the Microsoft Exchange user account for connector operations:

> **Note:** You need not perform this procedure if Microsoft Active Directory and Microsoft Exchange are installed on the same system.

1. Create a group, for example OIMEXCConGroup, on Microsoft Active Directory.
2. Make this group a member of the Account Operators group.
3. Assign all read permissions for the OIMEXCConGroup group.

> **Note:** You assign read permissions on the Security tab of the dialog box for creating the user account. This tab is displayed only in Advanced Features view. To switch to this view, select Advanced Features from the View menu in the Microsoft Active Directory console.

4. Assign the OIMEXCConGroup group to be a member of the Exchange View-Only Administrators group. Users in this group have permission to read all Exchange configuration.
5. Create a user, for example OIMEXCConUser on the target system.
6. Assign this user to the OIMEXCConGroup group. Using OIMEXCConUser, you can perform provisioning and reconciliation. You can also enable, disable, and delete a mailbox on Microsoft Exchange.

2.2 Installation

Installation information is divided across the following sections:

- Installation on Oracle Identity Manager
- Installation on the Target System

2.2.1 Installation on Oracle Identity Manager

Installation on Oracle Identity Manager involves the following procedures:

- Running the Connector Installer
- Creating the IT Resource

2.2.1.1 Running the Connector Installer

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

Ensure that the Microsoft Active Directory User Management connector is installed before you proceed to install the connector.

To run the Connector Installer:

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

   OIM_HOME/xellerate/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console Guide*.

3. Click **Deployment Management**, and then click **Install Connector**.

4. From the Connector List list, select **Exchange 9.1.1**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

   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 **Exchange 9.1.1**.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed, in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

   c. Compilation of adapters

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

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

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

   a. Ensuring that the prerequisites for using the connector are addressed

Note: At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-12 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

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 2–2.

Table 2–2 Files Copied During Connector Installation

File in the Installation Media Directory	Destination Directory
lib/xliExchange.jar	*OIM_HOME*/xellerate/JavaTasks
lib/xliExchangeRecon.jar	*OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources

Note: For a clustered environment, copy the files listed in Table 2–2 into their respective destination directories on each node of the cluster.

2.2.1.1.1 Copying the ldapbp.jar File

The ldapbp.jar file is used by the connector to enable LDAP-based search of user records on the target system. During the installation of the Microsoft Active Directory User Management connector, this file is copied into the ThirdParty directory of Oracle Identity Manager.

See the "Running the Connector Installer" section of *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for details.

Note: for a clustered environment, this JAR file must be copied into the ThirdParty directory on each node of the cluster.

2.2.1.1.2 Installing the Connector in an Oracle Identity Manager Cluster

While installing the connector in a clustered environment, you must copy all the JAR files and the contents of the resources directory into their destination directories on each node of the cluster. See Table 2–2, " Files Copied During Connector Installation" for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

2.2.1.2 Creating the IT Resource

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information for reconciliation and provisioning.

For reconciliation and provisioning in Microsoft Exchange 2000 and Microsoft Exchange 2003, Oracle Identity Manager uses the Microsoft Active Directory IT resource. See *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for instructions to create Microsoft Active Directory IT resources.

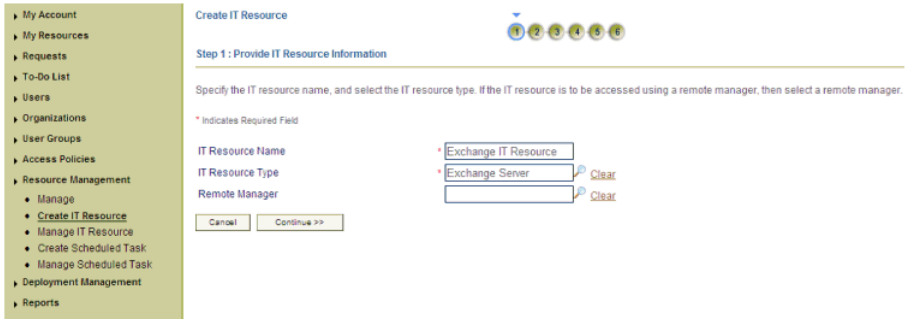
For reconciliation in Microsoft Exchange 2007, Oracle Identity Manager uses the Microsoft Active Directory IT resource. For provisioning in Microsoft Exchange 2007, Oracle Identity Manager uses the Microsoft Active Directory IT resource and Microsoft Exchange Server IT resource values.

To create the Microsoft Exchange Server IT resource:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Create IT Resource.**
4. On the Step 1: Provide IT Resource Information section, perform the following steps:
   - **IT Resource Name**: Enter `Exchange Server IT Resource`.
   - **IT Resource Type**: Select **Exchange Server** from the IT Resource Type list.
   - **Remote Manager**: At this point, do not enter a value in this field.

   Note: After you install a Remote Manager for the target system, specify the name of the IT resource for the Remote Manager as the value of the Remote Manager parameter. See "Installing the Remote Manager" on page 2-10 for information about whether or not you need to install a Remote Manager.
5. Click **Continue**. Figure 2–1 shows IT resource values added in the Create IT Resource page.

Figure 2–1 Step 1: Provide IT Resource Information



6. On the Step 2: Specify IT Resource Parameter Values section, specify values for the parameters of the IT resource and click **Continue**. Figure 2–2 shows IT resource parameter values added in the Create IT Resource page.

Figure 2–2 Step 2: Specify IT Resource Parameter Values

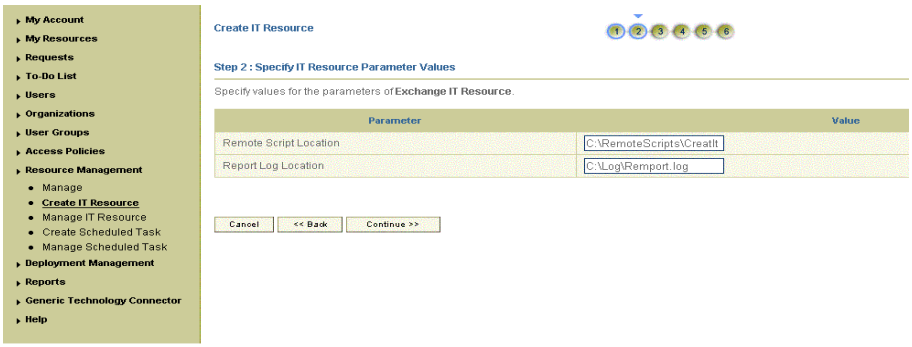


Table 2–3 describes the parameters for this IT resource.

Table 2–3 Parameters of the IT Resource

Parameter	Description
Remote Script Location	Enter the full path of the CreateMailboxExchange2007.vbs script placed in the remote system (This remote system is the system where Exchange 2007 has been installed). The Remote Manager uses this script to create mailboxes on the target system. **Note:** This parameter is case-sensitive. Therefore, you must enter the correct case (uppercase and lowercase) of the path to the directory where the script is copied. Sample value: *RM_HOME*/RemoteScripts/CreateMailboxExchange2007.vbs
Report Log Location	Enter the full path of the directory where you want the log files to be generated. The log file stores the outcome of each run of the CreateMailboxExchange2007.vbs script. You must create the directory if it does not already exist. **Note:** This parameter is case-sensitive. Therefore, you must enter the correct case (uppercase and lowercase) of the path to the directory where the log files are to be generated. Sample value: RM_HOME/Log/Report.log Report.log is the name of the log file generated. You can change this file name.

7. The Step 3: Set Access Permission to IT Resource page is displayed. On this page, the SYSTEM ADMINISTRATORS group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

Note: This step is optional.

If you want to assign groups to the IT resource and set access permissions for the groups, then:

a. Click **Assign Group**.

b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the ALL USERS group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

c. Click **Assign**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

   Note:

   - This step is optional.

   - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

   a. Click **Update Permissions**.

   b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

   c. Click **Update**.

9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

   Note:

   - This step is optional.

   - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

   a. Select the **Unassign** check box for the group that you want to unassign.

   b. Click **Unassign**.

10. Click **Continue**.

11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

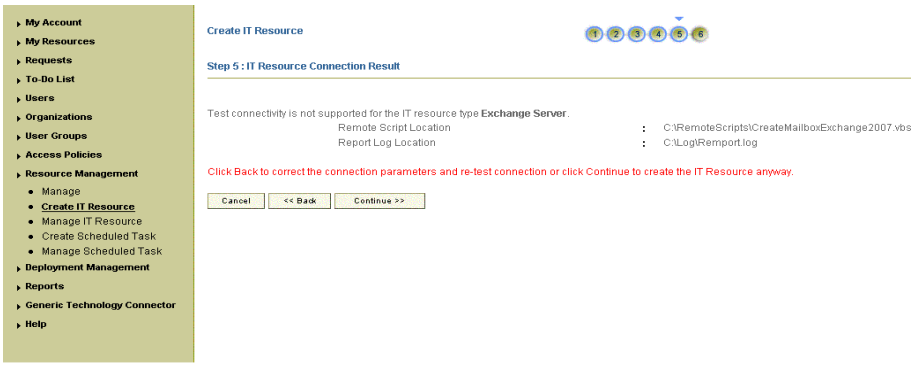
12. To proceed with the creation of the IT resource, click **Continue**. Figure 2–3 shows the IT resource details that you created in the Create IT Resource page.

Figure 2–3 Step 4: Verify IT Resource Details

13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Create**. If the test fails, then you can perform one of the following steps:

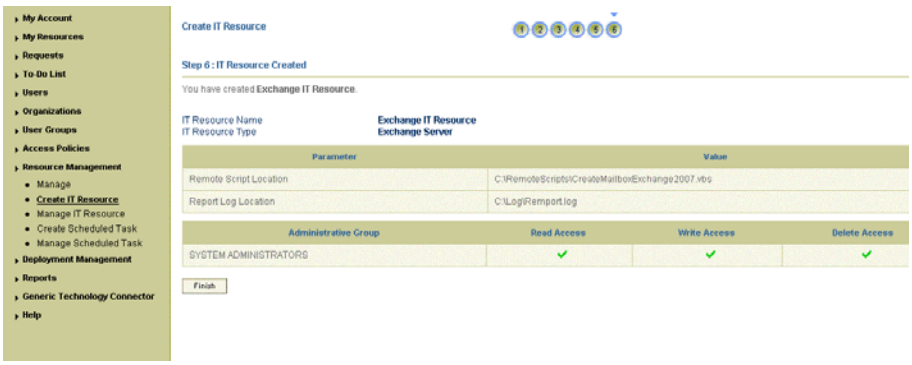
    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.
    - Proceed with the creation process by clicking **Continue**. You can fix the problem later, and then rerun the connectivity test by using the Diagnostic Dashboard. Figure 2–4 shows the IT resource connection result in the Create IT Resource page.

Figure 2–4 Step 5: IT Resource Connection Result Page



14. The Step 6: IT Resource Created page displays the details of the IT resource that you created. Click **Finish**. Figure 2–5 shows the IT resource created in the Create IT Resource page.

Figure 2–5 IT Resource Created Page of Oracle Identity Manager



2.2.2 Installation on the Target System

This section discusses the following topics:

- Installing the Remote Manager
- Enabling Client-Side Authentication for the Remote Manager

Note: The procedure to configure the Remote Manager is described in "Configuring the Remote Manager" on page 2-15.

2.2.2.1 Installing the Remote Manager

The Remote Manager enables mailbox provisioning operations on Microsoft Exchange 2007.

Note: If Microsoft Exchange 2007 is running on 64-bit Microsoft Windows Server, then you must install the 64-bit version of JDK 1.4.2_15 or JDK 1.5 before you install the Remote Manager.

You must install the Remote Manager for Microsoft Exchange 2007 if you have not installed the Remote Manager for Microsoft Active Directory. See *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for information about this Remote Manager.

A single Remote Manager can be used with multiple Microsoft Exchange installations (on multiple host computers) that are configured for a single Microsoft Active Directory installation. The Remote Manager can be installed on any Microsoft Exchange host on which Exchange Management tools are installed.

Note:

- See the "Deploying the Connector" chapter of *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for information about installing and configuring the Remote Manager for Microsoft Active Directory.
- In this guide, the directory in which you install the Remote Manager is referred to as *RM_HOME*.

To deploy the Remote Manager:

1. The Remote Manager installation files are shipped along with the Oracle Identity Manager installation files. Depending on the application server that you use, perform the procedure to install the Remote Manager on the target system computer 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 IBM WebSphere Application Server*
   - *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
   - *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*
2. 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

- *OIM_HOME*/xellerate/JavaTasks/xliActiveDirectory.jar
- *OIM_HOME*/xellerate/ScheduleTask/xliADRecon.jar
- *OIM_HOME*/xellerate/JavaTasks/xliExchange.jar
- *OIM_HOME*/xellerate/ScheduleTask/xliExchangeRecon.jar

3. Copy the CreateMailboxExchange2007.vbs file from the following directory on the installation media to the *RM_HOME*/scripts directory:

   scripts/CreateMailboxExchange2007.vbs

   Note: Ensure that the RM_HOME directory is secured using Microsoft Windows best practices. Only the target system user account for Oracle Identity Manager must have permissions to access the RM_HOME directory.

4. 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

5. Specify the name of the Remote Manager as the value of the Remote Manager IT resource parameter. This parameter is described in "Creating the IT Resource" on page 2-6.

   See *Oracle Identity Manager Administrative and User Console Guide* for information about modifying the value of an IT resource parameter.

2.2.2.2 Enabling Client-Side Authentication for the Remote Manager

To enable client-side authentication for the Remote Manager:

Note: If you have already enabled client-side authentication for the Remote Manager in Microsoft Active Directory, then you need not perform the procedure described in this section.

1. Open the *RM_HOME*/xlremote/config/xlconfig.xml file in a text editor.
2. Set the ClientAuth property to `true` as follows:

   ```
   <ClientAuth>true</ClientAuth>
   ```

3. Ensure that the RMIOverSSL property is set to true as follows:

   ```
   <RMIOverSSL>true</RMIOverSSL>
   ```

4. Perform Steps 2 through 3 in the *OIM_HOME*/config/xlconfig.xml file.

2.3 Postinstallation

Postinstallation information is divided across the following sections:

- Postinstallation on Oracle Identity Manager
- Postinstallation on the Target System
- Configuring the Remote Manager

2.3.1 Postinstallation on Oracle Identity Manager

Postinstallation on Oracle Identity Manager consists of the following procedures:

Note: In a clustered environment, you must perform these procedures on each node of the cluster.

- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

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

While you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory. Whenever you add a new resource bundle in 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, go to the *OIM_HOME*/xellerate/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:

   OIM_HOME/xellerate/bin/*BATCH_FILE_NAME*

2. Enter one of the following commands:

   - 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.

   In this command, `ConnectorResourceBundle` is the content category that you must delete from the server cache.

   See Also: The following file for information about content categories:

   OIM_HOME/config/xlconfig.xml

2.3.1.2 Enabling Logging

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 may 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.OIMCP.MEXC=LOG_LEVEL
     ```

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

     For example:

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

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

- **IBM WebSphere Application Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=LOG_LEVEL
     log4j.logger.OIMCP.MEXC=LOG_LEVEL
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     ```

```
log4j.logger.OIMCP.MEXC=INFO
```

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

WEBSHERE_HOME/AppServer/logs/SERVER_NAME/SystemOut.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="OIMCP.MEXC">
   <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="OIMCP.MEXC">
   <priority value="INFO"/>
</category>
```

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

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

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

```
log4j.logger.XELLERATE=LOG_LEVEL
log4j.logger.OIMCP.MEXC=LOG_LEVEL
```

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

     For example:

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

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

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

2.3.2 Postinstallation on the Target System

Postinstallation on the target system involves the following procedure:

2.3.2.1 Configuring SSL

You need not configure SSL for Microsoft Exchange if it is already configured on the Microsoft Active Directory target system to which your Microsoft Exchange is linked.

2.3.3 Configuring the Remote Manager

Note: Perform this procedure only if you have installed the Remote Manager for Microsoft Exchange 2007. The procedure to install the Remote Manager is described in "Installing the Remote Manager" on page 2-10.

If you have installed multiple Microsoft Exchange 2007 Remote Managers, then you must perform this procedure for each Remote Manager.

The IT resource for the Remote Manager contains connection information about the Remote Manager. The Remote Manager is used by Oracle Identity Manager to invoke the Exchange Management Shell script to create mailboxes in Microsoft Exchange 2007. When you run the Connector Installer, the IT resource for the Remote Manager is created in Oracle Identity Manager for Microsoft Exchange 2007.

For reconciliation in Microsoft Exchange 2007, Oracle Identity Manager uses the Microsoft Active Directory IT resource. For provisioning in Microsoft Exchange 2007, Oracle Identity Manager uses the Microsoft Active Directory IT resource, Exchange IT resource, and the Remote Manager IT resource values. For information about the Exchange IT resource parameters, see "Creating the IT Resource" on page 2-6.

This section discusses the following topics:

- Creating the IT Resource for the Remote Manager
- Configuring Oracle Identity Manager to Trust the Remote Manager
- Verifying That the Remote Manager Is Running

2.3.3.1 Creating the IT Resource for the Remote Manager

To create the IT resource for the Remote Manager:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Create IT Resource**.
4. On the Step 1: Provide IT Resource Information page, enter the following information:
   - **IT Resource Name**: Enter `Exchange Remote Manager IT Resource`.
   - **IT Resource Type**: Select **Remote Manager** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.
5. Click **Continue**.
6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Table 2–4 describes the parameters for this IT resource.

Table 2–4 Parameters of the IT Resource for the Remote Manager

Parameter	Description
service name	Enter a name for the remote manager. Sample value: `RManager`
url	Enter the IP address of the target system host computer and the port number at which the Remote Manager is listening. Sample value: `rmi//10.0.0.1:12346`

7. Click **Continue**.
8. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.
9. To proceed with the creation of the IT resource, click **Continue**.
10. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Create**. If the test fails, then you can perform one of the following steps:
    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.
    - Proceed with the creation process by clicking **Continue**. You can fix the problem later, and then rerun the connectivity test by using the Diagnostic Dashboard.
11. The Step 6: IT Resource Created page displays the details of the IT resource that you created. Click **Finish**.

2.3.3.2 Configuring Oracle Identity Manager to Trust the Remote Manager

To configure Oracle Identity Manager to trust the Remote Manager you have installed:

1. From the computer hosting the Remote Manager, copy the *RM_HOME*/xlremote/config/xlserver.cert file to a temporary directory on the Oracle Identity Manager host computer.

   Note: The server certificate in the *OIM_HOME* directory is also named xlserver.cert. Ensure that you do not overwrite that certificate.

2. To import the certificate by using the keytool utility, run the following command:

   ```
   JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
   RM_CERT_LOCATION/xlserver.cert -keystore OIM_HOME/xellerate/config/.xlkeystore
   -storepass PASSWORD
   ```

   In the preceding command, replace:

   – *JAVA_HOME* with the location of the Java directory for your application server.

   – *ALIAS* with an alias for the certificate in the store.

- *RM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.
- *PASSWORD* with the password of the keystore.

3. Copy the *OIM_HOME*/xellerate/config/xlserver.cert file to a temporary directory on the Remote Manager host computer.
4. To import the certificate by using the keytool utility on the Remote Manager host computer, run the following command:

```
JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
OIM_CERT_LOCATION/xlserver.cert -keystore RM_HOME/xlremote/config/.xlkeystore
-storepass PASSWORD
```

In the preceding command, replace:

- *JAVA_HOME* with the location of the Java directory for your application server.
- *ALIAS* with an alias for the certificate in the store.
- *OIM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.
- *PASSWORD* with the password of the keystore.

Note: It is recommended that you follow security best practices and change the default passwords used for the Remote Manager keystore. To change the Remote Manager keystore password, follow the instructions given in *Oracle Identity Manager Installation and Configuration Guide* for your application server.

2.3.3.3 Verifying That the Remote Manager Is Running

To ensure that the Remote Manager is running:

1. Use the following script to start the Remote Manager:

   RM_HOME/xlremote/remotemanager.bat
2. Log in to the Design Console.
3. Expand **Administration**, and double-click **Remote Manager**.
4. Search for and open the Remote Manager that you have created.
5. Click the Refresh icon. The screen displays details of the Remote Manager that you have configured. The running check box should be selected for the Remote Manager. This implies that the status of the Remote Manager is active.

3

Using the Connector

This chapter discusses the following:

- The "Guidelines on Using the Connector" section described the guidelines that you must apply while using the connector.
- The "Configuring the Lookup.Exchange.Configuration Lookup Definition" section describes the parameters of the Lookup.Exchange.Configuration lookup definition.
- The "Scheduled Task for Lookup Field Synchronization" section describes the Exchange Mail Store Lookup Reconciliation scheduled task.
- The "Configuring Reconciliation" section describes the different types of reconciliation and the scheduled tasks that are created for this connector.
- The "Configuring Scheduled Tasks" section describes the procedure to configure scheduled tasks that are created when you deploy the connector.
- The "Configuring Provisioning" section describes how to use this connector for provisioning.

3.1 Guidelines on Using the Connector

This section contains the following topics:

- Guidelines on Configuring Reconciliation Runs
- Guidelines on Performing Provisioning Operations

3.1.1 Guidelines on Configuring Reconciliation Runs

The following are guidelines that you must apply while configuring reconciliation:

- The connector does not support Delete Mailbox reconciliation in Microsoft Exchange 2007. This is because when you delete a mailbox in Microsoft Exchange 2007, the corresponding Microsoft Active Directory user object is also removed.
- Before a mailbox reconciliation run is performed, you must ensure that the lookup definitions are synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before mailbox reconciliation runs, and, when required, before provisioning operations.
- The scheduled tasks for lookup field synchronization must be run before the scheduled tasks for reconciliation of existing and deleted mailbox data.
- The scheduled task for reconciliation of mailbox data must be run before the scheduled task for reconciliation of deleted mailbox data.

- If the operating environment consists of one Microsoft Active Directory installation and multiple Microsoft Exchange 2007 installations, then to reconcile mailboxes from a particular Exchange installation:

  1. Change the value of the AD Server IT Resource attribute of the mailbox reconciliation scheduled task (Exchange Reconciliation Task) so that it points to the required Exchange installation.

     Note: This scheduled task is explained in detail later in this chapter.

  2. Run the scheduled task.

3.1.2 Guidelines on Performing Provisioning Operations

The following are guidelines that you must apply while performing provisioning operations:

- When you perform a Create Mailbox provisioning operation on Microsoft Exchange 2007, a Remote Manager is used to run the Create User cmdlet (script) that creates the mailbox for the user on the target system.
- The following points describe the behavior of the connector during Enable, Disable, and Delete Mailbox provisioning operations:
  - When you perform an Enable Mailbox provisioning operation on Microsoft Exchange 2000, 2003, or 2007, the following target system attributes are set to their default values:
    * Max Incoming Message Size (KB)
    * Max Outgoing Message Size (KB)
  - When you perform a Disable Mailbox provisioning operation on Microsoft Exchange 2000, 2003, or 2007, the following target system attributes are set to zero (0):
    * Max Incoming Message Size (KB)
    * Max Outgoing Message Size (KB)
  - When you perform a Delete Mailbox provisioning operation on Microsoft Exchange 2000, 2003, or 2007, the connector deletes the Microsoft Exchange attributes of that user.
- While performing provisioning operations on Microsoft Exchange 2007, you must select the Log On Name, Exchange IT Resource, and the Exchange Remote Manager IT resource fields along with the mandatory fields of the process form. You must not select these fields while performing provisioning operations on Microsoft Exchange 2000 and 2003. If you select these fields for Microsoft Exchange 2000 and 2003, then provisioning fails.
- According to Microsoft, you must restart Microsoft Exchange 2000 and Microsoft Exchange 2003 each time you enable or disable a mailbox through provisioning. However, you need not restart Microsoft Exchange 2007 after enabling or disabling a mailbox through provisioning, because it is a supported operation in Microsoft Exchange 2007.

Note: The Enable Mailbox and Disable Mailbox actions are not directly supported by Microsoft Exchange 2000 or Microsoft Exchange 2003. However, the connector supports both provisioning and reconciliation of Enable Mailbox and Disable Mailbox actions through flag fields on the process form.

- Specifying multibyte values for fields

Note: This point is also mentioned in the "Known Issues" chapter.

Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

Suppose you can enter 50 characters of English in the Display Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

- The character length of target system fields must be taken into account when specifying values for the corresponding Oracle Identity Manager fields

  During a provisioning operation, you must keep the lengths of target system fields in mind while entering values for Oracle Identity Manager process form fields. The character limit specified for some process form fields may be more than that of the corresponding target system field.

- If the operating environment consists of one Microsoft Active Directory installation and multiple Microsoft Exchange 2007 installations, then to perform a provisioning operation on a particular Exchange installation:

  1. Run the scheduled task for lookup field synchronization (Exchange Mail Store Lookup Reconciliation).
  2. While performing the provisioning operation on the Administrative and User Console, select the IT resource for the Exchange installation.

3.2 Configuring the Lookup.Exchange.Configuration Lookup Definition

When you deploy the connector, the Lookup.Exchange.Configuration lookup definition is created in Oracle Identity Manager. The entries in this lookup definition are used during both reconciliation and provisioning.

To configure the Lookup.Exchange.Configuration lookup definition:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the **Lookup.Exchange.Configuration** lookup definition.
4. Enter decode values for each of the parameters listed in Table 3–1.

Table 3–1 Attributes of the Lookup.Exchange.Configuration Lookup Definition

Parameter Name	Description	Default/Sample Value
PageSize	This parameter is used during reconciliation. The value represents the number of records to be fetched for a reconciliation run. You can configure this value according to your requirement. The value must be between 1 and 1000. It is recommended that you set the value of this parameter to 100.	100
ldapUserObjectClass	This is the object class used in the schema. By default Microsoft Active Directory has the user object class. You can change this value if you want to define your own schema.	user
ROExgInMsgSizeCol	If you create a copy of the process form, then specify the name of the attribute (column) in the new process form that holds the incoming message size value.	UD_MSEXCHG_INMSGSIZE
ROExgOutMsgSizeCol	If you create a copy of the process form, then specify the name of the attribute (column) in the new process form that holds the outgoing message size value.	UD_MSEXCHG_OUTMSGSIZE
DefaultInComingMsgSize	Enter the maximum incoming message size (in KB). This value is used when you enable a mailbox.	10240
DefaultOutGoingMsgSize	Enter the maximum incoming message size (in KB). This value is used when you enable a mailbox.	10240
AD Configuration Lookup	This parameter holds the name of the configuration lookup definition in Microsoft Active Directory. The default value is `Lookup.AD.Configuration`. If you create a copy of the Lookup.AD.Configuration lookup definition, then you must enter the name of that copy.	Lookup.AD.Configuration

5. Click **Save**.

3.3 Scheduled Task for Lookup Field Synchronization

The Exchange Mail Store Lookup Reconciliation scheduled task is used to fetch the list of mail stores created on the target system. This data is used to update the list of mail stores in Oracle Identity Manager.

Table 3–2 lists 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 is left empty, then reconciliation is not performed.

Table 3–2 Attributes of the Exchange Mail Store Lookup Reconciliation Scheduled Task

Attribute	Description
AD IT Resource	Enter the name of the Microsoft Active Directory IT resource Sample value: `ADITResource`
Lookup Code Name	Name of the lookup definition to which mail store data must be copied Default value: `Lookup.ExchangeReconciliation.MailStore`

After mail store lookup synchronization, the mail store names are stored in the Lookup.ExchangeReconciliation.MailStore lookup definition in the following format:

MAIL_STORE_NAME/*ADMINISTRATIVE_GROUP_NAME*/*MAIL_STORE_SERVER_NAME*

In the format, the mail store is located under the administrative group and this group is located in the Exchange server.

During a provisioning operation, you can view the values in the lookup field and select the value that you want to use.

3.4 Configuring Reconciliation

The following sections provide information about the attributes of the scheduled tasks:

> **See Also:** The "Reconciliation Configuration Options" section in *Oracle Identity Manager Connector Concepts* for detailed information about the configuration options described in some of the following topics

- Limited Reconciliation vs. Regular Reconciliation
- Full Reconciliation vs. Incremental Reconciliation
- Reconciliation Scheduled Tasks
- Creating the Reconciliation Scheduled Task (Optional)

3.4.1 Limited Reconciliation vs. Regular Reconciliation

This section discusses the Query attribute of the scheduled tasks for 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 specify the subset of newly added or modified target system records that must be reconciled. You do this by creating a query condition to act as a filter for reconciliation.

To create a query condition in a nonnative format, use a combination of target system fields and the following logical operators:

> **Note:** You can use any target system fields, even the ones that are not supported (by default) for reconciliation and provisioning.

- The AND operator represented by the ampersand (&)
- The OR operator represented by the vertical bar (|)
- The EQUAL operator represented by the equal sign (=)

You must apply the following guidelines while creating the query condition:

- The default Query attribute value is `(objectClass=user)`. When you create query, it is recommended that you retain the default value as one of the query conditions. For example:

  ```
  (&(mailNickName=*)(objectClass=user))
  ```

- You must independently verify that the query returns the objects that you want it to return. The scheduled task does not validate your query.
- For the target system fields, 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 special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

Note: The default Query attribute value is `(objectClass=user)`.

The following are sample query condition:

- `(&(objextClass=user)(givenname=john)`
- `(&(objectClass=user)(sn=Doe)`
- `(&(&(sn=Doe)(givenname=John))(objectClass=user))`
- `(|(|(sn=lastname)(givenname=firstname))(objectClass=user))`

While performing the procedure described in the section, set the value of the Query attribute to the query condition that you create.

3.4.2 Full Reconciliation vs. Incremental Reconciliation

This section discusses the Submit All Records attribute of the scheduled tasks for reconciliation in Microsoft Exchange.

After you deploy the connector, you first reconcile all the existing target system records into Oracle Identity Manager. At the end of this reconciliation run, the MEXC Timestamp attribute of the scheduled task is set to the time stamp at which the scheduled task finished running. This is a full reconciliation run.

During the next reconciliation run, the value of MEXC Timestamp is used to determine the time stamp at which the last run finished. User records added or modified after the time stamp are selected for reconciliation during the current run. This is incremental reconciliation.

Some user records may never be reconciled into Oracle Identity Manager during subsequent reconciliation runs. For example, user records that are added or modified around the time that the MEXC Timestamp attribute is updated may not meet the time-stamp criterion for reconciliation during the next reconciliation run. To ensure that such records are reconciled into Oracle Identity Manager, you must run full reconciliation at periodic intervals.

While configuring the reconciliation scheduled tasks by performing the procedure described in "Configuring Scheduled Tasks" on page 3-12:

- To run full reconciliation, set the value of the Submit All Records attribute to `yes`.
- To continue with incremental reconciliation, accept the default value of `no` for the attribute.

3.4.3 Reconciliation Scheduled Tasks

When you run the Connector Installer, reconciliation scheduled tasks are automatically created in Oracle Identity Manager. The Microsoft Exchange connector provides the following scheduled tasks for reconciliation:

- Exchange Reconciliation Task
- Exchange Delete Recon Task

3.4.3.1 Exchange Reconciliation Task

The Exchange Reconciliation Task scheduled task is used to reconcile data from active mailboxes. Table 3–3 lists the attributes of this scheduled task.

Table 3–3 Attributes of the Exchange Reconciliation Task Scheduled Task

Attribute	Description
ResourceObject	This attribute holds the name of the resource object against which reconciliation runs must be performed. Default value: `Exchange` Note: For the resource object shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the resource object, then you can enter the unique name for that resource object as the value of this attribute.
Recon Attribute Lookup Code Name	Enter the name of the lookup table containing the mapping for the Exchange attributes. You are not allowed to delete attributes from this table. Default value: `AtMap.Exchange`
User Search Base	Enter the DN in which the search for user accounts is rooted in. This specifies the exact location in the LDAP tree from where the accounts are to be reconciled. If any account does not come under the specified DN, then the account is not reconciled. Default value: `dc=company,dc=com` **Note:** You can also include the organizational unit in the value that you enter for this attribute. For example: `ou=testDisable,dc=company,dc=com`
User Search Scope	Enter the search scope used to locate user accounts. Default value: `subtree`
Submit All Records	Enter `yes` to configure the connector for full reconciliation. Enter `no` to configure the connector for incremental reconciliation. Default value: `no` See "Full Reconciliation vs. Incremental Reconciliation" on page 3-6 for more information about this attribute.
Distribution Group Name	Enter the name of the distribution group from which mailboxes are reconciled. A star symbol denotes that the reconciliation run brings mailboxes from all distribution groups, available with the exchange enabled Microsoft Active Directory server. Default value: `*`
Run Distribution Group Mailbox Recon	Enter `yes` if you want to run mailbox reconciliation from the distribution group. Default value: `no`

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

Attribute	Description
Run Query-Based Distribution Group Mailbox Recon	Enter yes if you want to run mailbox reconciliation from a query-based distribution group. Default value: `no`
Query	Enter the query condition to be used during the reconciliation of the mailboxes. Default value: `(&(mailNickName=*)(objectClass=user))` By default the scheduled task is configured to fetch accounts having mailboxes and mail users. This value is < `(&(homeMDB=*)(objectClass=user))` > if only the mailbox account must be fetched. See "Limited Reconciliation vs. Regular Reconciliation" for more information. **Note:** By default, the value of objectClass is `user`. You can modify this value according to the user's schema on the target system.
Mail Store Name	Enter the name of the mail store from which the mailboxes are to be reconciled. A star symbol denotes that the reconciliation run brings mailboxes from all mail store names, available with the Exchange enabled Microsoft Active Directory server. Default value: `*`
Storage Group Name	Enter the name of the storage group from which the mailboxes are to be reconciled. A star symbol denotes that the reconciliation run brings mailboxes from all storage group names, available with the Exchange enabled Microsoft Active Directory server. Default value: `*`
Mail Store Server Name	Enter the name of the Exchange server from where the mail stores are to be reconciled. A star symbol denotes that the reconciliation run brings mail stores from all mail store server names, available with the Exchange enabled Microsoft Active Directory server. Default value: `*`
AD Server IT Resource	Enter the name of the IT resource for Microsoft Active Directory server. Sample value: `ADITResource`
Reconciliation Type	Enter a value to specify the mode of reconciliation in which the connector is configured. Default value: `MailStoreRecon`
MEXC Timestamp	This attribute stores the date and time when the previous reconciliation run ended. Default value: `0`
Task Scheduler Name	This attribute holds the name of the scheduled task. Value: `Exchange Reconciliation Task` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that scheduled task as the value of the attribute in that scheduled task.
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.Exchange.Configuration` **Note:** You must not change the value of this attribute.

Note: You must enter appropriate values for Reconciliation Type and Run Query-Based Distribution Group Mailbox Recon parameters. If you enter incorrect values, then reconciliation fails and an error message is displayed.

3.4.3.1.1 Configuring Mail Store Reconciliation

You can configure the reconciliation of mailboxes from either all mail stores or from a specific mail store. If you want to configure the reconciliation of mailboxes from a specific mail store, then you must enter the combination of the mail store name, group name, and the server name of that mail store. You can specify one of the following combinations:

- The asterisk (*) in all fields

  This will fetch mailboxes from all mail stores.

- Mail store name, distribution group name, and Exchange server name

If you enter an incorrect combination of values in the mailStoreName, groupName, and serverName fields, then reconciliation fails and a message is displayed stating that the combination of parameters entered is incorrect. The correct combination for this entry is displayed on the server console and also recorded in the log file.

3.4.3.2 Exchange Delete Recon Task

This scheduled task is used to reconcile data about deleted mailboxes. Table 3–4 lists the attributes of this scheduled task.

Note: Delete reconciliation is not supported in Microsoft Exchange 2007.

Table 3–4 Attributes of the Exchange Delete Recon Task Scheduled Task

Attribute	Description
User Search Base	The DN in which the search for user accounts is rooted in. Default value: `dc=company,dc=com` **Note:** You can also include the organizational unit in the value that you enter for this attribute. For example: `ou=testDisable,dc=company,dc=com`
User Search Scope	Enter the search scope used to locate user accounts. Default value: `subtree`
Task Scheduler Name	Enter the name of the scheduled task for delete reconciliation. Default value: `Exchange Delete Recon Task`
AD Server IT Resource	Enter the name of the IT resource for Microsoft Active Directory server. Sample value: `ADITResource`
Target Resource Object	Enter the name of the Microsoft Exchange resource object to be created. This is a user configurable name. Default value: `Exchange`

Table 3–4 (Cont.) Attributes of the Exchange Delete Recon Task Scheduled Task

Attribute	Description
MEXC_Timestamp	This attribute stores the date and time when the previous reconciliation run started for mailboxes. This timestamp is used for delete reconciliation. Default value: `0`
Query	Enter the query condition to be used during the reconciliation of the mailboxes. Default value: `(objectClass=user)` **Note:** By default, the value of objectClass is `user`. You can modify this value according to the user's schema on the target system.
Recon Attribute Lookup Code Name	Enter the name of the lookup table containing the mapping for the Exchange attributes. You are not allowed to delete attributes from this table. Default value: `AtMap.Exchange`
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.Exchange.Configuration` **Note:** You must not change the value of this attribute.

Note: Each attribute of a scheduled task must have a value. For some attributes, you can either enter a value or accept the default value. For the rest, you must accept the default value. If even a single attribute value is left empty, then reconciliation is not performed.

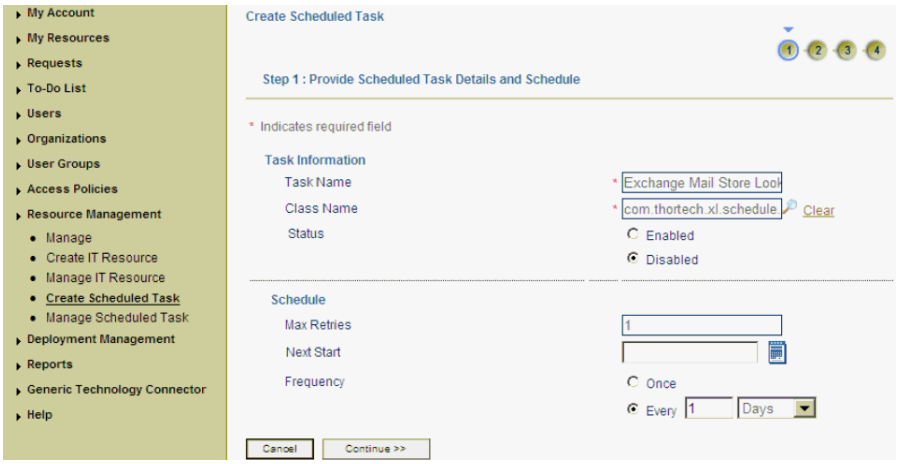
3.4.4 Creating the Reconciliation Scheduled Task (Optional)

You can use the Exchange Reconciliation Task scheduled task to perform different types of reconciliation. If you use the same scheduled task for all the reconciliation types, you must change the value for the reconciliation type, every time you run the scheduled task. Alternatively, you can create a different scheduled task for each reconciliation type by creating a copy of the existing scheduled task. See "Types of Reconciliation Enabled by the Connector" on page 1-6 for more information about the types of reconciliation supported by the connector.

To create a copy of the scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Expand **Resource Management**.
3. Select **Create Scheduled Task.**
4. On the Step 1: Provide Scheduled Task Details and Schedule page, enter the following information:
   - In the **Task Name** field, enter the name of the scheduled task, for example, `Exchange Mail Store Lookup Reconciliation`.
   - In the **Class Name** field, enter the class name of the scheduled task, whose copy you are creating. Figure 3–1 shows the scheduled task created in the Create Scheduled Task page.

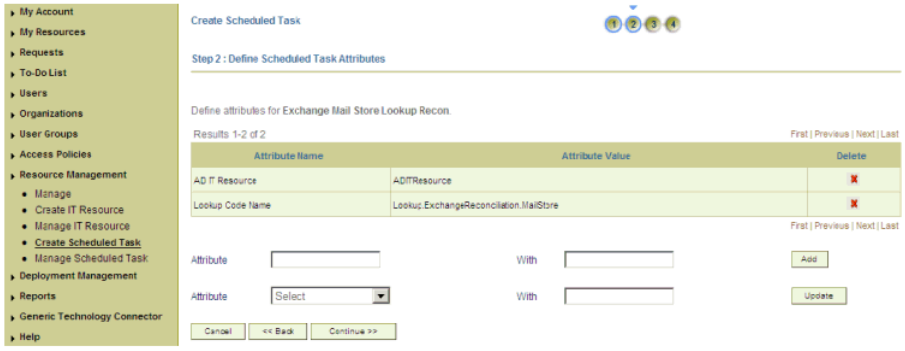
Figure 3–1 Step 1: Provide Scheduled Task Details and Schedule



5. Click **Continue.**

6. On the Step 2: Define Scheduled Task Attributes page, in the **Task Attributes** section, enter the attributes of the scheduled task whose copy you are creating, specify values for the attributes, and click **Add**. Figure 3–2 shows the attributes fields in the Create Scheduled Task page.

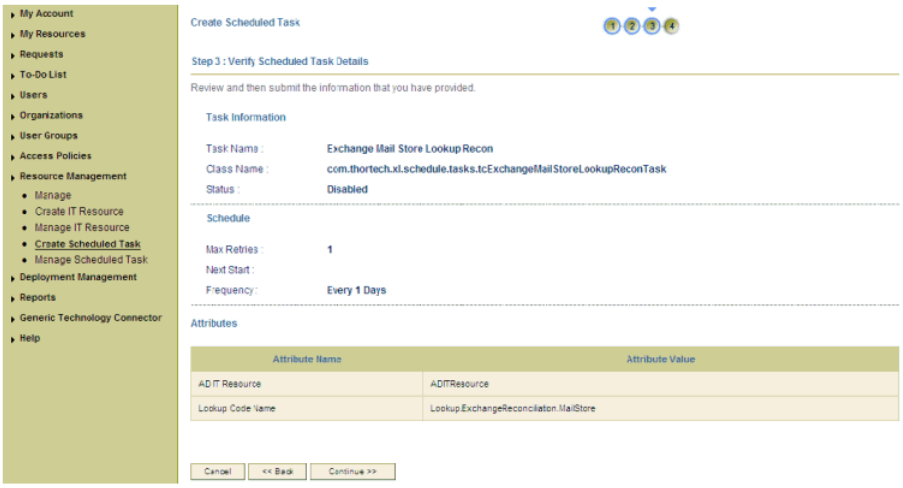
Figure 3–2 Step 2: Define Scheduled Task Attributes



7. Click **Continue.**

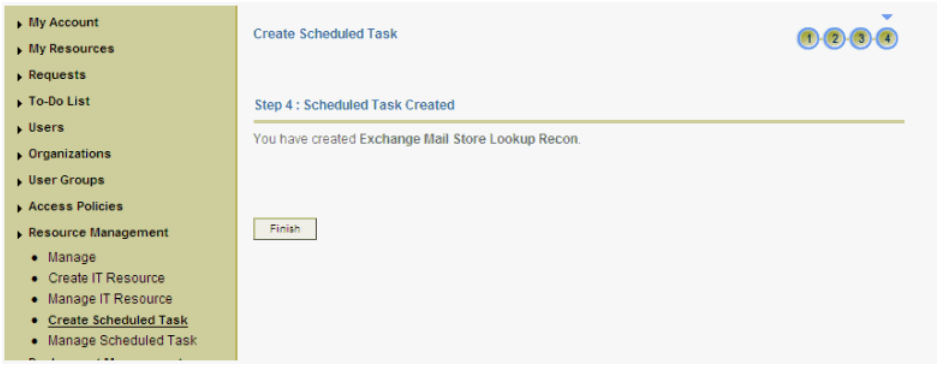
8. On the Step 3: Verify Scheduled Task Details page, review the information that you have entered and then click **Continue** to proceed. Figure 3–3 shows the details of the scheduled task that is created in the Create Scheduled Task page.

Figure 3–3 Step 3: Verify Scheduled Task Details



9. The Step 4: Scheduled Task Created page displays a message specifying the successful creation of the scheduled task. Figure 3–4 shows the success message for creation of the scheduled task in the Create Scheduled Task page.

Figure 3–4 Step 4: Scheduled Task Created



3.5 Configuring Scheduled Tasks

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

Table 3–5 lists the scheduled tasks that you must configure.

Table 3–5 Scheduled Tasks

Scheduled Task Name	Description
Exchange Mail Store Lookup Reconciliation	This scheduled task is used to synchronize the values of mail stores between the target system and Oracle Identity Manager. For information about this scheduled task and its attributes, see "Scheduled Task for Lookup Field Synchronization" on page 3-4.
Exchange Reconciliation Task	This scheduled task is used to reconcile mailbox related data. For information about this scheduled task and its attributes, see "Exchange Reconciliation Task" on page 3-7.

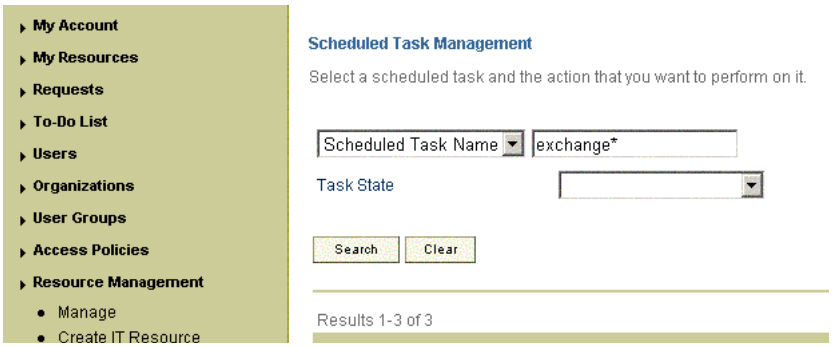
Table 3–5 (Cont.) Scheduled Tasks

Scheduled Task Name	Description
Exchange Delete Recon Task	This scheduled task is used to reconcile data about deleted mailboxes. For information about this scheduled task and its attributes, see "Exchange Delete Recon Task" on page 3-9.

To configure a scheduled task:

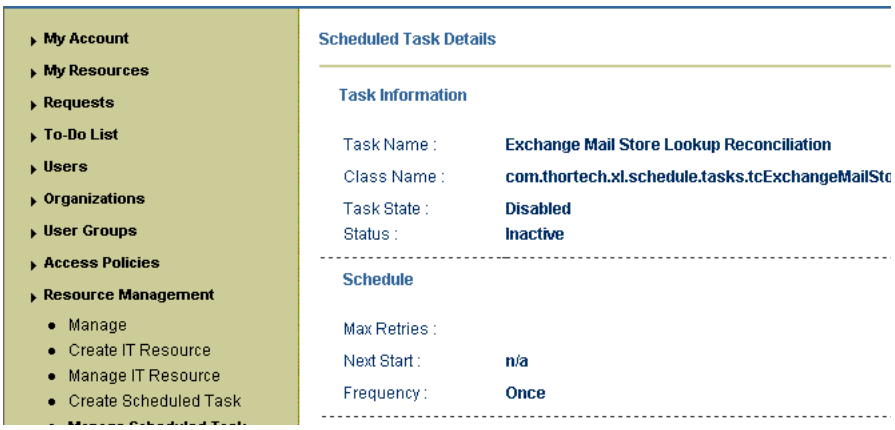
1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
5. In the search results table, click the edit icon in the Edit column for the scheduled task. Figure 3–5 shows the search results for the scheduled task name in the Scheduled Task Management page.

Figure 3–5 Select Scheduled Task



6. In the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**. Figure 3–6 shows the details of the scheduled task that you selected in the Scheduled Task Details page.

Figure 3–6 Edit Scheduled Task



7. In the Edit Scheduled Task page, modify the following details of the scheduled task and click **Continue**.

- **Status:** Specify whether or not you want to leave the task in the enabled state after it is created. In the enabled state, the task is ready for use. If the task is disabled, then you must enable it before you can use it.
- **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.

Figure 3–7, shows Status, Max Retries, Next Start, and Frequency field details that you can modify in the Edit Scheduled Task page.

Figure 3–7 Modify Scheduled Task Details

8. In the Attributes page, specify the values for the attributes of the scheduled task. To do so, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**. Figure 3–8 shows the attribute details in the Attributes page.

Figure 3–8 Specify Attribute Value

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 is left empty, then reconciliation is not performed.
- Reconciliation can be run in partial mode or in custom mode depending on values configured for the `Query` scheduled task attribute.
- Reconciliation type depends on the MEXC Timestamp and Submit All Records attributes. If the value for Submit All Records is yes, then all mail boxes are fetched from the target system regardless of the value of the MEXC Timestamp attribute.

9. Click **Save Changes** to commit all the changes to the database.

Note: If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See the "The Task Scheduler Form" section in *Oracle Identity Manager Design Console Guide* for information about this feature.

3.6 Configuring Provisioning

This section discusses the following topics:

- Using the Connector for Provisioning
- Performing Provisioning Operations

3.6.1 Using the Connector for Provisioning

Apply the following guideline when you start using the connector for provisioning operations:

Before you provision the Microsoft Exchange resource object to a user, ensure that the user has an account in Microsoft Active Directory. If the user does not have a Microsoft Active Directory account, then the provisioning operation fails.

To create a Microsoft Active Directory account for the user, you can follow one of the following approaches:

- In Oracle Identity Manager, provision the Microsoft Active Directory resource object to the user.
- Manually create an account in Microsoft Active Directory for the user.

Note: Mail redirection function can be set during Microsoft Active Directory provisioning. If mail redirection is set, then there is no need to provision Microsoft Exchange resource object. Provisioning is not required as mails are not physically stored in the mailbox, but are redirected on receipt.

3.6.2 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a Microsoft Exchange account for the user. The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

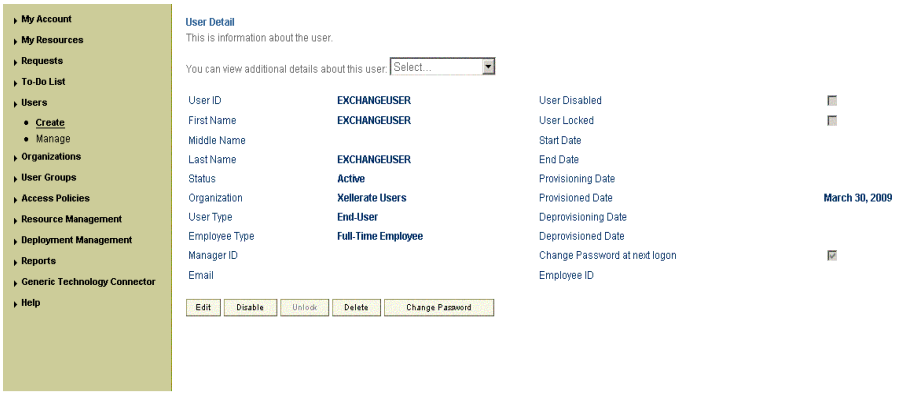
> **See Also:** *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

To provision a resource by using the direct provisioning approach:

> **Note:** Before you provision a Microsoft Exchange resource, ensure that a Microsoft Active Directory resource is already provisioned.
>
> If the Allow Multiple check box of the resource object is selected, then you can provision more than one mailbox for an OIM User. However, the target system supports only one mailbox for each user.

1. Log in to the Administrative and User Console.
2. From the Users menu:
   - Select **Create** if you want to first create the OIM User, provision a Microsoft Active Directory user, and then provision a Microsoft Exchange mailbox to the user.
   - Select **Manage** if you want to provision a Microsoft Exchange mailbox to an existing OIM User.
3. If you select Create, on the Create User page, enter values for the OIM User fields, and then click **Create User.**
4. If you select Manage, then search for the OIM User and select the link for the user from list of users displayed in the search results.
5. In the User Detail page, select **Resource Profile** from the list at the top of the page. Figure 3–9 shows the details of the user that you created in the User Detail page.

Figure 3–9 Select Resource Profile

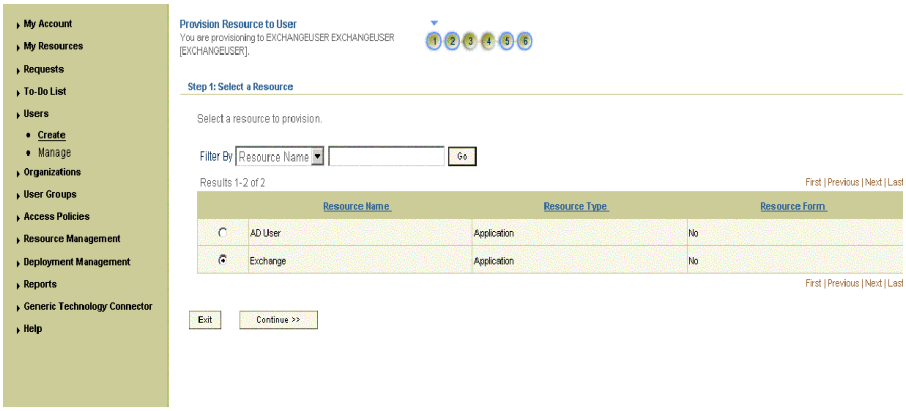


6. In the Resource Profile page, click **Provision New Resource.** Figure 3–10 shows the resource name that you provision in the User Detail Resource Profile page.

Figure 3–10 Provision New Resource

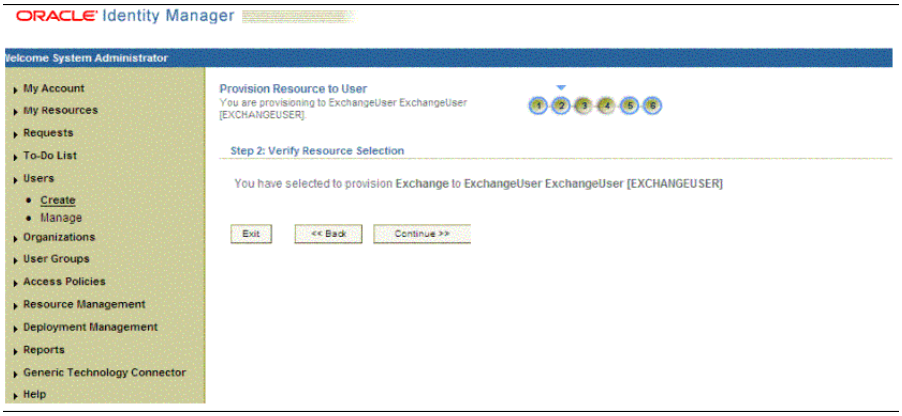
7. In the Provision Resource to User page, select **Exchange** from the list, and then click **Continue.** Figure 3–11 shows Exchange resource selected to provision in the Provision Resource to User page.

Figure 3–11 Step 1: Select a Resource



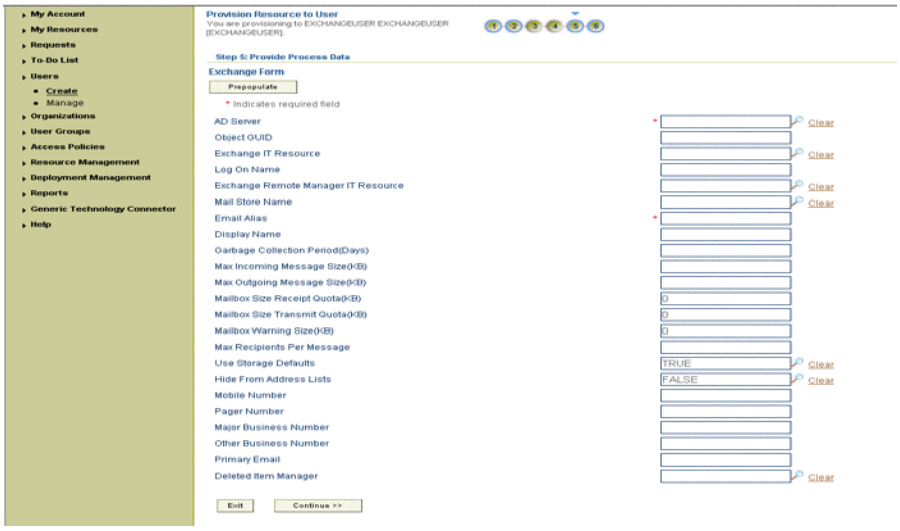
8. In the Provision Resource to User page, click **Continue.** Figure 3–12 shows the resource name selected for provisioning to the Exchange User in the Provision Resource to User page.

Figure 3–12 Step 2: Verify Resource Selection



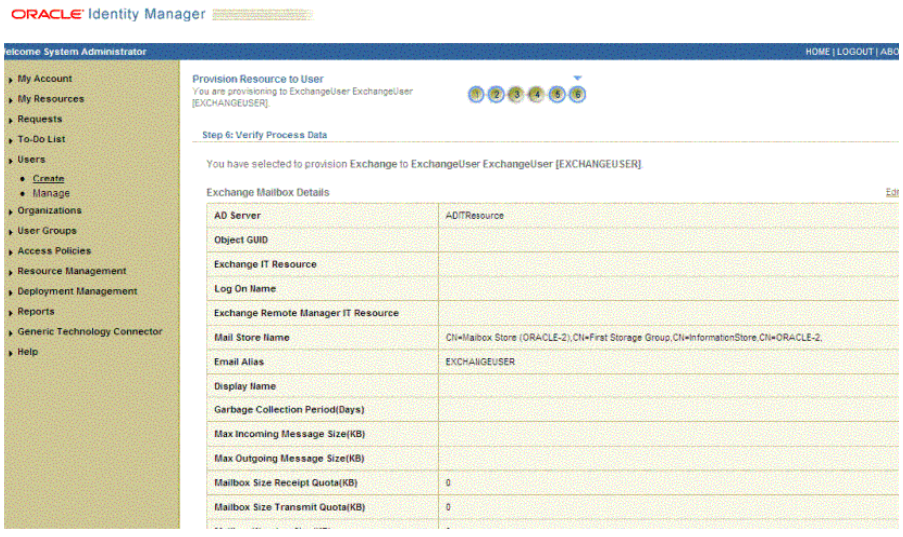
9. In the Provision Resource to User page, enter the details of the mailbox that you want to create on the target system and then click **Continue.** Figure 3–13 shows the details of the mailbox name that is provisioned to the Exchange User in the Provision Resource to User page.

Figure 3–13 Step 5: Provide Process Data



10. In the Provision Resource to User page, verify the data that you entered and then click **Continue.** Figure 3–14 shows the details of the process data you created in the Provision Resource to User page.

Figure 3–14 Step 6: Verify Process Data



The mailbox is created on the target system and provisioned as a resource to the OIM User. The page that is displayed provides options to disable or revoke the resource from the OIM User.

4

Extending the Functionality of the Connector

This chapter describes procedures that you can perform to modify the connector for addressing your specific business requirements.

This chapter discusses the following optional procedures:

Note: These procedures are aimed at extending the functionality of the connector:

- The "Modifying Existing Field Mappings" section described the procedure to modify the mappings between fields of the target system and Oracle Identity Manager.
- The "Adding New Fields for Target Resource Reconciliation" section describes the procedure to add mappings between fields of the target system and Oracle Identity Manager
- The "Adding New Fields for Provisioning" section describes the procedure to add mappings between fields of the target system and Oracle Identity Manager.
- The "Configuring the Connector for Multiple Installations of the Target System" section describes the procedure to configure the connector for multiple installations of the target system.

4.1 Modifying Existing Field Mappings

Default mappings between fields of the target system and Oracle Identity Manager are listed in the following sections:

- "Mailbox Fields for Target Resource Reconciliation" on page 1-7
- "Mailbox Fields for Provisioning" on page 1-11

If you want to modify these mappings, then:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the lookup definition that you want to modify.

   Table 4–1 describes the contents of the lookup definition that contains field mapping information for reconciliation and provisioning.

Table 4–1 Lookup Definitions That Store Field Mapping Information

Lookup Definition	Contents of the Code Key Column	Contents of the Decode Column
Lookup.Exchange.Configuration This is used during reconciliation and provisioning.	Names of fields on Microsoft Active Directory	Names of process form fields for Microsoft Active Directory
AtMap.Exchange This is used during provisioning.	Names of Microsoft Exchange fields on Microsoft Active Directory	Names of process form fields for Microsoft Exchange

4. Make the required change in the field mappings by modifying the Code Key and Decode values.

   For example, you can change the Code Key value for distinguishedName to sAMAccountName.

5. Click the save icon.

4.2 Adding New Fields for Target Resource Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to add new fields for target resource reconciliation.

By default, the fields listed in Table 1–3, " Mailbox Fields for Target Resource Reconciliation" are mapped for reconciliation between the target system and Oracle Identity Manager. If required, you can add new fields for target resource reconciliation.

Before you add a new field for target resource reconciliation, you must first determine the target system name of the field as follows:

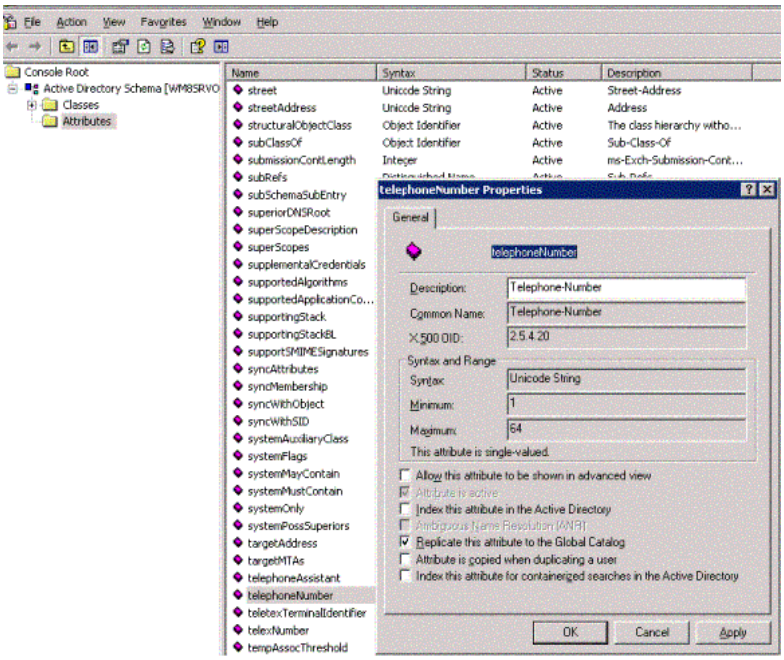
1. Install the Microsoft Active Directory schema, if it is not already installed.

   Refer to the Microsoft Web site for information about installing the schema.

2. Open the Microsoft Active Directory schema.
3. Expand the **Console Root** folder, expand the schema, and then click **Attributes**.
4. Search for the field that you want to add, and then note down its name.

   For example, if you want to add the Telephone Number field for reconciliation, then note down telephoneNumber. Figure 4–1 shows the Telephone Number field added in the telephoneNumber Properties dialog box.

Figure 4–1 New Field Added for Reconciliation

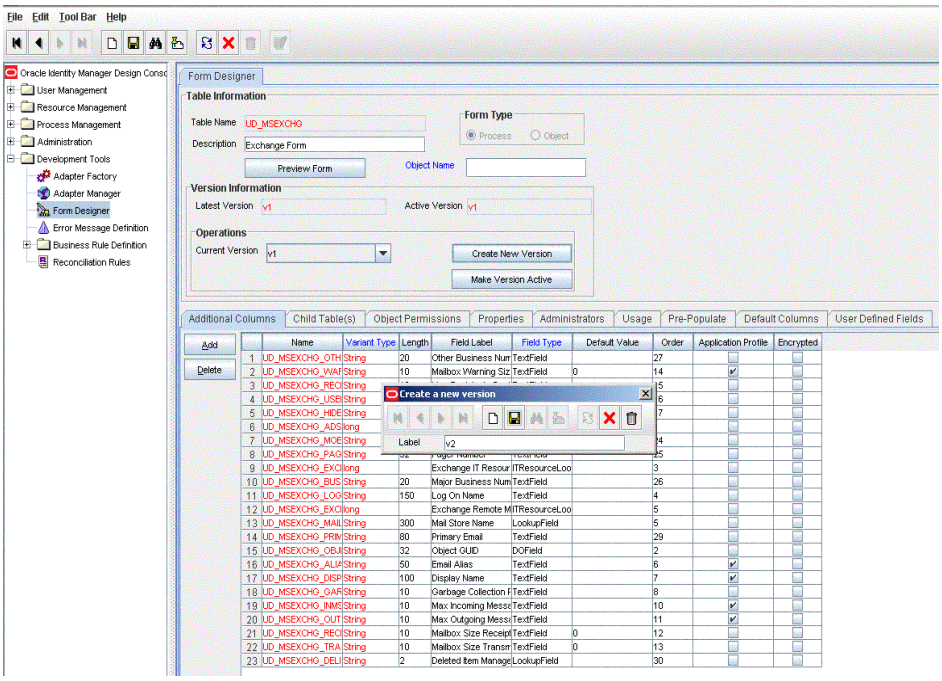


To add a new field for target resource reconciliation:

> **See Also:** *Oracle Identity Manager Design Console Guide for detailed information about these steps*

1. Log in to the Oracle Identity Manager Design Console.
2. Create a new version of the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Search for and open the **UD_MSEXCHG** process form.
   d. Click **Create New Version**. On the Create a new version dialog box, enter a new version in the Label field, and then click the **Save** icon. Figure 4–2 shows the new version of the form created in the process form.

Figure 4–2 New Version of Process Form



3. Add the new field on the process form as follows:

   a. Click **Add**. A field is added to the list. Enter the details of the field.

      For example, if you are adding the Telephone Number field, enter `UD_MSEXCHG_TELEPHONE_NUMBER` in the **Name** field and then enter the rest of the details of this field.

   b. Click **Save**.

   c. To activate the newly created form, click **Make Version Active.** Figure 4–3 shows details of the new field added in the process form.

Figure 4–3 New Field Added to the Process Form

Additional Columns | Child Table(s) | Object Permissions | Properties | Administrators | Usage | Pre-Populate

Add / Delete

	Name	Variant Type	Length	Field Label	Field Type
1	UD_MSEXCHG_OTHERNUMBER	String	20	Other Business Number	TextField
2	UD_MSEXCHG_WARNSIZE	String	10	Mailbox Warning Size(KB)	TextField
3	UD_MSEXCHG_RECIPLIMIT	String	10	Max Recipients Per Message	TextField
4	UD_MSEXCHG_USEDEFAULTS	String	5	Use Storage Defaults	LookupField
5	UD_MSEXCHG_HIDEFROMADDRLISTS	String	5	Hide From Address Lists	LookupField
6	UD_MSEXCHG_ADSERVER	long		AD Server	ITResourceLoo
7	UD_MSEXCHG_MOBILE	String	20	Mobile Number	TextField
8	UD_MSEXCHG_PAGER	String	32	Pager Number	TextField
9	UD_MSEXCHG_EXCHANGEITRESOURCE	long		Exchange IT Resource	ITResourceLoo
10	UD_MSEXCHG_BUSINESS	String	20	Major Business Number	TextField
11	UD_MSEXCHG_LOGONNAME	String	150	Log On Name	TextField
12	UD_MSEXCHG_EXCHREMOTEMANAGER	long		Exchange Remote Manager IT Resource	ITResourceLoo
13	UD_MSEXCHG_MAILSTORENAME	String	300	Mail Store Name	LookupField
14	UD_MSEXCHG_PRIMARYEMAIL	String	80	Primary Email	TextField
15	UD_MSEXCHG_OBJECTGUID	String	32	Object GUID	DOField
16	UD_MSEXCHG_ALIAS	String	50	Email Alias	TextField
17	UD_MSEXCHG_DISPLAYNAME	String	100	Display Name	TextField
18	UD_MSEXCHG_GARBAGECOLL	String	10	Garbage Collection Period(Days)	TextField

4. Add the new field to the list of reconciliation fields in the resource object as follows:

   a. Expand **Resource Management.**

b. Double-click **Resource Objects.**

c. Search for and open the **Exchange User** resource object.

d. On the Object Reconciliation tab, click **Add Field.**

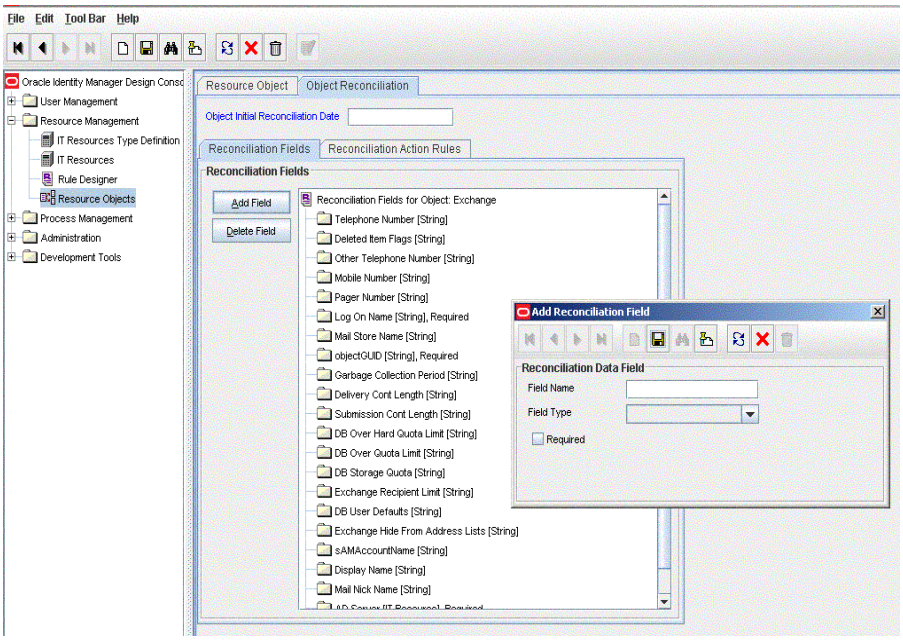
e. In the Add Reconciliation Field dialog box, enter the details of this field.

For example, enter `Telephone Number` in the **Field Name** field and select **String** from the Field Type list.

Later in this procedure, you will enter the field name as the Decode value of the entry that you create in the lookup definition for reconciliation.

f. Click **Save**. Figure 4–4 shows the new reconciliation field added to the resource object in the process form.

Figure 4–4 New Field Added to the Resource Object



5. Create a reconciliation field mapping for the new field on the process form as follows:

a. Expand **Process Management.**

b. Double-click **Process Definition.**

c. From the Process Definition table, select and open the **Exchange User** resource object.

d. Click **Reconciliation Field Mappings** and then click **Add Field Map.**

e. In the Field Name field, select the value for the field that you want to add.

For example, select `Telephone Number`.

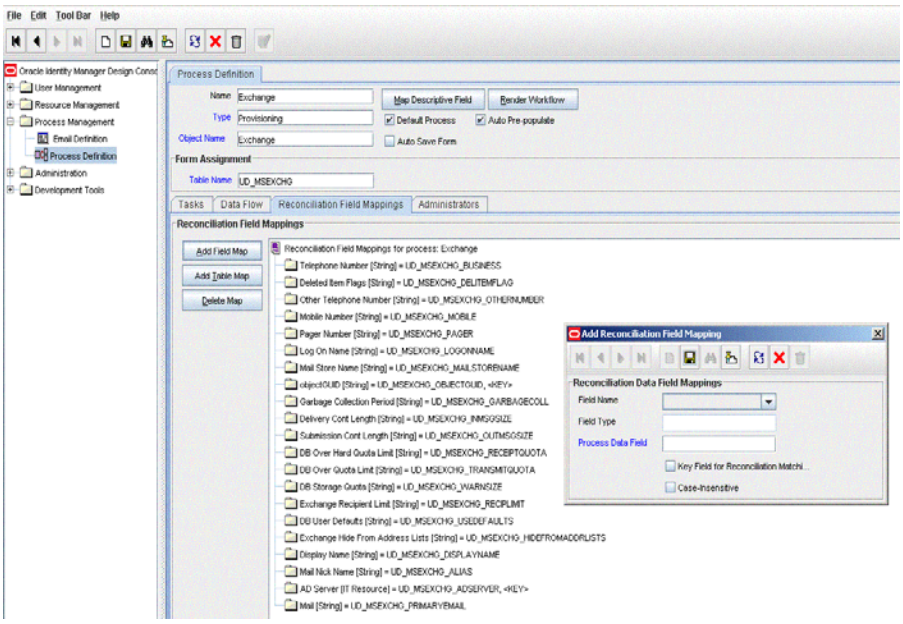
f. In the **Field Type** field, select the type of the field that is prepopulated.

g. Double-click the **Process Data Field** field. A list of process data columns is displayed. From the list, select the process data column corresponding to the process data field.

For example, select `Telephone Number = UD_EXCHANGEUSER_TELEPHONE_NUMBER`.

h. Click the **Save** icon. Figure 4–5 shows the mapping of new reconciliation field to the Process Data Field in the process form.

Figure 4–5 Reconciliation Field Mappings



6. Create an entry for the field in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

   b. Double-click **Lookup Definition.**

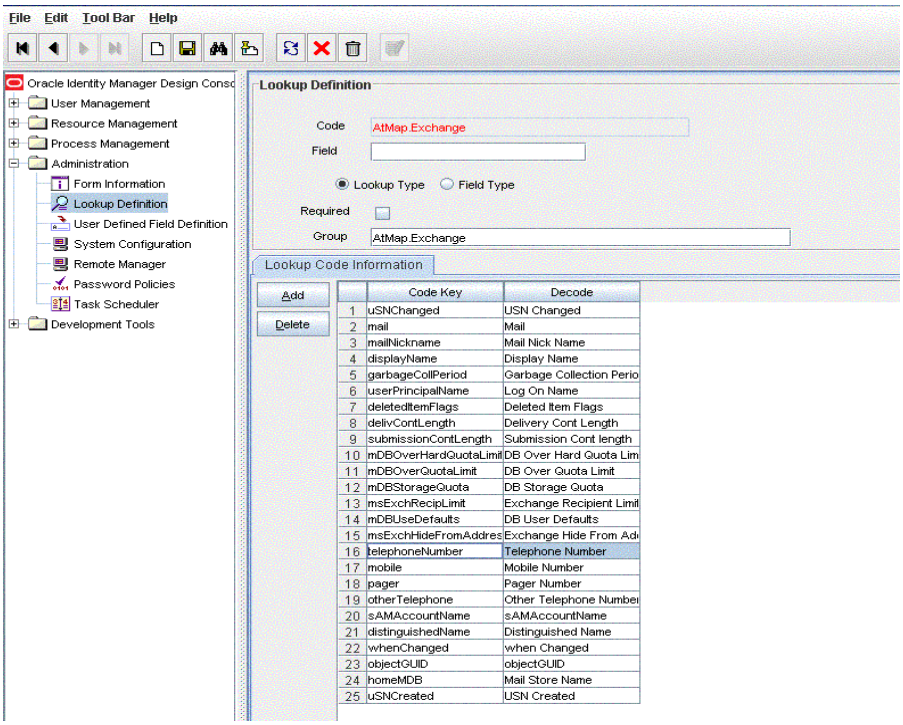
   c. Search for and open the **AtMap.Exchange** lookup definition.

   d. Click **Add** and enter the Code Key and Decode values for the field. The Code Key value must be the name of the field on the target system, which you determined at the start of this procedure.

      For example, enter `telephoneNumber` in the **Code Key** field and then enter Telephone Number in the **Decode** field.

   e. Click **Save**. Figure 4–6 shows the code key and the decode value added to the lookup definition in the process form.

Figure 4–6 AtMap.Exchange Lookup Definition



4.3 Adding New Fields for Provisioning

Note: This section describes an optional procedure. Perform this procedure only if you want to add new fields for provisioning

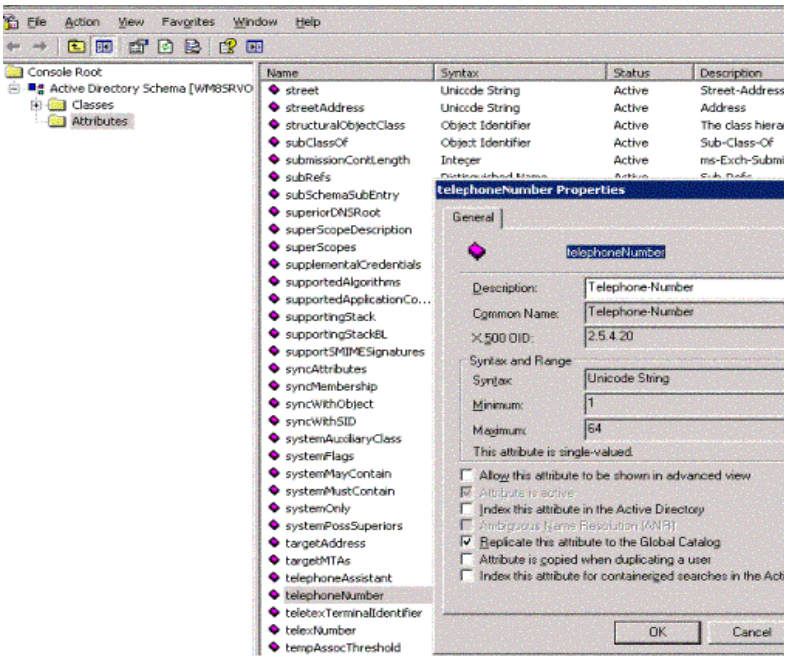
By default, the fields listed in Table 1–6, " Mailbox Fields Used in Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional fields for provisioning.

Before you add a new field for provisioning, you must first determine the name of the field from the Microsoft Active Directory schema as follows:

1. Log in to Microsoft Active Directory.
2. Open the Microsoft Active Directory schema.
3. Expand the **Console Root** folder, expand the schema, and then click **Attributes**.
4. Search for the field that you want to add, and then note down its name.

   For example, if you want to add the Telephone Number field for reconciliation, then note down telephoneNumber. Figure 4–7 shows the Telephone Number added in the telphoneNumber Properties dialog box.

Figure 4–7 New Field Added for Provisioning

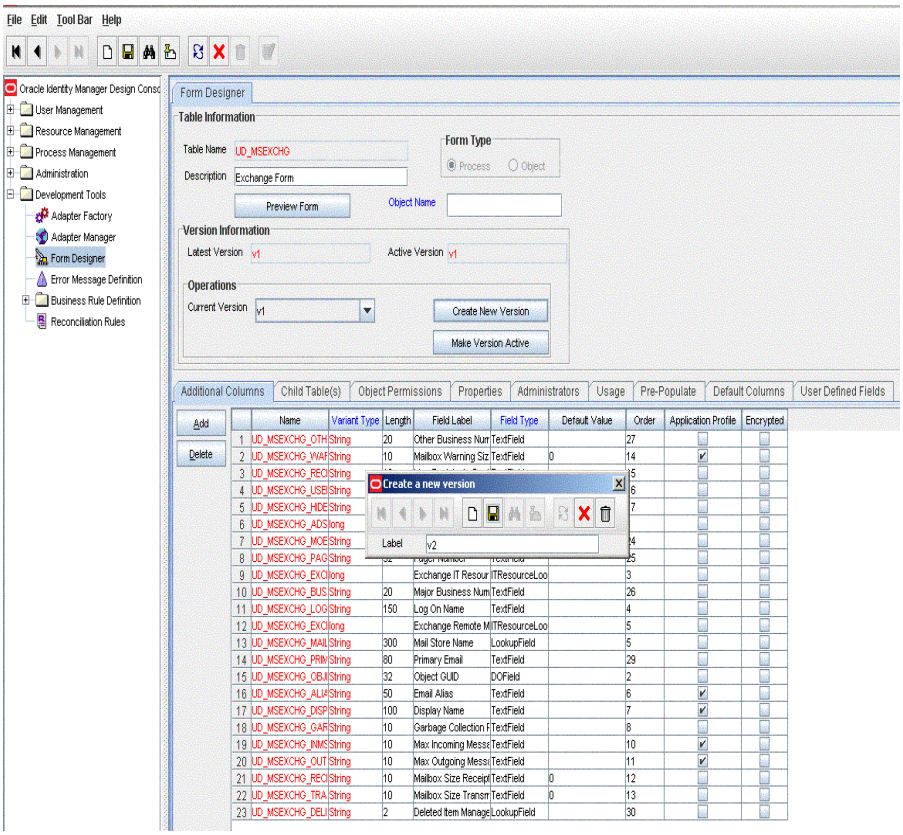


To add a new field for provisioning:

> **See Also:** *Oracle Identity Manager Design Console Guide for detailed information about these steps*

1. Log into Oracle Identity Manager Design Console.
2. Create a new version of the process form:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Search for and open the **UD_MSEXCHG** process form.
   d. Click **Create New Version**. On the Create a new version dialog box, enter a new version in the Label field, and then click the **Save** icon. Figure 4–8 shows the new version form created in the process form.

Figure 4–8 New Version Created in the Process Form



3. Add the new field on the process form.

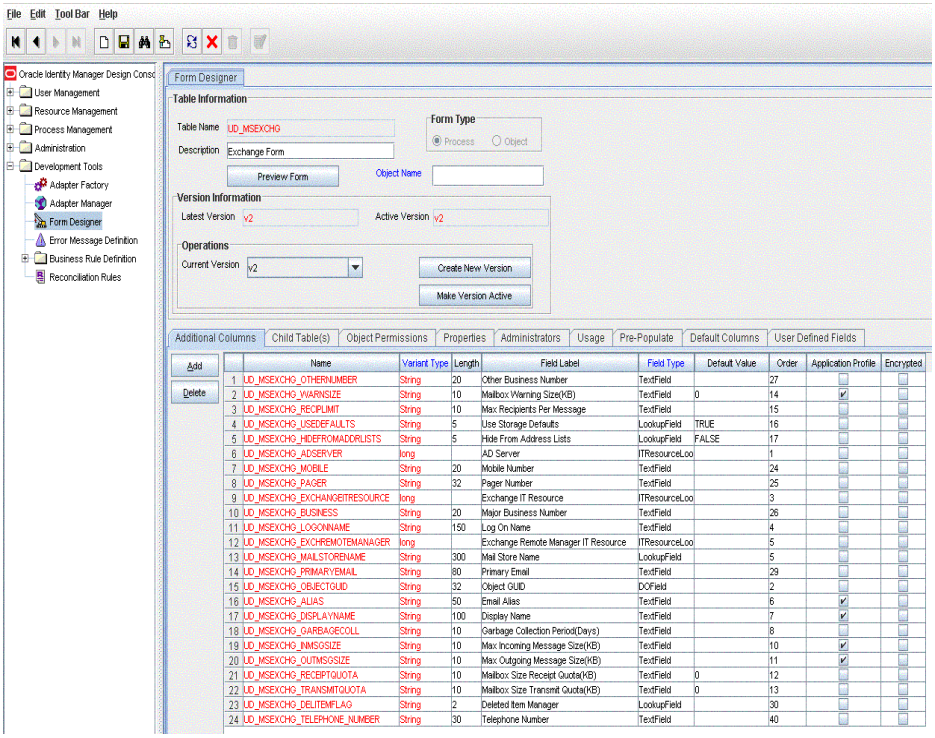
   If you have added the field on the process form by performing Step 3 of "Adding New Fields for Target Resource Reconciliation" on page 4-2, then you need not add the field again. If you have not added the field, then:

   a. Click **Add**. A field is added to the list. Enter the details of the field.

      For example, if you are adding the Telephone Number field, enter `UD_MSEXCHG_TELEPHONE_NUMBER` in the **Name** field and then enter the rest of the details of this field.

   b. Click **Save** and then click **Make Version Active.** Figure 4–9 shows the new field added in the process form.

Figure 4–9 New Field Added in the Process Form



4. Create a new variable in the Adapter Factory section:

   a. Expand **Development Tools**.

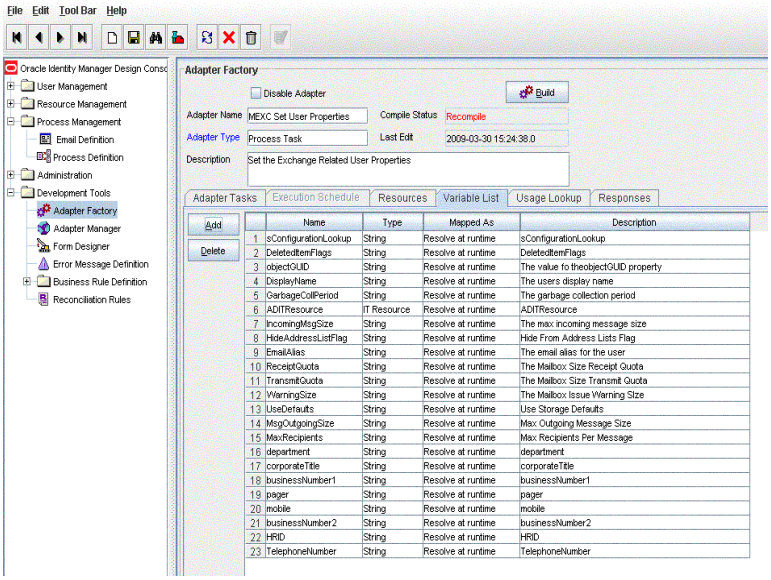
   b. Click **Adapter Factory** and query to get all adapters. The adapter factory table is displayed.

   c. Double-click **MEXC Set User Properties.**

      Navigate to the **Variable List** tab, click **Add**, and create a new variable corresponding to the value that you want to provision.

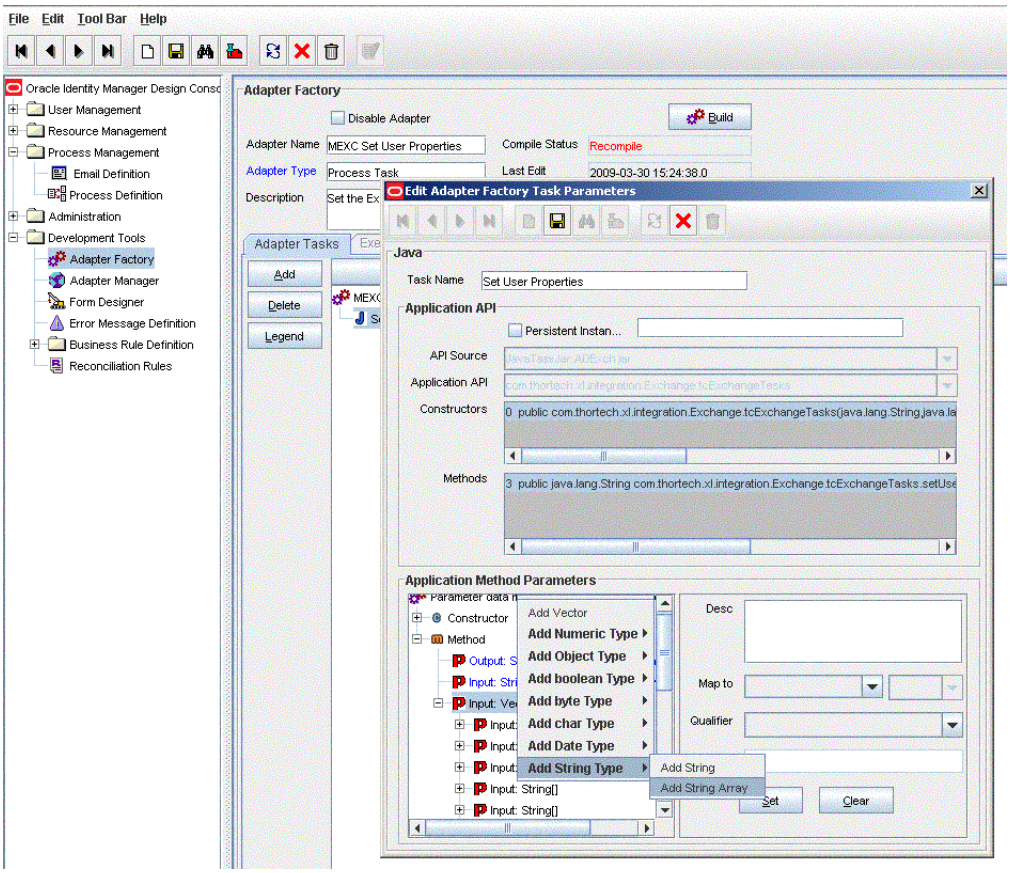
      Click **Save**. Figure 4–10 shows the new variable added in the process form.

Figure 4–10 New Variable Added in the Process Form



5. Add string array to the vector:
   a. In the Adapters Task tab, double-click **Set User Properties**.
   b. Expand the method and right-click **Input: Vector**.
   c. Select **Add String Type** and then select **Add String Array.** A new string array item is added at the end of the vector.
   d. Right-click **Input: String[ ]**, select **Add String** and then add two strings.
   e. Click **Save**. Figure 4–11 shows the string array added to the vector in the process form.

Figure 4–11 String Array Added to the Vector

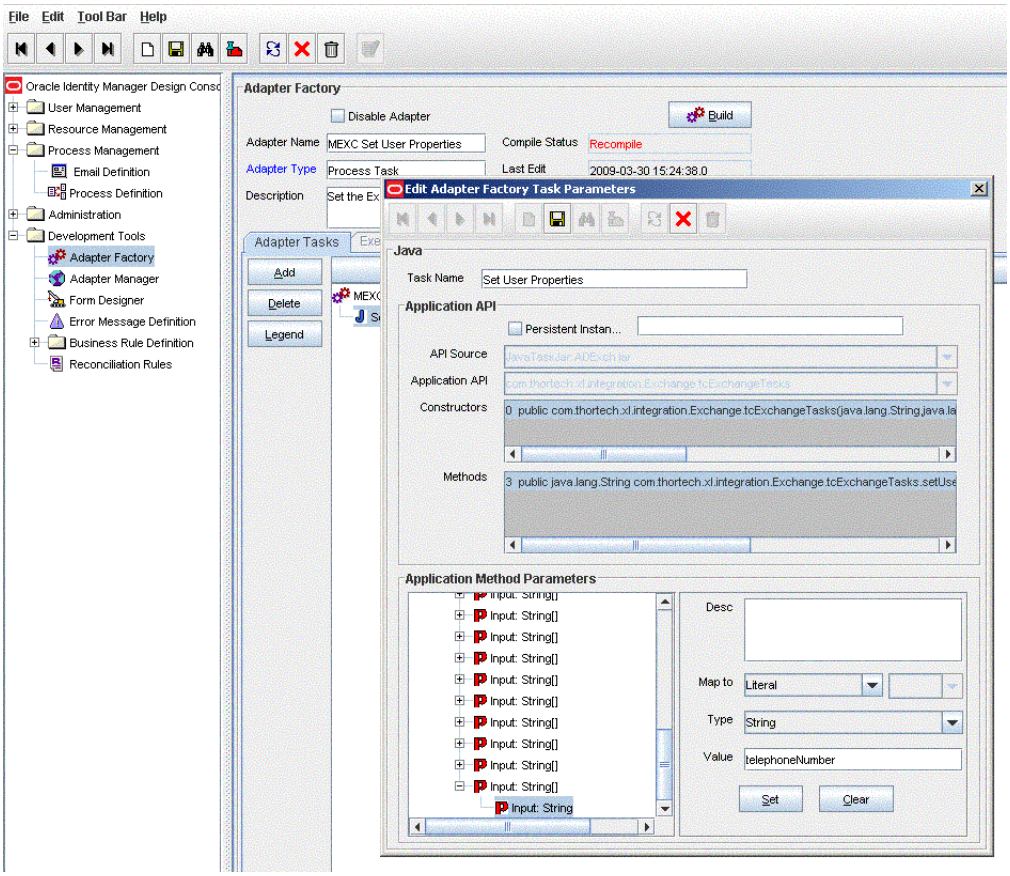


6. Map the string:

   a. Map the first item to a literal. The value of the literal should be the attribute value on the target system.

   b. Click **Save**. Figure 4–12 shows the string mapped to a literal in the process form.

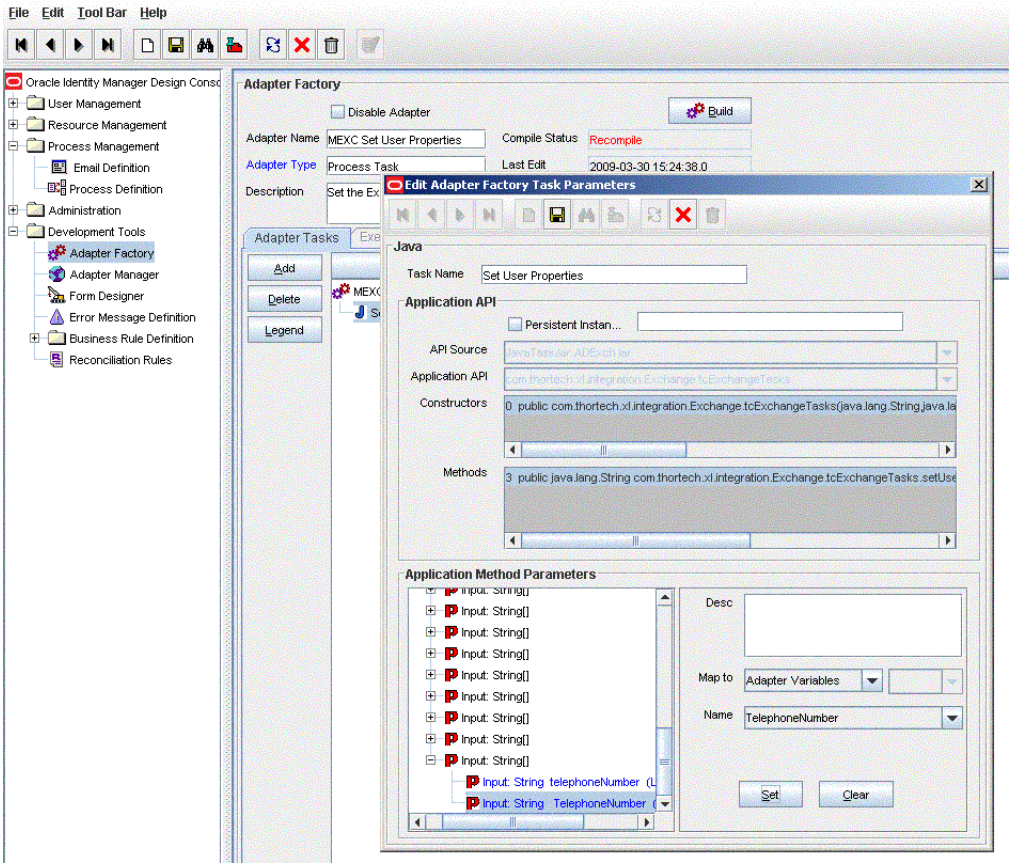
Figure 4–12 String Mapped to Literal



c. Map the second item to the corresponding adapter variable:

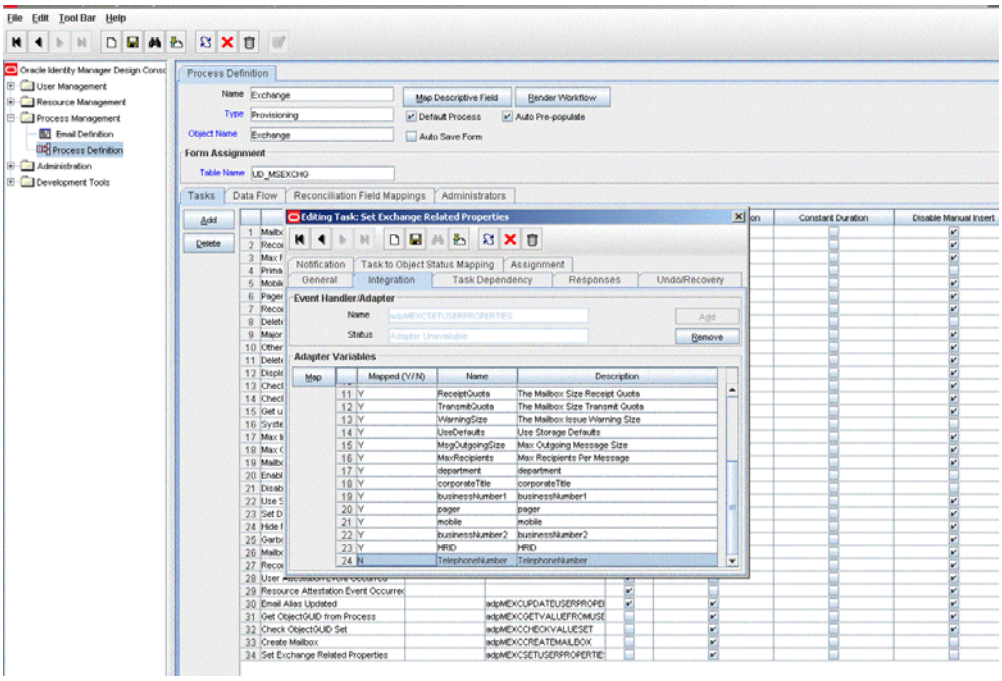
d. Click **Save.** Figure 4–13 shows the string mapped to the adapter variable in the process form.

Figure 4–13 String Mapped to Adapter Variable



7. Map the variable to process data:
   a. Expand **Process Management**.
   b. Double-click **Process Definition**.
   c. Select **Set the Exchange Related User Properties**.
   d. Double-click **Process Task** and navigate to the **Integration** tab. The newly mapped variable will have the mapped status as N. Figure 4–14 shows the newly mapped variable in the process definition.

Figure 4–14 Mapped Variable in Process Definition

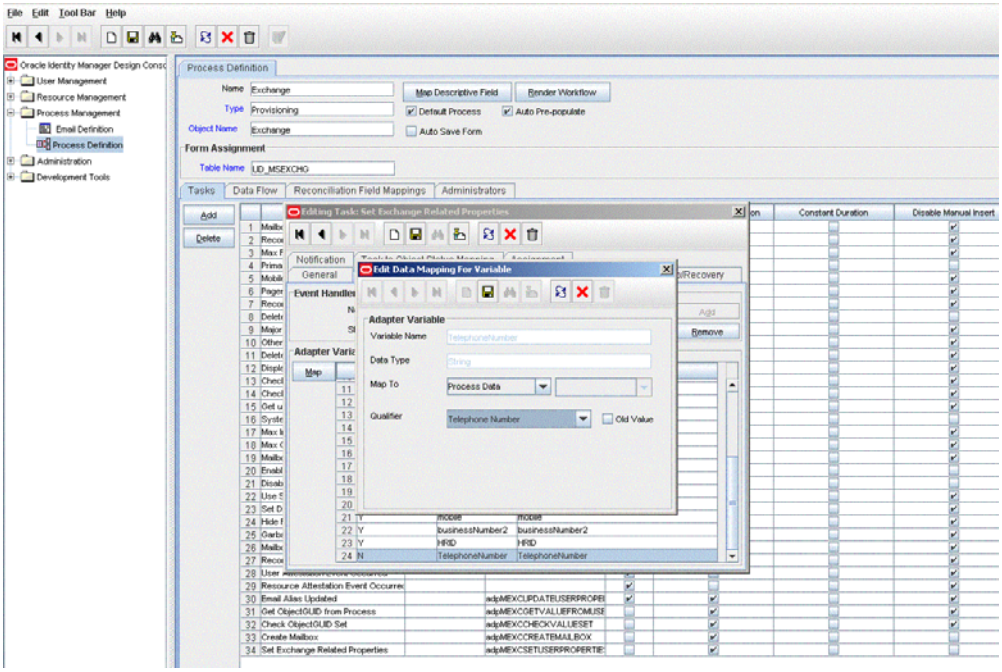


e. In the Map To field, select **Process Data**.

f. In the **Qualifier** field, select the name of the form label, which you have entered in the form.

g. Click **Save**. Figure 4–15 shows the adapter variable mapped to the process data field.

Figure 4–15 Variable Mapped to Process Data Field



4.4 Configuring the Connector for Multiple Installations of the Target System

Note: This section describes an optional procedure. Perform this procedure only if you want to configure the connector for multiple installations of the target system.

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

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

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

To configure the connector for multiple installations of the target system:

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

1. Create and configure one IT resource for each target system installation.

   The IT Resources form is in the Resource Management folder. An IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same IT resource type. For information about the procedure to create an IT resource, see "Creating the IT Resource" on page 2-6.

2. Create copies of the reconciliation scheduled tasks for each installation of the target system. While creating a scheduled task, specify attribute values corresponding to the target system installation for which you are creating the scheduled task.

   Refer to "Reconciliation Scheduled Tasks" on page 3-7 for information about the values to be specified for the scheduled task attributes.

3. Manually synchronize the lookup definitions in Oracle Identity Manager with the lookup field values on the target system.

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

4.4.1 Creating Copies of the Connector

To create a copy of the connector:

1. Create copies of the IT resource, resource object, process form, provisioning process, scheduled tasks, and lookup definitions that hold attribute mappings.
2. Create a copy of the Lookup.Exchange.Configuration lookup definition. In the copy that you create, change the values of the following entries to match the details of the process form copy that you create.
   - ROExgInMsgSizeCol

- ROExgOutMsgSizeCol

See "Configuring the Lookup.Exchange.Configuration Lookup Definition" for information about these entries.

3. Map the new process tasks to the copy of the Lookup.Exchange.Configuration lookup definition.
4. If you have create a copy of the Lookup.AD.Configuration, then you must enter the name of the copy in the AD Configuration Lookup Code Key of the Lookup.Exchange.Configuration lookup definition.

5

Known Issues

The following is a known issue associated with this release of the connector:

- **Bug 7207232**

  Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

A

Special Characters Supported for Alias Name

Table A–1 lists the special characters supported by Oracle Identity Manager and Microsoft Exchange 2007 for the Alias Name field. You can use these characters in combination with letters (alphabets) and digits from 0 to 9 while creating the user on the target system.

Note: Microsoft Exchange 2000 and Microsoft Exchange 2003 supports any character.

Table A–1 Special Characters That Can Be Used in the Alias Name Field

Name of the Character	Character
exclamation point	!
number sign	#
dollar sign	$
percent sign	%
ampersand	&
single quotation mark	'
asterisk	*
plus sign	+
dash	_
slash	/
equal to sign	=
question mark	?
caret	^
underscore	_
comma	.
left brace	{
vertical bar	|
right brace	}
tilde	~

Index

T

X