

# Oracle® Identity Manager

## Connector Guide for Microsoft Exchange



11.1.1  
E27258-26  
July 2020

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2014, 2020, Oracle and/or its affiliates.

Primary Author: Alankrita Prakash

Contributing Authors: Gowri G. R

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

Audience	x
Documentation Accessibility	x
Related Documents	x
Conventions	x

## What's New in Oracle Identity Manager Connector for Microsoft Exchange?

---

Software Updates	xii
Documentation-Specific Updates	xv

## 1 About the Connector

---

1.1	Certified Components	1-1
1.2	Usage Recommendation	1-2
1.3	Certified Languages	1-3
1.4	Connector Architecture	1-4
1.4.1	Architecture of the Microsoft Exchange Connector	1-4
1.4.2	Reconciliation and Provisioning of Mailboxes Across Multiple Domains	1-8
1.5	Features of the Connector	1-8
1.5.1	Full and Incremental Reconciliation	1-8
1.5.2	Limited Reconciliation	1-9
1.5.3	Reconciliation of Deleted User Records	1-9
1.5.4	Reconciliation of Lookup Definitions	1-9
1.5.5	Support for Multiple Domains	1-9
1.5.6	Transformation and Validation of Account Data	1-9
1.5.7	Support for Running Custom PowerShell Scripts	1-10
1.6	Lookup Definitions Used During Connector Operations	1-10
1.6.1	Lookup.Exchange.Configuration	1-10
1.6.2	Lookup.Exchange.UM.Configuration	1-11
1.6.3	Lookup Definitions for Attribute Mappings	1-12
1.6.4	Lookup.Exchange.DistributionGroups	1-15

1.6.5	Lookup.Exchange.MailboxDatabase	1-15
1.6.6	Lookup.Exchange.RecipientType.Options	1-16
1.7	Target Resource Reconciliation	1-16
1.7.1	Mailbox Fields for Target Resource Reconciliation	1-16
1.7.2	Reconciliation Rule	1-18
1.7.2.1	Reconciliation Rule for the Connector	1-18
1.7.2.2	Viewing Reconciliation Rules	1-19
1.7.3	Reconciliation Action Rules	1-20
1.7.3.1	Reconciliation Action Rules for the Connector	1-20
1.7.3.2	Viewing Reconciliation Action Rules	1-20
1.8	Provisioning	1-21
1.8.1	Mailbox Provisioning Functions Supported by the Connector	1-21
1.8.2	Mailbox Fields for Provisioning	1-22

## 2 Deploying the Connector

---

2.1	Preinstallation	2-1
2.1.1	Preinstallation on the Target System	2-1
2.1.1.1	Privileges for Exchange 2007 Service Account	2-2
2.1.1.2	Privileges for Exchange 2010 Service Account	2-2
2.1.1.3	Privileges for Exchange 2013 Service Account	2-2
2.1.1.4	Privileges for Exchange 2016 Service Account	2-2
2.1.2	Installing, Configuring, and Running the Connector Server	2-3
2.1.2.1	Prerequisites for the Connector Server	2-3
2.1.2.2	Installing the Connector Server	2-4
2.1.2.3	Configuring the Connector Server	2-4
2.1.2.4	Enabling Logging	2-5
2.1.2.5	Configuring Log File Rotation	2-6
2.1.2.6	Running the Connector Server	2-7
2.2	Installation	2-8
2.2.1	Installing the Connector in Oracle Identity Manager	2-8
2.2.1.1	Running the Connector Installer	2-9
2.2.1.2	Configuring the IT Resource for the Target System	2-10
2.2.2	Deploying the Connector Bundle on the Connector Server	2-13
2.2.2.1	Copying and Extracting the Connector Bundle to the Connector Server	2-13
2.2.2.2	Configuring the IT Resource for the Connector Server	2-13
2.3	Postinstallation	2-15
2.3.1	Configuring Oracle Identity Manager 11.1.2 or Later	2-15
2.3.1.1	Creating and Activating a Sandbox	2-16
2.3.1.2	Creating a New UI Form	2-16
2.3.1.3	Creating an Application Instance	2-16

2.3.1.4	Publishing a Sandbox	2-17
2.3.1.5	Harvesting Entitlements and Sync Catalog	2-17
2.3.1.6	Updating an Existing Application Instance with a New Form	2-17
2.3.2	Localizing Field Labels in UI Forms	2-18
2.3.3	Clearing Content Related to Connector Resource Bundles from the Server Cache	2-19
2.3.4	Linking the Exchange Resource Object with the AD User Resource Object	2-20
2.3.5	Configuring Oracle Identity Manager for Request-Based Provisioning	2-21
2.3.5.1	Importing Request Datasets Using Deployment Manager	2-22
2.3.5.2	Copying Predefined Request Datasets	2-22
2.3.5.3	Importing Request Datasets into MDS	2-23
2.3.5.4	Enabling the Auto Save Form Feature	2-25
2.3.5.5	Running the PurgeCache Utility	2-25
2.3.6	Configuring SSL Between Oracle Identity Manager and Connector Server	2-25
2.3.6.1	Installing Certificate Services on Windows Server 2003	2-25
2.3.6.2	Installing Certificate Services for Windows Server 2008	2-26
2.3.6.3	Exporting the Certificate	2-27
2.3.6.4	Configuring the Connector Server for SSL	2-27
2.3.6.5	Configuring Oracle Identity Manager for SSL	2-28
2.3.7	Setting up the Lookup Definition for Connection Pooling	2-30
2.4	Upgrading the Connector	2-30
2.4.1	Preupgrade Steps	2-31
2.4.2	Upgrade Steps	2-31
2.4.3	Postupgrade Steps	2-32
2.5	About Cloning the Connector	2-33

## 3 Using the Connector

---

3.1	Guidelines on Using the Connector	3-1
3.1.1	Guidelines on Configuring Reconciliation	3-1
3.1.2	Guidelines on Performing Provisioning Operations	3-1
3.2	Scheduled Tasks for Lookup Field Synchronization	3-2
3.3	Configuring Reconciliation	3-3
3.3.1	Performing Full Reconciliation and Incremental Reconciliation	3-3
3.3.2	Limited Reconciliation By Using Filters	3-4
3.3.3	Reconciliation Scheduled Tasks	3-6
3.3.3.1	Exchange Target Resource User Reconciliation	3-7
3.3.3.2	Exchange Target Resource Delete User Reconciliation	3-9
3.3.3.3	Exchange Leave Of Absence Update Task	3-9
3.4	Configuring Scheduled Tasks	3-9

3.5	Configuring Provisioning in Oracle Identity Manager Release 11.1.1	3-11
3.5.1	Using the Connector for Provisioning	3-11
3.5.2	Performing Provisioning Operations	3-11
3.5.2.1	Direct Provisioning	3-12
3.5.2.2	Request-Based Provisioning	3-13
3.5.3	Switching Between Request-Based Provisioning and Direct Provisioning	3-14
3.5.3.1	Switching From Request-Based Provisioning to Direct Provisioning	3-15
3.5.3.2	Switching From Direct Provisioning to Request-Based Provisioning	3-15
3.6	Configuring Provisioning in Oracle Identity Manager Release 11.1.2	3-16
3.7	Configuring Action Scripts	3-16
3.7.1	About Configuring Action Scripts	3-17
3.7.2	Running a Custom PowerShell Script	3-18

## 4 Extending the Functionality of the Connector

---

4.1	Adding New Fields for Target Resource Reconciliation	4-1
4.2	Adding New Multivalued Fields for Target Resource Reconciliation	4-6
4.2.1	Adding New Multivalued Fields	4-7
4.2.2	Adding Secondary Email Addresses as Multivalued Fields	4-9
4.2.3	Defining Lookup Definition for Custom Multivalued Attributes in Oracle Identity Manager 11.1.2	4-12
4.3	Adding New Fields for Provisioning	4-13
4.4	Adding New Multivalued Fields for Provisioning	4-17
4.5	Configuring Validation of Data During Reconciliation and Provisioning	4-23
4.6	Configuring Transformation of Data During User Reconciliation	4-25

## 5 Troubleshooting

---

## 6 Frequently Asked Questions

---

6.1	FAQs Related to Exchange 2007 or Later	6-1
6.2	FAQs Related to Exchange 2010 or Later	6-3
6.3	FAQs Related to Exchange 2007	6-4

## A Files and Directories On the Connector Installation Media

---

**B** Special Characters Supported for Alias Name

---

**C** Microsoft Exchange Fields Supported for Reconciliation and Provisioning

---

Index

---

## List of Figures

---

1-1	Architecture of the Connector Supporting Exchange Server 2007	1-5
1-2	Architecture of the Connector Supporting Exchange Server 2010	1-7
1-3	Reconciliation Rule for the Exchange Connector	1-19
1-4	Reconciliation Action Rules for the Connector	1-21
2-1	Edit IT Resource Details and Parameters Page for the Exchange Connector Server	
	IT Resource	2-14
4-1	Adding a New Version of Process Form	4-2
4-2	Adding a New Reconciliation Field	4-3
4-3	Adding a Reconciliation Field Mapping	4-4
4-4	Reconciliation Field Mappings	4-5
4-5	Adding an Entry to Reconciliation Lookup	4-6
4-6	Adding a New Process Task	4-14
4-7	Selecting an Adapter for New Process Task	4-15
4-8	Mapping Adapter Variables for New Process Task	4-16

## List of Tables

---

1-1	Certified Components	1-2
1-2	Entries in the Lookup.Exchange.Configuration Lookup Definition	1-10
1-3	Entries in the Lookup.Exchange.UM.Configuration	1-11
1-4	Entries in the Lookup Definitions for Attribute Mappings	1-13
1-5	Mailbox Fields for Target Resource Reconciliation	1-17
1-6	Action Rules for Target Resource Reconciliation	1-20
1-7	Mailbox Provisioning Functions Supported by the Connector	1-22
2-1	Log Levels	2-6
2-2	Parameters of the Exchange IT Resource for the Target System	2-12
2-3	Parameters of the Exchange Connector Server IT Resource	2-15
2-4	Parameters in the Properties File	2-23
2-5	Connection Pooling Properties	2-30
3-1	Attributes of the Scheduled Tasks for Lookup Field Synchronization	3-2
3-2	Keywords and Syntax for the Filter Attribute	3-4
3-3	Attributes of the Exchange Target Resource User Reconciliation Scheduled Task	3-7
3-4	Attributes of the Exchange Target Resource Delete User Reconciliation Scheduled Task	3-9
5-1	Troubleshooting Common Connector Issues	5-1
5-2	Troubleshooting Connector Issues with Exchange 2010	5-3
5-3	Troubleshooting Connector Issues with Exchange 2007	5-3
A-1	Files and Directories On the Connector Installation Media	A-1
B-1	Special Characters That Can Be Used in the Alias Name Field	B-1
C-1	Single-valued Fields Supported by Microsoft Exchange	C-1
C-2	Multi-valued Fields Supported by Exchange 2010	C-1
C-3	Multi-valued Fields Supported by Exchange 2007	C-2

# Preface

This guide describes the connector that is used to onboard applications pertaining to Microsoft Exchange into Oracle Identity Governance.

## Audience

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

## Documentation Accessibility

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

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Related Documents

For information about installing and using Oracle Identity Manager, visit the following Oracle Help Center page:

[http://docs.oracle.com/cd/E52734\\_01/index.html](http://docs.oracle.com/cd/E52734_01/index.html)

For information about Oracle Identity Manager Connectors documentation, visit the following Oracle Help Center page:

[http://docs.oracle.com/cd/E22999\\_01/index.htm](http://docs.oracle.com/cd/E22999_01/index.htm)

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

<b>Convention</b>	<b>Meaning</b>
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 for release 11.1.1.6.0 of the Microsoft Exchange connector.

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 the software updates:

- [Software Updates in Release 11.1.1.6.0](#)
- [Software Updates in Release 11.1.1.5.0](#)

## Software Updates in Release 11.1.1.6.0

The following software updates have been made in release 11.1.1.6.0:

- [Support for Multiple Domains](#)
- [Support for Multi-valued Attributes](#)
- [Support for Minimum Privileges for Exchange Server 2010](#)
- [Performance Improvements During Target Resource Reconciliation with Distribution Groups](#)
- [Support for Reconciliation from a Particular Organization Unit](#)
- [Support for Reconciliation from a Particular Mailbox Database](#)
- [Resolved Issues in Release 11.1.1.6.0](#)

## Support for Multiple Domains

This release of the connector supports topologies like a single Exchange server supporting all domains in a forest. The domains in the forest could be in a parent-child

relationship or they could be peer domains. In other words, the connector supports this topology using a single IT resource. The connector IT resource is Exchange server specific and not domain-specific.

See [Reconciliation and Provisioning of Mailboxes Across Multiple Domains](#) for more information.

## Support for Multi-valued Attributes

This release of the connector supports managing multi-valued attributes of Mailbox and MailUser recipients. By default, the multi-valued attributes are not shipped with the connector. To customize or add new attributes, see [Support for Addition of New Fields](#).

## Support for Minimum Privileges for Exchange Server 2010

This release of the connector supports managing recipients on Exchange Server 2010 using minimum privileges. The connector uses only the Recipient Management role.

## Performance Improvements During Target Resource Reconciliation with Distribution Groups

Performance has been improved during target resource reconciliation with distribution groups.

In addition, if a distribution group was removed from Recon Attribute Map, then the connector honors this instead of fetching it from the target system.

## Support for Reconciliation from a Particular Organization Unit

The connector now supports reconciliation from a particular Organization Unit (OU).

## Support for Reconciliation from a Particular Mailbox Database

The connector now supports reconciliation from a particular mailbox database.

## Resolved Issues in Release 11.1.1.6.0

The following are issues resolved in release 11.1.1.6.0:

Bug Number	Issue Description
14594530	This issue was applicable to Exchange 2010. The connector could not manage users with minimum privilege, Recipient Management Role. It required Domain Admin credentials for account management.
14745591	This issue was applicable to Exchange 2010. The connector did not support multiple domain topology within a forest.
14786992	The connector did not fetch the correct mailbox database during reconciliation.
14748032	The connector threw ParameterBindingException due to incorrect date format.

Bug Number	Issue Description
16032917	Reconciliation stopped whenever fetching distribution groups of a single user failed. Now, such errors are ignored and reconciliation of other users is continued.

## Software Updates in Release 11.1.1.5.0

The following software updates have been made in release 11.1.1.5.0:

- [ICF Based Connector](#)
- [Enhanced Performance](#)
- [Support for Multiple Domains](#)
- [Support for Addition of New Fields](#)
- [Support for Transformation and Validation of Data](#)
- [Support for Running Scripts](#)
- [Support for Connection Pooling](#)

### ICF Based Connector

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager connectors require.

The Oracle Identity Manager Connector for Microsoft Exchange is an ICF-based connector. The ICF uses classpath isolation, which allows the connector to co-exist with legacy versions of the connector.

For more information about the ICF and its advantages, see *Understanding the Identity Connector Framework in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

### Enhanced Performance

The performance of this release of the connector is enhanced when compared with the performance of the previous Java-based connectors.

This connector uses PowerShell cmdlets in the context of the .NET Connector Framework to communicate with Microsoft Exchange and to perform connector operations.

### Support for Multiple Domains

This release of the connector supports multiple domains (part of the parent-child domain topology only) in a forest with a single Exchange resource object. In the previous connector, each domain had to be represented by an Exchange resource object.

See [Reconciliation and Provisioning of Mailboxes Across Multiple Domains](#) for more information.

## Support for Addition of New Fields

This release of the connector supports the addition of single-valued and multi-valued fields that are supported by Microsoft Exchange for provisioning and reconciliation. See the following sections for more information:

- [Adding New Fields for Target Resource Reconciliation](#)
- [Adding New Multivalued Fields for Target Resource Reconciliation](#)
- [Adding New Fields for Provisioning](#)
- [Adding New Multivalued Fields for Provisioning](#)
- [Microsoft Exchange Fields Supported for Reconciliation and Provisioning](#)

## Support for Transformation and Validation of Data

You can configure transformation of data, such as process form field data or any other object, that is brought into Oracle Identity Manager during reconciliation. In addition, you can configure validation of data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. See the following sections for more information:

- [Configuring Validation of Data During Reconciliation and Provisioning](#)
- [Configuring Transformation of Data During User Reconciliation](#)

## Support for Running Scripts

From this release onwards, you can run scripts on a computer where the Microsoft Exchange connector is deployed. You can configure the scripts to run before or after the create, update, or delete an account provisioning operations. For example, you could configure a script to run before a user is created by the Microsoft Active Directory User Management connector.

See [Configuring Action Scripts](#) for more information.

## Support for Connection Pooling

This release of the connector supports the connection pooling feature based on the ICF. In earlier releases, a connection with the target system was established at the start of a reconciliation run and closed at the end of the reconciliation run. With the introduction of connection pooling, multiple connections are established by the ICF and held in reserve for use by the connector.

See [Setting up the Lookup Definition for Connection Pooling](#) for more information.

## Documentation-Specific Updates

The following sections discuss the documentation-specific updates:

- [Documentation-Specific Updates in Release 11.1.1.6.0](#)
- [Documentation-Specific Updates in Release 11.1.1.5.0](#)

## Documentation-Specific Updates in Release 11.1.1.6.0

The following documentation-specific update has been made in revision "26" of release 11.1.1.6.0:

The "Target Systems" row of [Table 1-1](#) has been updated to include support for Microsoft Exchange 2019.

The following documentation-specific update has been made in revision "25" of release 11.1.1.6.0:

The "Oracle Identity Governance or Oracle Identity Manager" row of [Table 1-1](#) has been updated to include Oracle Identity Governance 12c (12.2.1.4.0) certification.

The following documentation-specific update has been made in revision "24" of release 11.1.1.6.0:

Information about overwriting Active Directory's account email address with an auto generated email address has been added to [FAQs Related to Exchange 2010 or Later](#).

The following documentation-specific updates have been made in revision "23" of release 11.1.1.6.0:

- [Privileges for Exchange 2016 Service Account](#) has been added.
- Minor updates to the document structure for better readability.

The following documentation-specific update has been made in revision "22" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of [Table 1-1](#) has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12c (12.2.1.3.0) certification.

The following are the documentation-specific updates in revision "21" of release 11.1.1.6.0:

- The following rows of [Table 2-2](#) have been updated:
  - ExchangeServerHost
  - ExchangeUser
  - ExchangeUserPassword
- The "Target Systems" row of [Table 1-1](#) has been updated.

The following are documentation-specific updates in revision "20" of release 11.1.1.6.0:

- The "Target Systems" row of [Table 1-1](#) has been updated.
- The "ExchangeServerType" row of [Table 2-2](#) has been updated.

The following are documentation-specific updates in revision "19" of release 11.1.1.6.0:

- The "Connector Server" row has been added to [Table 1-1](#).
- The "JDK" row of [Table 1-1](#) has been renamed to "Connector Server JDK".

The following are documentation-specific updates in revision "18" of release 11.1.1.6.0:

- [Privileges for Exchange 2013 Service Account](#) has been added.
- A new row has been added to [Table 5-1](#).
- [Installing Certificate Services for Windows Server 2008](#) has been added.

The following is a documentation-specific update in revision "17" of release 11.1.1.6.0:

Information regarding coexistence of Microsoft Exchange 9.x and 11.x connectors has been modified in [FAQs Related to Exchange 2007 or Later](#).

The following are documentation-specific updates in revision "16" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of [Table 1-1](#) has been updated.
- Information specific to Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) has been added to [Usage Recommendation](#).

The following is a documentation-specific update in revision "15" of release 11.1.1.6.0:

A "Note" has been added at the beginning of [Extending the Functionality of the Connector](#).

The following is a documentation-specific update in revision "14" of release 11.1.1.6.0:

The "Other systems" row of [Table 1-1](#) has been updated.

The following is a documentation-specific update in revision "13" of release 11.1.1.6.0:

A syntax error in [Configuring Log File Rotation](#) has been fixed.

The following are documentation-specific updates in revision "12" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of [Table 1-1](#) has been modified to include Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0).
- Information specific to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0) has been added to Step 5 of [Localizing Field Labels in UI Forms](#).
- A sample procedure has been added to the following sections:
  - [Adding New Multivalued Fields for Target Resource Reconciliation](#)
  - [Adding New Multivalued Fields for Provisioning](#)
- Step 6.i has been added to [Adding New Multivalued Fields for Target Resource Reconciliation](#).

The following is a documentation-specific update in revision "11" of release 11.1.1.6.0:

- Microsoft Exchange 2013 has been added as a target system supported by this connector. This information is present in the "Target Systems" row of [Table 1-1](#).

The following are documentation-specific updates in revision "10" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row in [Table 1-1](#) has been modified.
- [Usage Recommendation](#) has been modified.
- [Architecture of the Microsoft Exchange Connector](#) has been modified.

- [Prerequisites for the Connector Server](#) has been modified.
- [Configuring Action Scripts](#) has been modified.

The following are documentation-specific updates in revision "9" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row in [Table 1-1](#) has been modified.
- A note has been added in the "Files in the Dataset directory" and "xml\Exchange-Datasets.xml" rows of [Table A-1](#).
- [Installing, Configuring, and Running the Connector Server](#) has been modified.
- The following sections have been added:
  - [Usage Recommendation](#)
  - [Configuring Oracle Identity Manager 11.1.2 or Later](#)
  - [Localizing Field Labels in UI Forms](#)
  - [Configuring Provisioning in Oracle Identity Manager Release 11.1.1](#)
  - [Configuring Provisioning in Oracle Identity Manager Release 11.1.2](#)
- Instructions specific to Oracle Identity Manager release 11.1.2.x have been added in the following sections:
  - [Running the Connector Installer](#)
  - [Configuring the IT Resource for the Target System](#)
  - [Configuring the IT Resource for the Connector Server](#)
  - [Configuring Scheduled Tasks](#)

## Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific updates have been made in the revision "8" of the release 11.1.1.5.0:

- In [Certified Components](#), the target systems have been updated as follows:
  - Microsoft Exchange 2007 SP1, SP2, SP3 (64-bit)
  - Microsoft Exchange 2010 RTM, SP1, SP2, SP3 (64-bit)
- In [Certified Components](#), the target system host platforms have been updated as follows:
  - Microsoft Windows Server 2012

The following documentation-specific update has been made in the revision "7" of the release 11.1.1.5.0:

- [Table 2-2](#) has been updated for the values of Container, DomainName and ExchangeServerType parameters.

The following documentation-specific updates have been made in the revision "6" of the release 11.1.1.5.0:

- [Table 1-1](#) has been updated.
- In [Installing, Configuring, and Running the Connector Server](#), the note about .NET connector server has been updated.
- [Configuring Log File Rotation](#) has been added.

- The descriptions of the Container and DomainName parameters have been updated in [Table 2-2](#).
- [Configuring Action Scripts](#) has been updated.

The following documentation-specific updates have been made in the revision "4" of the release 11.1.1.5.0:

- In [Certified Components](#), the target system host platforms have been updated as follows:
  - Microsoft Windows Server 2003 (32-bit and 64-bit) or later
  - Microsoft Windows Server 2008 (32-bit and 64-bit) or later

The following documentation-specific updates have been made in the revision "3" of the release 11.1.1.5.0:

- In [Installing, Configuring, and Running the Connector Server](#), a note about installing a patch for .NET Framework 3.5 has been added.
- Updated [Installation](#) to indicate that the connector must be installed both in Oracle Identity Manager and in the connector server. Moved Section 2.3.3, "Configuring the IT Resource for the Connector Server" to [Configuring the IT Resource for the Connector Server](#).

The following documentation-specific update has been made in the revision "2" of the release 11.1.1.5.0:

- In [Certified Components](#), the target system, Microsoft Exchange 2010 SP2 (64-bit) has been added.

# 1

## About the Connector

This chapter introduces the Microsoft Exchange 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**.

This connector supports two recipient types, UserMailbox and MailUser. The term **recipients** is used in this guide to refer to both recipient types. In other cases, the terms **UserMailbox** and **MailUser** are used in this guide to refer to specific recipient types.

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:

- [Certified Components](#)
- [Usage Recommendation](#)
- [Certified Languages](#)
- [Connector Architecture](#)
- [Features of the Connector](#)
- [Lookup Definitions Used During Connector Operations](#)
- [Target Resource Reconciliation](#)
- [Provisioning](#)

### 1.1 Certified Components

These are the software components and their versions required for installing and using the connector.

**Table 1-1 Certified Components**

Item	Requirement
Oracle Identity Governance or Oracle Identity Manager	<p>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</p> <ul style="list-style-type: none"> <li>• Oracle Identity Governance 12c (12.2.1.4.0)</li> <li>• Oracle Identity Governance 12c (12.2.1.3.0)</li> <li>• Oracle Identity Manager 11g Release 1 (11.1.1.5.6) and any later BP in this release track</li> <li>• Oracle Identity Manager 11g Release 2 (11.1.2.0.6) and any later BP in this release track</li> <li>• Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0)</li> <li>• Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)</li> </ul>
Target systems	<p>The target system can be any one or a combination of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Exchange 2007 SP1, SP2, SP3 (64-bit)</li> <li>• Microsoft Exchange 2010 RTM, SP1, SP2, SP3 (64-bit)</li> <li>• Microsoft Exchange 2013, 2016, 2019</li> </ul> <p>For the Exchange 2013, 2016, 2019 support, patch 25467073 must be applied on Release 11.1.1.6.0 of the Exchange Connector. This patch can be obtained from My Oracle Support under Patches and Updates.</p>
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 Update 24 or later
Other systems	<p>You must ensure the following software are installed in your operating environment:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory</li> <li>• Microsoft Active Directory User Management connector 11.1.1.5.0 or later</li> </ul> <p>You must deploy the Microsoft Active Directory User Management connector before you can deploy and use the Microsoft Exchange connector.</p> <p>See Deploying the Connector in <i>Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management</i> for instructions to deploy the Microsoft Active Directory connector.</p> <ul style="list-style-type: none"> <li>• .NET Connector Server</li> </ul> <p>The Microsoft Exchange connector operates in the context of the .NET Framework. The .NET connector server can be downloaded from the following page:</p> <p><a href="http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html">http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html</a></p>

## 1.2 Usage Recommendation

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of these connector versions.

- If you are using an Oracle Identity Manager release 9.1.0.2 or later and earlier than Oracle Identity Manager 11g Release 1 (11.1.1.5.6), then you must use the 9.0.4 version of this connector.

- If you are using Oracle Identity Manager 11g Release 1 (11.1.1.5.6) or later, Oracle Identity Manager 11g Release 2 (11.1.2.0.6) or later, Oracle Identity Manager 11g Release 2 (11.1.2.2.0), or Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.x version of this connector. However, if you are using Microsoft Exchange 2003, then you must use the 9.x versions for both Microsoft Active Directory User Management and Microsoft Exchange connectors.

## 1.3 Certified Languages

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

## 1.4 Connector Architecture

Learn about the architecture of the connector and reconciling and provisioning mailboxes across multiple domains.

This section discusses the following topics:

- [Architecture of the Microsoft Exchange Connector](#)
- [Reconciliation and Provisioning of Mailboxes Across Multiple Domains](#)

### 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 and reconciliation operations. This means that the connector only supports target resource reconciliation with Microsoft Exchange.

### 1.4.1 Architecture of the Microsoft Exchange Connector

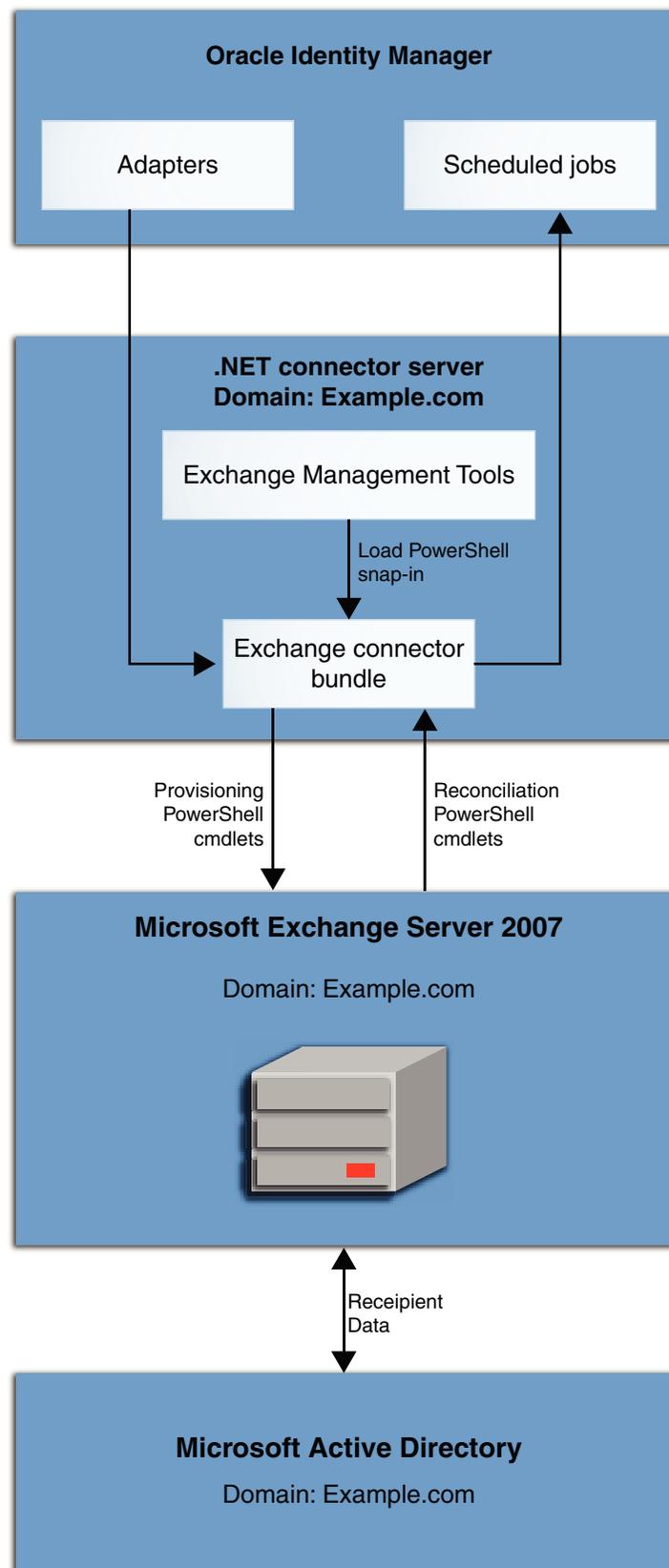
The connector uses Exchange-related PowerShell cmdlets to perform recipient administration activities on the Exchange Server. The connector supports UserMailbox and MailUser recipient types. The .NET connector server is mandatory for both Exchange 2007 and Exchange 2010 target system versions.

### See Also:

<http://technet.microsoft.com/en-us/library/bb201680%28v=exchg.141%29.aspx> for more information about recipient types

[Figure 1-1](#) shows the architecture of the connector supporting Exchange Server 2007. In this architecture diagram, the .NET connector server is installed on a different computer in the same domain as that of the Exchange Server computer. You can also install the .NET connector server on the same computer hosting Exchange Server.

Figure 1-1 Architecture of the Connector Supporting Exchange Server 2007

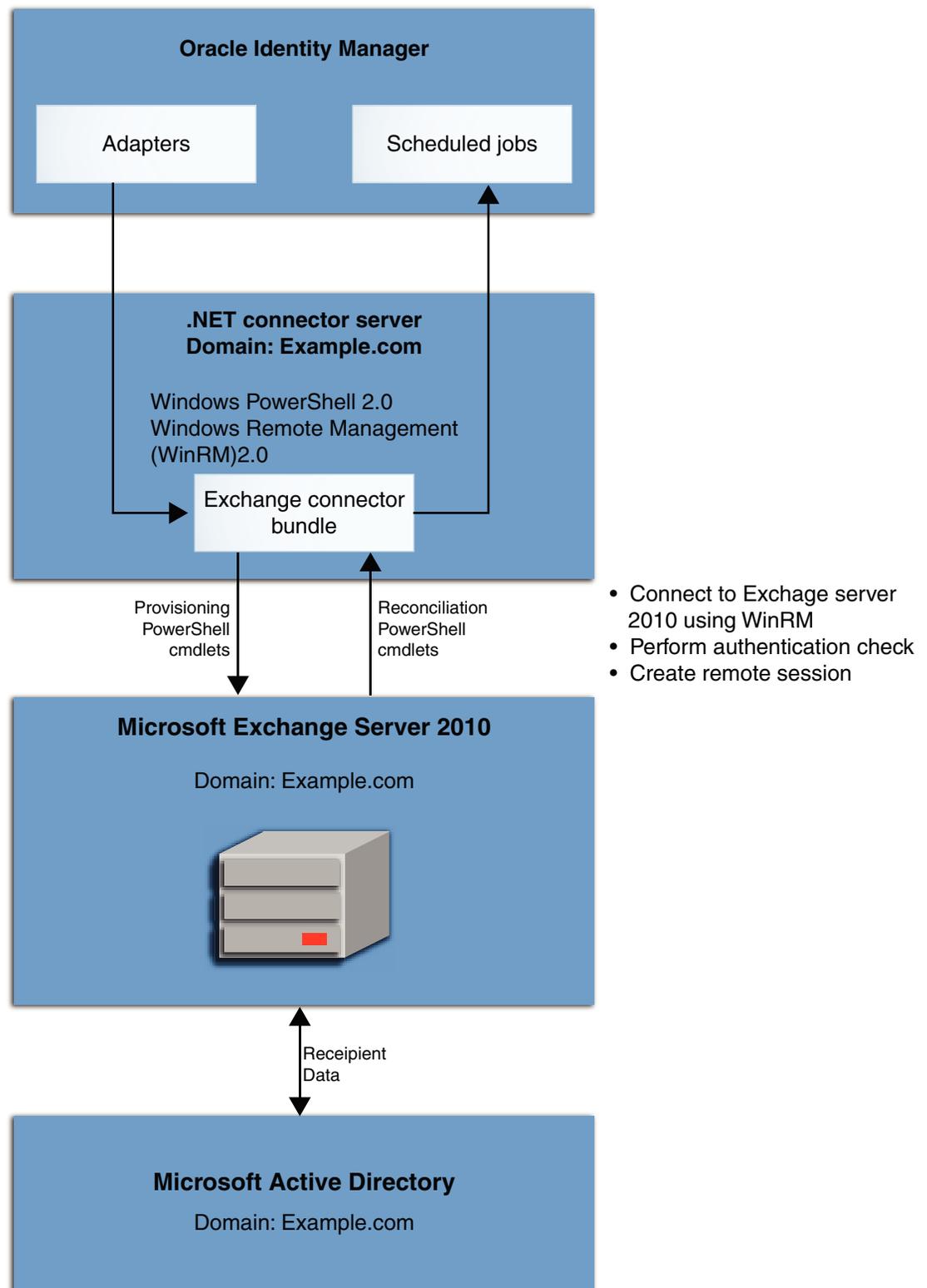


Oracle Identity Manager (OIM) communicates with Exchange Server 2007 via connector bundle using various adapters and scheduled jobs. The connector bundle is deployed on a Windows computer with the .NET connector server installed. To communicate with Exchange Server 2007, the connector loads the Microsoft.Exchange.Management.PowerShell.Admin snap-in locally to create a runspace, which is the environment for running PowerShell cmdlets. This snap-in becomes available when Exchange Management Tools are installed. For this reason, Exchange Management Tools must be installed on the Windows computer hosting the connector server.

For more information on hardware requirements, installing, and configuring connector server, see [Installing, Configuring, and Running the Connector Server](#).

[Figure 1-2](#) shows the architecture of the connector supporting Exchange Server 2010. In this architecture diagram, the .NET connector server is installed on a different computer in the same domain as that of the Exchange Server computer. You can also install the connector server on the same computer hosting Exchange Server.

Figure 1-2 Architecture of the Connector Supporting Exchange Server 2010



Oracle Identity Manager (OIM) communicates with Exchange Server 2010 via connector bundle using various adapters and scheduled jobs. The connector bundle

is deployed on a Windows computer with the .NET connector server installed. To communicate with Exchange Server 2010, OIM uses remote Shell, which in turn uses Windows PowerShell 2.0 and Windows Remote Management (WinRM) 2.0 without the need for Exchange Management Tools. Therefore, Exchange Management Tools are not required to be installed on the connector server for Exchange Server 2010. For more information, see the following topic on Remote Exchange Management at:

<http://technet.microsoft.com/en-in/library/dd297932%28v=exchg.141%29.aspx>

Run the **Enable-PSRemoting** cmdlet to configure the Exchange Server computer to receive Windows PowerShell remote commands that are sent by using the WS-Management technology. For more information about the Enable-PSRemoting cmdlet, see:

<http://technet.microsoft.com/en-us/library/hh849694.aspx>

For more information on hardware requirements, installing, and configuring connector server, see [Installing, Configuring, and Running the Connector Server](#).

## 1.4.2 Reconciliation and Provisioning of Mailboxes Across Multiple Domains

The connector supports reconciliation and provisioning of mailboxes for users across multiple Microsoft Active Directory domains. The domains can be in a parent child relationship or can be peer domains.

For example:

- Users in Child Domain 1, Child Domain 2, and Parent Domain can have mailboxes in the same single Exchange Server.
- Users in Peer Domain 1 and Peer Domain 2 can have mailboxes in the same single Exchange Server. In this case, Exchange Server can be configured against Peer Domain 1 or Peer Domain 2.

## 1.5 Features of the Connector

The features of the connector include full and incremental reconciliation, limited reconciliation, transformation and validation of account data and so on.

- [Full and Incremental Reconciliation](#)
- [Limited Reconciliation](#)
- [Reconciliation of Deleted User Records](#)
- [Reconciliation of Lookup Definitions](#)
- [Support for Multiple Domains](#)
- [Support for Running Custom PowerShell Scripts](#)

### 1.5.1 Full and Incremental Reconciliation

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

reconciliation, user accounts that have been added or modified since the last reconciliation run are fetched into Oracle Identity Manager.

You can perform a full and incremental reconciliation against a single domain by providing a value for the `DomainController` parameter of the scheduled task. If the `DomainController` parameter is blank, reconciliation is performed against all domains in the forest.

See [Performing Full Reconciliation and Incremental Reconciliation](#) for more information.

## 1.5.2 Limited Reconciliation

You can set a reconciliation filter as the value of the `Filter` attribute of the user reconciliation scheduled task. This filter specifies the subset of added and modified target system records that must be reconciled.

See [Limited Reconciliation By Using Filters](#) for more information.

## 1.5.3 Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records. In target resource mode, if a user record is deleted on the target system, then the corresponding Exchange User resource is revoked from the OIM User.

See [Exchange Target Resource Delete User Reconciliation](#) for more information.

## 1.5.4 Reconciliation of Lookup Definitions

You can configure the connector for reconciliation of the distribution groups and mailbox database in the target system to be populated in the lookup definitions on Oracle Identity Manager.

See the following sections for more information:

- [Lookup.Exchange.DistributionGroups](#)
- [Lookup.Exchange.MailboxDatabase](#)
- [Scheduled Tasks for Lookup Field Synchronization](#)

## 1.5.5 Support for Multiple Domains

The connector supports multiple domains in a forest with a single Exchange resource object.

See [Connector Architecture](#) for more information.

## 1.5.6 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation.

The following sections provide more information:

- [Configuring Validation of Data During Reconciliation and Provisioning](#)
- [Configuring Transformation of Data During User Reconciliation](#)

## 1.5.7 Support for Running Custom PowerShell Scripts

You can run custom PowerShell scripts on a computer where the Microsoft Exchange connector is deployed. You can configure the scripts to run before or after the create, update, or delete an account provisioning operations.

For example, you could configure a script to run before a user is created by the connector.

See [Configuring Action Scripts](#) for more information.

## 1.6 Lookup Definitions Used During Connector Operations

Lookup definitions are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

The lookup definitions are as follows:

- [Lookup.Exchange.Configuration](#)
- [Lookup.Exchange.UM.Configuration](#)
- [Lookup Definitions for Attribute Mappings](#)
- [Lookup.Exchange.DistributionGroups](#)
- [Lookup.Exchange.MailboxDatabase](#)
- [Lookup.Exchange.RecipientType.Options](#)

### 1.6.1 Lookup.Exchange.Configuration

The Lookup.Exchange.Configuration lookup definition holds connector configuration entries that are used during reconciliation and provisioning operations.

[Table 1-2](#) lists the default entries in this lookup definition.

**Table 1-2 Entries in the Lookup.Exchange.Configuration Lookup Definition**

Code Key	Decode	Description
AuthenticationMechanism	Kerberos	This entry is used when the connector is configured against Exchange 2010 to remotely connect to the Exchange Server. Do not modify this entry.
Bundle Name	Exchange.Connector	This entry holds the name of the connector bundle package. Do not modify this entry.
Bundle Version	2.0.0.1	This entry holds the version of the connector bundle class. Do not modify this entry.

**Table 1-2 (Cont.) Entries in the Lookup.Exchange.Configuration Lookup Definition**

Code Key	Decode	Description
Connector Name	Org.IdentityConnectors.Exchange.ExchangeConnector	This entry holds the name of the connector class. Do not modify this entry.
Container	UseDefault	This entry is used internally. Do not modify this entry.
DomainName	UseDefault	This entry is used internally. Do not modify this entry.
DirectoryAdminName	UseDefault	This entry is used internally. Do not modify this entry.
DirectoryAdminPassword	UseDefault	This entry is used internally. Do not modify this entry.
DefaultIncomingMessage Size	10MB	During Enable operation, the connector first sets the IncomingMessageSize of the recipient to this value. After the operation completes, the connector updates the target system with the actual size in the process form. Provide appropriate default value for your organization.
DefaultOutgoingMessage Size	10MB	During Enable operation, the connector first sets the OutgoingMessageSize of the recipient to this value. After the operation completes, the connector updates the target system with the actual size in the process form. Provide appropriate default value for your organization.
Mode	OIM	This entry is used internally. Do not modify this entry.
User Configuration Lookup	Lookup.Exchange.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do not modify this entry.
UseSSLForRemotePower Shell	false	This entry is used when the connector is configured against Exchange 2010 to remotely connect to the connector. Do not modify this entry.

## 1.6.2 Lookup.Exchange.UM.Configuration

The Lookup.Exchange.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations.

[Table 1-3](#) lists the default entries in this lookup definition.

**Table 1-3 Entries in the Lookup.Exchange.UM.Configuration**

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.Exchange.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See <a href="#">Lookup Definitions for Attribute Mappings</a> for more information about this lookup definition.

**Table 1-3 (Cont.) Entries in the Lookup.Exchange.UM.Configuration**

Code Key	Decode	Description
Recon Attribute Map	Lookup.Exchange.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes.  See <a href="#">Lookup Definitions for Attribute Mappings</a> for more information about this lookup definition.
Recon Transformation Lookup	Lookup.Exchange.UM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation.  See <a href="#">Configuring Transformation of Data During User Reconciliation</a> for more information about adding entries in this lookup definition.
Recon Validation Lookup	Lookup.Exchange.UM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation.  See <a href="#">Configuring Validation of Data During Reconciliation and Provisioning</a> for more information about adding entries in this lookup definition.
Provisioning Validation Lookup	Lookup.Exchange.UM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations.  See <a href="#">Configuring Validation of Data During Reconciliation and Provisioning</a> for more information about adding entries in this lookup definition.

### 1.6.3 Lookup Definitions for Attribute Mappings

The Lookup.Exchange.UM.ProvAttrMap and Lookup.Exchange.UM.ReconAttrMap lookup definitions hold attribute mappings used during connector operations.

- The Lookup.Exchange.UM.ProvAttrMap lookup definition holds mappings between process form fields (Code Key values) and target system attributes (Decode values) used during provisioning operations.

You can add entries to this lookup if you want to map new target system attributes for provisioning. See [Adding New Fields for Provisioning](#) for more information.

- The Lookup.Exchange.UM.ReconAttrMap lookup definition holds mappings between resource object fields (Code Key values) and target system attributes (Decode values) used during reconciliation operations.

You can add entries to this lookup definition if you want to map new target system attributes for reconciliation. See [Adding New Fields for Target Resource Reconciliation](#) for more information.

[Table 1-4](#) lists the default entries in these lookup definitions.

 **See Also:**

The following pages in Microsoft technical library for a description of the parameters in the Decode column

For MailUser recipient type:

- For Microsoft Exchange 2007, see [http://technet.microsoft.com/en-us/library/aa995971\(v=exchg.80\).aspx](http://technet.microsoft.com/en-us/library/aa995971(v=exchg.80).aspx)
- For Microsoft Exchange 2010, see <http://technet.microsoft.com/en-us/library/aa995971%28v=exchg.141%29.aspx>

For UserMailbox recipient type:

- For Microsoft Exchange 2007, see [http://technet.microsoft.com/en-us/library/bb123981\(v=exchg.80\).aspx](http://technet.microsoft.com/en-us/library/bb123981(v=exchg.80).aspx)
- For Microsoft Exchange 2010, see <http://technet.microsoft.com/en-us/library/bb123981%28v=exchg.141%29.aspx>

**Table 1-4 Entries in the Lookup Definitions for Attribute Mappings**

Code Key	Decode	Comments
Alias	Alias	
Database[LOOKUP]	Database	You must provide a value for this parameter only for the UserMailbox recipient type. It is mandatory for Microsoft Exchange 2007. It is <i>not</i> mandatory for Microsoft Exchange 2010.
Display Name	DisplayName	
Distribution Groups~Distribution Group[LOOKUP]	DistributionGroup	
Email Address Policy Enabled	EmailAddressPolicyEnabled	
External Email Address	ExternalEmailAddress	This parameter is mandatory for the MailUser recipient type.
Hidden From Address Lists Enabled	HiddenFromAddressListsEnabled	
Mailbox Size Receipt Quota	ProhibitSendReceiveQuota	
Mailbox Size Transmit Quota	ProhibitSendQuota	
Mailbox Warning Size	IssueWarningQuota	
Maximum Recipients	RecipientLimits	
Max Incoming Message Size	MaxReceiveSize	
Max Outgoing Message Size	MaxSendSize	
Message Body Format	MessageBodyFormat	This parameter only applies to MailUser recipient type.
Message Format	MessageFormat	This parameter only applies to MailUser recipient type.

**Table 1-4 (Cont.) Entries in the Lookup Definitions for Attribute Mappings**

Code Key	Decode	Comments
Primary SMTP Address	PrimarySmtpAddress	
Recipient Type	RecipientType	<p>The value of this parameter can be UserMailbox or MailUser.</p> <p>This parameter is used by the connector for internal purposes. It does not represent any attribute on the target system.</p> <p><b>Note:</b> It is mandatory to set a value for this attribute.</p>
Retain Deleted Items	UseDatabaseRetentionDefaults	This parameter only applies to UserMailbox recipient type.
Retain Deleted Items For	RetainDeletedItemsFor	This parameter is not applicable to MailUser recipient type on Microsoft Exchange 2007.
Retain Deleted Items Until Backup	RetainDeletedItemsUntilBackup	This parameter only applies to UserMailbox recipient type.
ReturnValue	<p>__UID__</p> <p><b>Note:</b> This value represents the GUID of the user on the target system, used by the connector for internal purposes.</p>	
Simple Display Name	SimpleDisplayName	This parameter is used to display an alternative description of the object.
UD_EX_CH--Distribution Group[LOOKUP]	DistributionGroup	This parameter represents the distinguished name of the distribution group.
Use Prefer Message Format	UsePreferMessageFormat	This parameter only applies to MailUser recipient type.
User Logon Name	<p>Depending on the lookup, the decode value is as follows:</p> <ul style="list-style-type: none"> <li>For Lookup.Exchange.UM.ProvAttrMap: __NAME__</li> </ul> <p><b>Note:</b> This value represents the User Principal Name of the user on the target system, used by the connector for internal purposes.</p> <ul style="list-style-type: none"> <li>For Lookup.Exchange.UM.ReconAttrMap: SamAccountName</li> </ul>	
Use Storage Defaults	UseDatabaseQuotaDefaults	This parameter only applies to UserMailbox recipient type.

## 1.6.4 Lookup.Exchange.DistributionGroups

The Lookup.Exchange.DistributionGroups lookup definition holds all the distribution groups available on the target system. This lookup is populated by running the Exchange User Distribution Group Lookup Reconciliation task.

 **Note:**

Distribution groups of type MailUniversalDistributionGroup only are supported.

An entry in the Code Key column has the following format:

*IT resource instance key~Distinguished name of the distribution group*

An entry in the Decode column has the following format:

*IT resource name~Distinguished name of the distribution group*

The following table shows sample entries:

Code Key	Decode
27~CN=TestGroup3,CN=Users,DC=connectordev,DC=us,DC=oracle,DC=com	Exchange IT Resource~CN=TestGroup3,CN=Users,DC=connectordev,DC=us,DC=oracle,DC=com
27~CN=newChildgroup,DC=bangalore,DC=connectordev,DC=us,DC=oracle,DC=com	Exchange IT Resource~CN=newChildgroup,DC=bangalore,DC=connectordev,DC=us,DC=oracle,DC=com

## 1.6.5 Lookup.Exchange.MailboxDatabase

The Lookup.Exchange.MailboxDatabase lookup definition holds all the databases available on the target system. This lookup is populated by running the Exchange User Mailbox Database Group Lookup Reconciliation task.

An entry in the Code Key column has the following format:

*IT resource instance key~Distinguished name of the database*

An entry in the Decode column has the following format:

*IT resource name~Distinguished name of the database*

The following table shows a sample entry:

Code Key	Decode
10~CN=Mailbox Database 0068647612,CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC =connectorqa,DC=com	Exchange IT Resource~CN=Mailbox Database 0068647612,CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC =connectorqa,DC=com

## 1.6.6 Lookup.Exchange.RecipientType.Options

The Lookup.Exchange.RecipientType.Options lookup definition indicates the type of account to be created on the target system. This option is a mandatory field on the process form.

If UserMailbox is selected, then a UserMailbox is created. If MailUser is selected, then a MailUser is created.

This lookup contains the following entries by default:

Code Key	Decode
UserMailbox	UserMailbox
MailUser	MailUser

## 1.7 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 Target Resource User Reconciliation scheduled task is used to start target resource reconciliation runs. This scheduled task is discussed in [Reconciliation Scheduled Tasks](#).

This section discusses the following topics:

- [Mailbox Fields for Target Resource Reconciliation](#)
- [Reconciliation Rule](#)
- [Reconciliation Action Rules](#)

### 1.7.1 Mailbox Fields for Target Resource Reconciliation

These are the mailbox fields from which values are fetched during a target resource reconciliation run.

**Table 1-5 Mailbox Fields for Target Resource Reconciliation**

Process Form Field	Target System Field	Description
Alias <b>Note:</b> This is a mandatory field.	Alias	Mailbox alias, which is generally the same as sAMAccountName <b>Note:</b> sAMAccountName is the user login for Microsoft Active Directory.
Archive Mailbox Size	ArchiveQuota	The archive mailbox size at which messages will no longer be accepted
Archive Mailbox Size Warning	ArchiveWarningQuota	The archive mailbox size at which a warning message is sent to the user
Database	Database	The distinguished name of the database that contains the mailbox object.
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 Address Policy Enabled	EmailAddressPolicyEnabled	Specifies whether the e-mail address policy for this mailbox is enabled. The two possible values for this parameter are \$true or \$false.
External Email Address	ExternalEmailAddress	This field is mandatory for MailUser recipient type. Specifies the e-mail address to which all the e-mails sent to the user would be automatically forwarded to.
Hidden From Address Lists Enabled	HiddenFromAddressListsEnabled	Specifies whether this mailbox is hidden from address lists. The two possible values for this parameter are \$true or \$false.
Mailbox Size Receipt Quota	ProhibitSendReceiveQuota	Specifies the mailbox size at which the user associated with this mailbox can no longer send or receive messages
Mailbox Size Transmit Quota	ProhibitSendQuota	Specifies the mailbox size at which the user associated with this mailbox can no longer send messages
Mailbox Warning Size	IssueWarningQuota	Specifies the mailbox size at which a warning message is sent to the user
Max Incoming Message Size	MaxReceiveSize	Specifies the maximum size of messages that this mailbox can receive
Max Outgoing Message Size	MaxSendSize	Specifies the maximum size of messages that this mailbox can send
Maximum Recipients	RecipientLimits	Specifies the maximum number of recipients per message to which this mailbox can send
Primary SMTP Address	PrimarySmtpAddress	Specifies the address that external users see when they receive a message from this mailbox

Table 1-5 (Cont.) Mailbox Fields for Target Resource Reconciliation

Process Form Field	Target System Field	Description
Recipient Type	RecipientType Note: This field is not a target system attribute. However, it is used by the connector for internal purposes.	Specifies the type of recipient in the Address Book. The connector supports the following recipient types: MailUser: A mail-enabled Active Directory user that represents a user outside the Exchange organization. Each MailUser has an external e-mail address. All messages sent to the MailUser are routed to this external e-mail address. A MailUser is similar to a mail contact, except that a MailUser has Active Directory logon credentials and can access resources. UserMailbox: A mailbox that is assigned to an individual user in your Exchange organization. It typically contains messages, calendar items, contacts, tasks, documents, and other important business data.
Retain Deleted Items Defaults	UseDatabaseRetentionDefaults	Specifies that this mailbox uses default values to handle deleted items or messages
Retain Deleted Items For	RetainDeletedItemsFor	Specifies the length of time to keep deleted items
Retain Deleted Items Until Backup	RetainDeletedItemsUntilBackup	Specifies whether to retain deleted items until the next backup. The two possible values for this parameter are \$true or \$false
Simple Display Name	SimpleDisplayName	Used to display an alternative description of the object when only a limited set of characters is permitted. This limited set of characters consists of ASCII characters 26 through 126, inclusively
Use Storage Defaults	UseDatabaseQuotaDefaults	Specifies that this mailbox uses the quota attributes specified for the mailbox database where this mailbox resides
User Logon Name	UserPrincipalName	Specifies the UPN for this mailbox. This is the logon name for the user. The UPN consists of a user name and a suffix. Typically, the suffix is the domain name where the user account resides.

## 1.7.2 Reconciliation Rule

Learn about the reconciliation rule for this connector and how to view it.

- [Reconciliation Rule for the Connector](#)
- [Viewing Reconciliation Rules](#)

### 1.7.2.1 Reconciliation Rule for the Connector

The following is the default reconciliation rule for this connector:

**Rule Name:** Exchange User Recon Rule

**Rule Element:** User Login Equals User ID

In this rule:

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

## 1.7.2.2 Viewing Reconciliation Rules

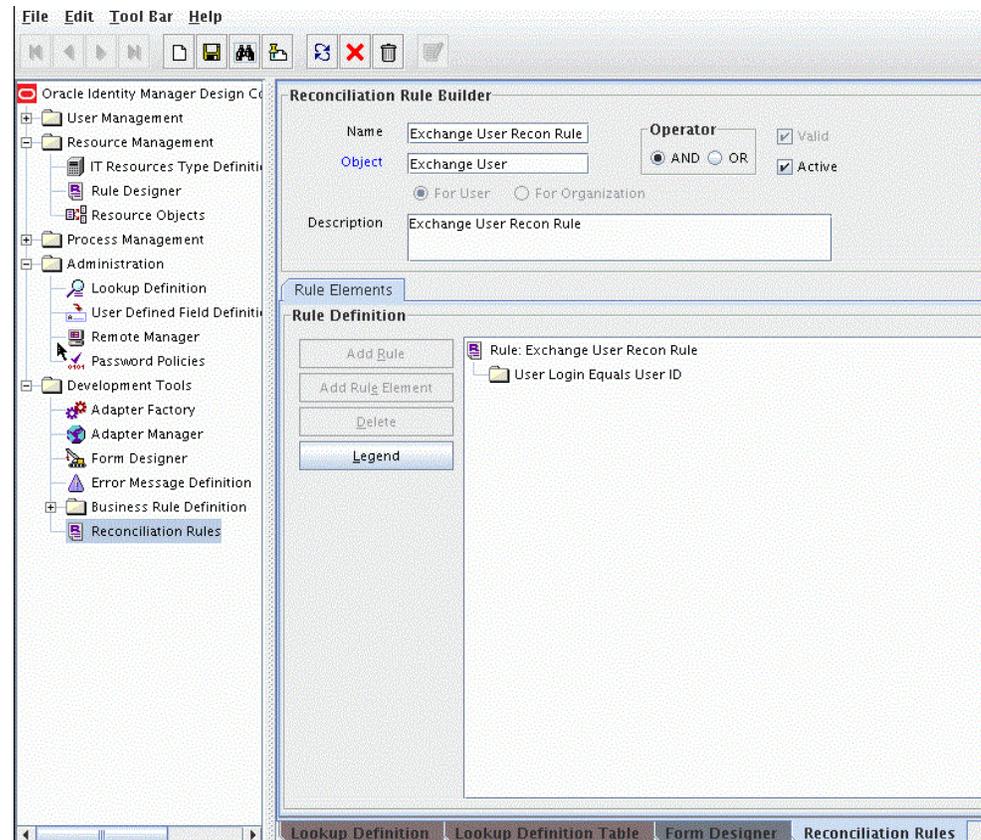
You can view the reconciliation rule for the connector after you deploy the connector.

### 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**



## 1.7.3 Reconciliation Action Rules

Learn about the reconciliation action rules for this connector and how to view them.

- [Reconciliation Action Rules for the Connector](#)
- [Viewing Reconciliation Action Rules](#)

### 1.7.3.1 Reconciliation Action Rules for the Connector

[Table 1-6](#) lists the action rules for target resource reconciliation.

**Table 1-6 Action Rules for Target Resource Reconciliation**

Rule Condition	Action
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

### 1.7.3.2 Viewing Reconciliation Action Rules

You can view the action rules for the connector after you deploy the connector.

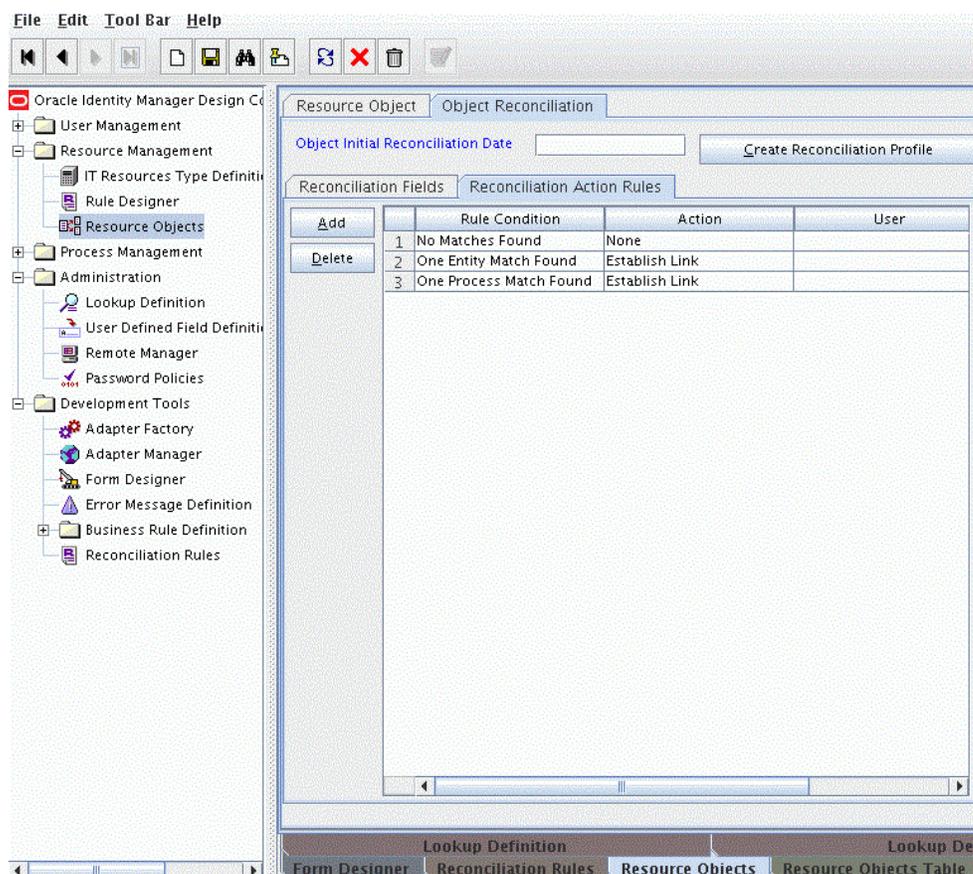


**Note:**

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 1-4](#) shows the reconciliation action rules for the connector.

Figure 1-4 Reconciliation Action Rules for the Connector



## 1.8 Provisioning

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

This section discusses the following topics:

- [Mailbox Provisioning Functions Supported by the Connector](#)
- [Mailbox Fields for Provisioning](#)

### 1.8.1 Mailbox Provisioning Functions Supported by the Connector

These are 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:**

Using the Adapter Factory in *Oracle Fusion Middleware Developing and Customizing Applications with Oracle Identity Manager* for generic information about adapters

**Table 1-7 Mailbox Provisioning Functions Supported by the Connector**

Function	Adapter
Alias Updated	ExchangeUpdateUser
Archive Mailbox Size Updated	ExchangeUpdateUser
Archive Mailbox Size Warning Updated	ExchangeUpdateUser
Create User	ExchangeCreateUser
Delete User	ExchangeDeleteUser
Disable User	ExchangeDisableUser
Display Name Updated	ExchangeUpdateUser
Distribution Group Delete	ExchangeRemoveChildTableValues
Distribution Group Insert	ExchangeAddChildTableValues
Distribution Group Update	ExchangeUpdateChildTableValues
Email Address Policy Enabled Updated	ExchangeUpdateUser
Enable User	ExchangeEnableUser
External Email Address Updated	ExchangeUpdateUser
Hidden From Address Lists Enabled Updated	ExchangeUpdateUser
Mailbox Size Receipt Quota Updated	ExchangeUpdateUser
Mailbox Size Transmit Quota Updated	ExchangeUpdateUser
Mailbox Warning Size Updated	ExchangeUpdateUser
Maximum Recipients Updated	ExchangeUpdateUser
Max Incoming Message Size Updated	ExchangeUpdateUser
Max Outgoing Message Size Updated	ExchangeUpdateUser
Primary SMTP Address Updated	ExchangeUpdateUser
Retain Deleted Items Defaults Updated	ExchangeUpdateUser
Retain Deleted Items For Updated	ExchangeUpdateUser
Retain Deleted Items Until Backup Updated	ExchangeUpdateUser
Simple Display Name Updated	ExchangeUpdateUser
Use Storage Defaults Updated	ExchangeUpdateUser

## 1.8.2 Mailbox Fields for Provisioning

The Code Key column in [Table 1-4](#) contains the mailbox fields used in provisioning operations. The Decode column contains the corresponding fields on Microsoft Exchange.

See [Table 1-5](#) for the descriptions of these mailbox fields.

# 2

## Deploying the Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.

- [Preinstallation](#)
- [Installation](#)
- [Postinstallation](#)
- [Upgrading the Connector](#)
- [About Cloning the Connector](#)

### 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 *Creating a Target System User Account for Connector Operations of Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for information about creating that user account.

## 2.1 Preinstallation

Preinstallation involves installing, configuring, and running the connector server, enabling logging and so on.

- [Preinstallation on the Target System](#)
- [Installing, Configuring, and Running the Connector Server](#)
- [Enabling Logging](#)

### 2.1.1 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.

Depending on the Exchange Server version you are using, ensure the account meets the following requirements:

- [Privileges for Exchange 2007 Service Account](#)

- [Privileges for Exchange 2010 Service Account](#)
- [Privileges for Exchange 2013 Service Account](#)
- [Privileges for Exchange 2016 Service Account](#)

### 2.1.1.1 Privileges for Exchange 2007 Service Account

The following are the minimum privileges required for an Exchange 2007 service account to manage recipients (UserMailbox and MailUser):

- The service account must be a member of Exchange Recipient Administrators group.  
For more information, see <http://technet.microsoft.com/en-us/library/aa996881%28v=exchg.80%29.aspx>.
- If you want to add a recipient to a distribution group or remove a recipient from a distribution group, then the service account must also be a member of Account Operators group in the domain where the distribution group exists.  
For more information, see <http://technet.microsoft.com/en-us/library/bb124340%28v=exchg.80%29.aspx> and <http://technet.microsoft.com/en-us/library/aa997627%28v=exchg.80%29.aspx>.

### 2.1.1.2 Privileges for Exchange 2010 Service Account

This following is the minimum privilege required for an Exchange 2010 service account to manage recipients (UserMailbox and MailUser):

The service account must be a member of Recipient Management group.

For more information, see <http://technet.microsoft.com/en-us/library/dd298028%28v=exchg.141%29.aspx>.

### 2.1.1.3 Privileges for Exchange 2013 Service Account

This following is the minimum privilege required for an Exchange 2013 service account to manage recipients (UserMailbox and MailUser):

The service account must be a member of Recipient Management group.

For more information, see <https://technet.microsoft.com/en-us/library/dd298028%28v=exchg.150%29.aspx>.

### 2.1.1.4 Privileges for Exchange 2016 Service Account

The following is the minimum privilege required for an Exchange 2016 service account to manage recipients (UserMailbox and MailUser):

The service account must be a member of Recipient Management group.

For more information, see <https://docs.microsoft.com/en-us/Exchange/permissions/permissions?view=exchserver-2016>.

## 2.1.2 Installing, Configuring, and Running the Connector Server

The **connector server** is an application that enables remote execution of the Exchange connector. As the Exchange connector is implemented in .NET, it requires a .NET connector server. The connector server can either be installed on the same computer as that of the Exchange Server or on a different computer in the same domain as that of the Exchange Server.

For more information, see [Connector Architecture](#).

This section contains the following topics:

- [Prerequisites for the Connector Server](#)
- [Installing the Connector Server](#)
- [Configuring the Connector Server](#)
- [Enabling Logging](#)
- [Configuring Log File Rotation](#)
- [Running the Connector Server](#)

### 2.1.2.1 Prerequisites for the Connector Server

The following prerequisites and requirements must be met for the connector server:

- The computer hosting the connector server must have Intel Dual-Core Processor, 2 GHz with 4 GB RAM or a computer with similar configuration.  
If you have a computer dedicated to the connector server, then 2 GB RAM is sufficient.
- Before you install the connector server, ensure that you have installed .NET Framework 3.5 SP1 on the same computer where you are installing the connector server.

In addition, you must install the following patch:

<http://support.microsoft.com/kb/981575>

The .NET connector server need not be installed on the Exchange server target system. It can be installed either on the Exchange server or on a system that belongs to the same domain as that of the Exchange server.

- If you are using Exchange Server 2007, then you must install Exchange Management Tools on the computer hosting the connector server. This is a mandatory requirement.
- If you are using Exchange Server 2010, then TCP port 80 must be open between the computer hosting the connector server and the remote Exchange 2010 server, and the port must be allowed through Windows Firewall on the Exchange 2010 server. In addition, ensure other prerequisites are met for remote Shell as mentioned in the Remote Exchange Management page at:

<http://technet.microsoft.com/en-in/library/dd297932%28v=exchg.141%29.aspx>

## 2.1.2.2 Installing the Connector Server

To install the connector server:

 **Note:**

If you have already installed Connector Server 11.1.1.5.0, then you can skip this procedure.

1. Download the connector server package (a zip file such as Connector\_Server\_111200.zip) from the Oracle Identity Manager Connector Downloads page at:  
<http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html>
2. Extract the contents of the connector server package and locate the ServiceInstall-*version*.msi file, such as ServiceInstall-1.4.0.0.msi.
3. Install the connector server by running the ServiceInstall-1.4.0.0.msi file.

If the **Setup Type - Typical** option is used during the installation, then the connector server will be installed at the C:\Program Files\Identity Connector\Connector Server directory.

 **Note:**

In this guide, *CONNECTOR\_SERVER\_HOME* represents the C:\Program Files\Identity Connector\Connector Server directory or the directory where the connector server was installed.

4. Upon successful installation, the connector server is registered as a Windows service and will be started automatically.
5. Stop the connector server Windows service.

## 2.1.2.3 Configuring the Connector Server

To configure the connector server:

1. Open the connectorserver.exe.config file located in the *CONNECTOR\_SERVER\_HOME* directory. In the connectorserver.exe.config file, set the following properties, as required by your deployment.

Property	Description
connectorserver.port	Port on which the connector server listens for requests. Default value: 8759

Property	Description
connectorserver.usessl	If set to <b>true</b> , the connector server uses SSL for secure communication with Oracle Identity Manager. If this property is set to <b>true</b> , then you must set the corresponding property in Exchange connector server IT resource to <b>true</b> . To setup SSL between OIM and connector server, see <a href="#">Configuring SSL Between Oracle Identity Manager and Connector Server</a> . Default value: <b>false</b> .
Certificatestorename	If the connectorserver.usessl property is set to true, then this property should point to your certificate store name.
connectorserver.key	Connector server key. See Step 2 for information about setting this value.

2. Set The connector server key in the connectorserver.exe.config file, as follows:

 **Note:**

This key value must be mentioned in the Exchange connector server IT resource property.

- a. Open a command prompt and navigate to `CONNECTOR_SERVER_HOME` directory.
- b. Run the `ConnectorServer.exe /setKey` command.  
This displays the prompt **Enter Key:**
- c. Enter an appropriate key and press Enter.  
This displays the prompt **Confirm Key:**
- d. Enter the same key to confirm and press Enter.  
This displays the message Key Updated.

### 2.1.2.4 Enabling Logging

The Exchange connector uses the built-in logging mechanism of the .NET framework. Logging for the Exchange connector is not integrated with Oracle Identity Manager. The log level is set in the .NET connector server configuration file (`ConnectorServer.exe.config`).

By default, logging is not enabled for the connector. To enable logging:

1. Navigate to `CONNECTOR_SERVER_HOME` directory. The default directory is `C:\Program Files\Identity Connectors\Connector Server`.  
The `ConnectorServer.exe.config` file must be present in this directory.
2. Search and locate the tag `<add name="myListener"` under the `<listeners>` tag.
3. The connector logs all information in the file indicated by the **initializeData** parameter. The default value is `c:\connectorserver.log`.

Edit this value as per your deployment needs. As the connector server runs using the service account, ensure the service account has write permissions on the log location and on the log file. Otherwise, there would be no logs generated even if you enable logging.

4. In the ConnectorServer.exe.config file, add the lines shown in bold text:

```
<system.diagnostics>
  <trace autoflush="true" indentsize="4">
    <listeners>
      <remove name="Default" />
      <add name="myListener"
type="System.Diagnostics.TextWriterTraceListener"
initializeData="c:\connectorserver.log" traceOutputOptions="DateTime">
        <filter type="System.Diagnostics.EventTypeFilter"
initializeData="Information" />
      </add>
    </listeners>
  </trace>
  <switches>
    <add name="ExchangeSwitch" value="4" />
  </switches>
</system.diagnostics>
```

The value="4" sets the log level to Verbose. This value can be set as follows:

**Table 2-1 Log Levels**

Value	Log Level
value="4" or value="Verbose"	Verbose level. Most granular.
value="3" or value="Information"	Information level.
value="2" or value="Warning"	Warning level.
value="1" or value="Error"	Error level.
value="0"	No logging.

### 2.1.2.5 Configuring Log File Rotation

Information about events that occur during the course of reconciliation and provisioning operations are stored in a log file. As you use the connector over a period time, the amount of information written to a log file increases. If no rotation is performed, then log files become huge.

To avoid such a scenario, perform the procedure described in this section to configure rotation of the log file.

To configure rotation of a log file on a daily basis:

1. Log in to the computer that is hosting the connector server.
2. Stop the connector server.
3. Back up the ConnectorServer.exe.config file. The default location of this file is C:\Program Files\Identity Connectors\Connector Server.
4. In a text editor, open the ConnectorServer.exe.config file for editing.
5. Search for the <listeners> and </listeners> elements and replace the text between these elements with the following:

```
<remove name="Default" />
<add name="FileLog"
type="Microsoft.VisualBasic.Logging.FileLogTraceListener,Microsoft.VisualBasic,Version=8.0.0.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"
initializeData="FileLogWriter"
traceOutputOptions="DateTime"
BaseFileName="ConnectorServerDaily"
Location="Custom"
CustomLocation="C:\ConnectorServerLog\"
LogFileCreationSchedule="Daily">
<filter type="System.Diagnostics.EventTypeFilter"
initializeData="Information"/>
</add>
```

6. Save the file and close it.
7. Start the connector server.

#### See Also:

The following URL for more information about configuring log file rotation:

<http://msdn.microsoft.com/en-us/library/microsoft.visualbasic.logging.filelogtracelistener.aspx>

## 2.1.2.6 Running the Connector Server

To run the connector server, perform one of the following steps depending on the Exchange Server version:

- If you are using Exchange Server 2007:
  1. Login to computer hosting the connector server.  
The login user must have permissions to perform the following steps.
  2. Open Windows services explorer. To do so:  
Click the **Start** button, then click to **Run...** Enter `Services.msc` and click **OK**.
  3. Locate the **Connector Server** service.
  4. Right-click on the service and click **Properties**.
  5. Click the **Log On** tab and select **This Account**.
  6. Click **Browse** to choose the service account having minimum privileges as described in [Privileges for Exchange 2007 Service Account](#). Then, enter password for this service account.
  7. Click **OK**.
  8. With this service selected, click **Run**.

After the above steps are completed successfully, the connector server runs with the service account that has the minimum privileges to perform recipient management tasks on Exchange Server 2007.

 **Note:**

The above steps are mandatory and must be completed successfully. This is because the Exchange connector uses the credentials of the user who starts the connector server to communicate with Exchange Server 2007. The user name and password information provided in the IT resource is not used.

- If you are using Exchange Server 2010:
  1. Login to computer hosting the connector server.  
The login user must have permissions to perform the following steps.
  2. Open Windows services explorer. To do so:  
Click the **Start** button, then click to **Run...** Then, enter `Services.msc` and click **OK**.
  3. Locate the **Connector Server** service and click **Run**.

 **Note:**

The Exchange connector uses the user credentials provided in the Exchange IT Resource. For more information, see [Configuring the IT Resource for the Target System](#). As the connector uses credentials provided in the IT resource to communicate with Exchange Server, any user can start the connector server.

Alternatively, the connector server can be started by the service account having minimum privileges as described in [Privileges for Exchange 2010 Service Account](#).

## 2.2 Installation

You must install the connector in Oracle Identity Manager and in the connector server.

The following sections provide information about installation:

- [Installing the Connector in Oracle Identity Manager](#)
- [Deploying the Connector Bundle on the Connector Server](#)

### 2.2.1 Installing the Connector in Oracle Identity Manager

Installation on Oracle Identity Manager involves running the connector installer and configuring the IT resource.

- [Running the Connector Installer](#)
- [Configuring the IT Resource for the Target System](#)

## 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/server/ConnectorDefaultDirectory`

 **Note:**

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

2. If you are using Oracle Identity Manager release 11.1.1., then:
  - a. Log in to the Administrative and User Console.
  - b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.
3. If you are using Oracle Identity Manager release 11.1.2.x, then:
  - a. Log in to Oracle Identity System Administration.
  - b. In the left pane, under System Management, click **Manage Connector**.
4. In the Manage Connector page, click **Install**.
5. From the Connector List list, select **Exchange Connector 11.1.1.6.0**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation in Step 1.

If you have copied the installation files into a different directory, then:

- a. In the **Alternative Directory** field, enter the full path and name of that directory.
  - b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
  - c. From the Connector List list, select **Exchange Connector 11.1.1.6.0**.
6. Click **Load**.
  7. 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.
8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:
    - a. Ensuring that the prerequisites for using the connector are addressed

 **Note:**

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

There are no prerequisites for some predefined connectors.

- b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

- c. Configuring the scheduled tasks

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 A-1](#).

## 2.2.1.2 Configuring the IT Resource for the Target System

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 both provisioning and reconciliation, the Microsoft Exchange connector uses Exchange IT Resource. This IT resource is created with default parameter values as part of the connector installation. You must update the IT resource parameters with information about the target system.

To configure the Microsoft Exchange Server IT resource:

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

- For Oracle Identity Manager release 11.1.1:  
Log in to the Administrative and User Console.
  - For Oracle Identity Manager release 11.1.2.x:  
Log in to Oracle Identity System Administration.
2. If you are using Oracle Identity Manager release 11.1.1, then:
    - a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
    - b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
  3. If you are using Oracle Identity Manager release 11.1.2.x, then in the left pane under Configuration, click **IT Resource**.
  4. In the IT Resource Name field on the Manage IT Resource page, enter `Exchange IT Resource` and then click **Search**.
  5. Click the edit icon corresponding to the Exchange IT resource.
  6. From the list at the top of the page, select **Details and Parameters**.
  7. Specify values for the parameters of the Exchange IT resource.

The following screenshot shows the Edit IT Resource Details and Parameters page for Exchange 2007:

**View IT Resource Details and Parameters**

You can view additional information about this IT resource : Details and Parameters

IT Resource Name: Exchange IT Resource  
IT Resource Type: Exchange Server

Parameter	Value
Configuration Lookup	Lookup.Exchange.Configuration
Connector Server Name	Exchange Connector Server
ExchangeServerHost	
ExchangeServerType	OnPremise2007
ExchangeUser	
ExchangeUserPassword	

[Edit](#)

[Back to Search Results](#)

### Note:

The ExchangeUser, ExchangeServerHost, and ExchangeUserPassword properties are not required if Exchange Server version is 2007. The connector uses the credentials of the user who started the connector server to connect to Exchange Server. This user is the service account having minimum privileges described in [Privileges for Exchange 2007 Service Account](#).

As the Exchange Management Tools are installed on connector server host computer, the connector knows to which Exchange Server it should connect to.

The following screenshot shows the Edit IT Resource Details and Parameters page for Exchange 2010:

**View IT Resource Details and Parameters**

You can view additional information about this IT resource : [Details and Parameters](#)

IT Resource Name: Exchange IT Resource  
IT Resource Type: Exchange Server

Parameter	Value
Configuration Lookup	Lookup.Exchange.Configuration
Connector Server Name	Exchange Connector Server
ExchangeServerHost	ExchangeServerHostName.example.com
ExchangeServerType	OnPremise2010
ExchangeUser	example\ExchangeServiceAccount
ExchangeUserPassword	*****

[Edit](#)

[Back to Search Results](#)

**Note:**

The ExchangeUser, ExchangeServerHost, and ExchangeUserPassword properties are required. The connector uses these properties to connect remotely to Exchange Server.

The ExchangeUser specified is the service account having minimum privileges described in [Privileges for Exchange 2010 Service Account](#).

[Table 2-2](#) describes each parameter of the Exchange IT resource.

**Table 2-2 Parameters of the Exchange IT Resource for the Target System**

Parameter	Description
Configuration Lookup	This parameter holds the name of the lookup definition that stores configuration information used during reconciliation and provisioning. Default value: Lookup.Exchange.Configuration
Connector Server Name	Name of the IT resource of the type "Connector Server." A default IT resource for the connector server is created during the connector installation. See <a href="#">Configuring the IT Resource for the Connector Server</a> for information about modifying the default IT resource. Default value: Exchange Connector Server
ExchangeServerType	Enter the type of Microsoft Exchange Server. For Exchange 2007, set the value to OnPremise2007. For Exchange 2010, set the value to OnPremise2010. For Exchange 2013, set the value to OnPremise2013. For Exchange 2016, set the value to OnPremise2016. Default value: OnPremise2007

**Table 2-2 (Cont.) Parameters of the Exchange IT Resource for the Target System**

Parameter	Description
ExchangeServerHost	Hostname of the computer hosting Exchange Server 2010, 2013, or 2016. This is required only if ExchangeServerType is set to OnPremise2010, OnPremise2013, or OnPremise2016.
ExchangeUser	User name of the service account having minimum privileges described in <a href="#">Privileges for Exchange 2010 Service Account</a> . Format: DomainName\UserName This is required only if ExchangeServerType is set to OnPremise2010, OnPremise2013, or OnPremise2016.
ExchangeUserPassword	Valid password for user specified for the ExchangeUser parameter. This is required only if ExchangeServerType is set to OnPremise2010, OnPremise2013, or OnPremise2016.

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

## 2.2.2 Deploying the Connector Bundle on the Connector Server

To deploy the connector bundle on the connector server, you must copy and extract the connector bundle to the connector server and then configure the IT resource for the connector server.

- [Copying and Extracting the Connector Bundle to the Connector Server](#)
- [Configuring the IT Resource for the Connector Server](#)

### 2.2.2.1 Copying and Extracting the Connector Bundle to the Connector Server

To copy and extract the connector bundle to the connector server:

#### Note:

If a single connector server is used for both Active Directory and Exchange connectors, and if the connector server already has the Active Directory connector DLL, do *not* update connector server with Active Directory connector DLL provided as part of the Exchange connector bundle ZIP file.

1. Stop the connector server.
2. From the installation media, copy and extract contents of the bundle/Exchange.Connector-2.0.0.1.zip file to the `CONNECTOR_SERVER_HOME` directory.
3. Start the connector server. See [Running the Connector Server](#) for information about starting the connector server.

### 2.2.2.2 Configuring the IT Resource for the Connector Server

During the installation of the connector, a default IT resource for the connector server for Microsoft Exchange is created with the name, Exchange connector server.

To configure or modify the IT resource for the connector server:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
  - For Oracle Identity Manager release 11.1.1:  
Log in to the Administrative and User Console.
  - For Oracle Identity Manager release 11.1.2.x:  
Log in to Oracle Identity System Administration.
2. If you are using Oracle Identity Manager release 11.1.1, then:
  - a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
  - b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.x, then in the left pane under Configuration, click **IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `Exchange Connector Server` and then click **Search**.
5. Click the edit icon corresponding to the Exchange connector server IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the Exchange connector server IT resource. [Figure 2-1](#) shows the Edit IT Resource Details and Parameters page.

**Figure 2-1 Edit IT Resource Details and Parameters Page for the Exchange Connector Server IT Resource**



[Table 2-3](#) provides information about the parameters of the Exchange connector server IT resource.

**Table 2-3 Parameters of the Exchange Connector Server IT Resource**

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: HostName
Key	Enter the key for the connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: 8759
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. If the value is zero or if no value is specified, the timeout is unlimited. Sample value: 300
UseSSL	Enter <code>true</code> to specify that you will configure SSL between Oracle Identity Manager and the connector server. Otherwise, enter <code>false</code> . Default value: <code>false</code> <b>See Also:</b> <a href="#">Configuring SSL Between Oracle Identity Manager and Connector Server</a> for information about enabling SSL

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

## 2.3 Postinstallation

Postinstallation involves configuring Oracle Identity Manager, localizing field labels, clearing server cache, configuring SSL, and so on.

- [Configuring Oracle Identity Manager 11.1.2 or Later](#)
- [Localizing Field Labels in UI Forms](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [Linking the Exchange Resource Object with the AD User Resource Object](#)
- [Configuring Oracle Identity Manager for Request-Based Provisioning](#)
- [Configuring SSL Between Oracle Identity Manager and Connector Server](#)
- [Setting up the Lookup Definition for Connection Pooling](#)

### 2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

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

These procedures are described in the following sections:

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Creating an Application Instance](#)
- [Publishing a Sandbox](#)
- [Harvesting Entitlements and Sync Catalog](#)

- [Updating an Existing Application Instance with a New Form](#)

### 2.3.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see *Managing Sandboxes in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

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

### 2.3.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see *Managing Forms in Oracle Fusion Middleware Administering Oracle Identity Manager*.

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

### 2.3.1.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see *Managing Application Instances in Oracle Fusion Middleware Administering Oracle Identity Manager*.

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

5. Publish the application instance for a particular organization.

 **Note:**

If you are using access policy-based provisioning, then specify the Active Directory connector application instance as the value for the Parent ApplInstance attribute.

### 2.3.1.4 Publishing a Sandbox

To publish the sandbox that you created in [Creating and Activating a Sandbox](#):

1. Close all the open tabs and pages.
2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in [Creating and Activating a Sandbox](#).
3. On the toolbar, click **Publish Sandbox**. A message is displayed asking for confirmation.
4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

### 2.3.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in [Scheduled Tasks for Lookup Field Synchronization](#).
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

### 2.3.1.6 Updating an Existing Application Instance with a New Form

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

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

## 2.3.2 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. Resource bundles are available in the connector installation media.



### Note:

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

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:
  - For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0) or later:  
`SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf`
  - For releases prior to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):  
`SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf`
6. Edit the BizEditorBundle.xlf file in the following manner:
  - a. Search for the following text:

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

- b. Replace with the following text:

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

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

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

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

```

<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_EXCHANGE_DISPLAYNAME__c_description']}]">
<source>Display Name</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ExchUserForm.entity.ExchU
serFormEO.UD_EXCHANGE_DISPLAYNAME__c_LABEL">
<source>Display Name</source>
<target/>
</trans-unit>

```

- d. Open the resource file from the connector package, for example `Exchange_fr.properties`, and get the value of the attribute from the file, for example, `global.udf.UD_EXCHANGE_DISPLAYNAME=Nom d'affichage`.
- e. Replace the original code shown in Step 6.c with the following:

```

<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_EXCHANGE_DISPLAYNAME__c_description']}]">
<source>Display Name</source>
<target>Nom d'affichage</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ExchUserForm.entity.ExchU
serFormEO.UD_EXCHANGE_DISPLAYNAME__c_LABEL">
<source>Display Name</source>
<target>Nom d'affichage</target>
</trans-unit>

```

- f. Repeat Steps 6.a through 6.d for all attributes of the process form.
  - g. Save the file as `BizEditorBundle_LANG_CODE.xlf`. In this file name, replace `LANG_CODE` with the code of the language to which you are localizing.  
Sample file name: `BizEditorBundle_fr.xlf`.
7. Repackage the ZIP file and import it into MDS.

#### See Also:

Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*, for more information about exporting and importing metadata files

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

## 2.3.3 Clearing Content Related to Connector Resource Bundles from the Server Cache

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database.

Whenever you add a new resource bundle to the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

 **Note:**

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

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

1. In a command window, switch to the `OIM_HOME/server/bin` directory.
2. Enter one of the following commands:

 **Note:**

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

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

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

On Microsoft Windows: `PurgeCache.bat All`

On UNIX: `PurgeCache.sh All`

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

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

In this format:

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

## 2.3.4 Linking the Exchange Resource Object with the AD User Resource Object

To link the Exchange resource object with the AD User resource object:

1. On the Design Console, expand **Resource Management** and then double-click **Resource Objects**.

2. Search for and open the **AD User** resource object.
3. On the Status Definition sub tab of the Resource Object tab, ensure that the **Disabled** and **Revoked** check boxes are selected.
4. To save the changes to the AD User resource object, click the Save icon.
5. Search for and open the **Exchange** resource object.
6. On the Depends On sub tab of the Resource Object tab, click **Assign**.
7. In the Assigned Objects Dialog box, move the **AD User** resource object from Unassigned Objects to Assigned Objects.
8. Click **OK**.
9. To save the changes to the Exchange resource object, click the Save icon.

## 2.3.5 Configuring Oracle Identity Manager for Request-Based Provisioning

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

### Note:

Perform the procedure described in this section only if both the conditions are true:

- You are using Oracle Identity Manager release 11.1.1.
- You want to perform request-based provisioning operations.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

### Note:

Direct provisioning allows the provisioning of multiple Microsoft Exchange accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

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

- [Importing Request Datasets Using Deployment Manager](#)
- [Copying Predefined Request Datasets](#)
- [Importing Request Datasets into MDS](#)
- [Enabling the Auto Save Form Feature](#)
- [Running the PurgeCache Utility](#)

### 2.3.5.1 Importing Request Datasets Using Deployment Manager

**Note:**

You can perform this procedure instead of the procedures described in [Copying Predefined Request Datasets](#) and [Importing Request Datasets into MDS](#).

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

To import a request dataset XML file by using the Deployment Manager:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management.

A dialog box for opening files is displayed.

4. Locate and open the request dataset XML file, Exchange-Datasets.xml, which is in the xml directory of the installation media.

Details of this XML file are shown on the **File Preview** page.

5. Click **Add File**.

The Substitutions page is displayed.

6. Click **Next**.

The Confirmation page is displayed.

7. Click **Import**.

8. Close the Deployment Manager dialog box.

The request dataset is imported into Oracle Identity Manager.

### 2.3.5.2 Copying Predefined Request Datasets

Predefined request datasets are shipped with this connector. The following is list of predefined request datasets available in the DataSet directory on the installation media:

ModifyResourceExchange.xml

ProvisionResourceExchange.xml

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

`/custom/connector/RESOURCE_NAME`

For example:

E:\MyDatasets\custom\connector\Exchng

 **Note:**

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

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

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets.

### 2.3.5.3 Importing Request Datasets into MDS

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

To import a request dataset definition into MDS:

1. Set up the environment for running the MDS Import utility as follows:
  - a. Set Environment Variable: Set the `OIM_ORACLE_HOME` environment variable to the Oracle Identity Management Oracle home directory inside the Middleware home directory. For example, for Microsoft Windows, set the `OIM_ORACLE_HOME` environment variable to `C:\Oracle\Middleware\Oracle_IDM1\` directory.
  - b. Set Up the Properties File: Set the necessary properties in the `weblogic.properties` file, which is located in the same folder as the utilities.

 **Note:**

While setting up the properties in the `weblogic.properties` file, ensure that the value of the `metadata_from_loc` property is the parent directory of the `/custom/connector/RESOURCE_NAME` directory. For example, while performing the procedure in [Copying Predefined Request Datasets](#), if you copy the files to the `E:\MyDatasets\custom\connector\Exchng` directory, then set the value of the `metada_from_loc` property to `E:\MyDatasets`.

**Table 2-4 Parameters in the Properties File**

Property Name	Description	Notes
<code>wls_servername</code>	Name of the Oracle WebLogic Server on which Oracle Identity Manager is deployed	

**Table 2-4 (Cont.) Parameters in the Properties File**

Property Name	Description	Notes
application_name	The application name	Value is: <ul style="list-style-type: none"> <li>oim if importing/exporting an out-of-the-box event handler.</li> <li>OIMMetadata for customizable metadata.</li> </ul> If importing or exporting custom data, set application_name to OIMMetadata.
metadata_from_loc	Directory location from which an XML file should be imported. This property is used by weblogicImportMetadata.sh script.	Microsoft Windows paths include // as file or directory separator.
metadata_to_loc	Directory location from which an XML file should be imported. This property is used by weblogicExportMetadata.sh script.	Microsoft Windows paths include // as file or directory separator.
metadata_files	Full path and name of an XML file. This property is used by weblogicExportMetadata.sh and weblogicDeleteMetadata.sh scripts.	For example, you may specify /file/User.xml to export a user entity definition. You can indicate multiple xml files as comma-separated values.

2. In a command window, change to the *OIM\_HOME*\server\bin directory.

3. Run one of the following commands:

- On Microsoft Windows

```
weblogicImportMetadata.bat
```

- On UNIX

```
weblogicImportMetadata.sh
```

4. When prompted, enter the following values:

- Please enter your username [weblogic]

Enter the username used to log in to WebLogic server

Sample value: WL\_User

- Please enter your password [weblogic]

Enter the password used to log in to WebLogic server

- Please enter your server URL [t3://localhost:7001]

Enter the URL of the application server in the following format:

```
t3://HOST_NAME_IP_ADDRESS:PORT
```

In this format, replace:

*HOST\_NAME\_IP\_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

*PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS at the following location:

*/custom/connector/RESOURCE\_NAME*

### 2.3.5.4 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

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

### 2.3.5.5 Running the PurgeCache Utility

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

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

## 2.3.6 Configuring SSL Between Oracle Identity Manager and Connector Server

You must configure SSL to secure communication between Oracle Identity Manager and Connector Server.

This procedure is mandatory if the connector server and the Exchange bundle are installed on the target system.

The following sections provide information about configuring SSL between Oracle Identity manager and connector server:

- [Installing Certificate Services on Windows Server 2003](#)
- [Installing Certificate Services for Windows Server 2008](#)
- [Exporting the Certificate](#)
- [Configuring the Connector Server for SSL](#)
- [Configuring Oracle Identity Manager for SSL](#)

### 2.3.6.1 Installing Certificate Services on Windows Server 2003

Before you configure SSL, you must install Certificate Services on the target system host computer:

To install Certificate Services on the target system host computer:

 **Note:**

Before you begin installing Certificate Services, you must ensure that Internet Information Services (IIS) is installed on the target system host computer.

1. Insert the operating system installation media into the CD-ROM or DVD drive.
2. Click **Start**, **Settings**, and **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. Click **Add/Remove Windows Components**.
5. Select **Certificate Services**.
6. In the Windows Components Wizard, follow the instructions to start Certificate Services.

 **Note:**

While providing input to the wizard, select **Enterprise root CA** as the CA type. This is required for adding a policy with the Domain Controller template, which is a step that you perform in the next procedure.

### 2.3.6.2 Installing Certificate Services for Windows Server 2008

To install Certificate Services on the target system host computer:

1. Select **Administrative Tools** from the Control Panel to open the Server Manager Window.

 **Note:**

Ensure that the Web Server IIS role has been added from the Server Manager.

2. In the Select Server Roles window of the installation wizard, select **Active Directory Certificate Services** and click **Next**. The Introduction to Active Directory Certificate Services window appears.
3. In the Introduction to Active Directory Certificate Services window, click **Next**. The Role Services window appears.
4. In the Role Services window, select the **Certification Authority** and **Certification Authority Web Enrollment** options and click **Next**. The Specify Setup Type window appears.
5. In the Specify Setup Type window, select **Enterprise** and click **Next**. The Specify CA Type window appears.
6. In the Specify CA Type window, select **Root CA** and click **Next**. The Set Up Private Key window appears.

7. In the Set Up Private Key window, select **Create a new private key** and click **Next**. The Configure Cryptography for CA window appears.
8. In the Configure Cryptography for CA page, select a value for the Key character length field from the drop-down list and click **Next**. The Configure CA Name window appears.
9. In the Configure CA Name window, specify values for the available fields and click **Next**. The Set Validity Period window appears.
10. In the Set Validity Period window, specify values for the available fields and click **Next**. The Configure Certificate Database window appears.
11. In the Configure Certificate Database window, specify values for the available fields and click **Next**. The Confirm Installation Selections window appears.
12. In the Confirm Installation Selections window, review the presented information, click **Install**, then click **Close**.

### 2.3.6.3 Exporting the Certificate

To export the certificate generated by CA:

1. Click **Start** and then **Run**.
2. Enter the following command, and then click OK:  

```
mmc
```

The Microsoft Management Console is displayed.
3. In the Console Root window, on the left pane, expand **Certificates - Local Computer), Personal**, and then **Certificates**.
4. Right-click **Certificates**, select **All Tasks**, and then click **Export**.
5. In the wizard that is displayed, select all default values to create a certificate file (.cer). Ensure to specify a file name (for example, C:\ExchangeSSLCer.cer) in the wizard, and then click **Finish**.

### 2.3.6.4 Configuring the Connector Server for SSL

To configure the connector server for SSL:

1. Create a certificate store and add the certificate created in [Exporting the Certificate](#) to the store. To do so:
2. In a command window, enter the following:

```
C:\>certutil -f -addstore sslstore C:\ExchangeSSLCer.cer
```

This command creates a new certificate store with the name 'sslstore' and adds the certificate ExchangeSSLCer to this store.

3. Navigate to the location where connector server is installed and locate the Connector Server\ConnectorServer.exe.Config file.
4. In a text editor, open the ConnectorServer.exe.Config file for editing:
5. Change the values of the following lines:

From:

```
<add key="connectorserver.usssl" value="false" />
```

```
<add key="connectorserver.certificatestorename"
value="ConnectorServerSSLCertificate" />
```

To:

```
<add key="connectorserver.usessl" value="true" />
<add key="connectorserver.certificatestorename" value="sslstore" />
```

6. Restart the connector server.

### 2.3.6.5 Configuring Oracle Identity Manager for SSL

The following is the procedure to configure Oracle Identity Manager for SSL:

1. Copy the certificate generated in Step 1 of [Configuring the Connector Server for SSL](#) to the computer on which Oracle Identity Manager is running.
2. Import the target system certificate into the JDK used by Oracle Identity Manager by running the following command:

- For Oracle Identity Manager running on Oracle WebLogic Application Server:

```
keytool -import -keystore MY_CACERTS -file CERT_FILE_NAME -
storepass PASSWORD
```

In this command:

- *MY\_CACERTS* is the full path and name of the certificate store (the default is cacerts).

- *CERT\_FILE\_NAME* is the full path and name of the certificate file.

- *PASSWORD* is the password of the keystore.

The following is a sample command:

```
keytool -import -keystore /home/testoc4j/OIM/
jrockit_160_14_R27.6.5-32/jre/lib/security/cacerts -file /home/
ExchangeSSLCer.cer -storepass changeit
```

- For Oracle Identity Manager running on IBM WebSphere Application Server:

In a terminal window, change to the *WEBSPHERE\_HOME\AppServer\java\jre\bin* directory and run the following command:

```
keytool -import -alias ALIAS_NAME -keystore MY_CACERTS -file
CERT_FILE_NAME -storepass PASSWORD
```

In this command:

- *ALIAS\_NAME* is the alias for the certificate store.

- *MY\_CACERTS* is the full path and name of the certificate store (the default is cacerts).

- *CERT\_FILE\_NAME* is the full path and name of the certificate file.

- *PASSWORD* is the password of the keystore.

The following is a sample command:

```
keytool -import -alias exchange_cert -keystore /scratch/jdoe/r2was/
was9461/java/jre/lib/security/cacerts -file /scratch/jdoe/first/
CS.cer -storepass changeit
```

3. Import the target system certificate into the keystore of the application server by running the following command:

- For Oracle Identity Manager running on Oracle WebLogic Application Server:

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -  
file CERT_FILE_NAME -storepass PASSWORD
```

In this command:

- *CERT\_FILE\_NAME* is the full path and name of the certificate file.

- *PASSWORD* is the password of the keystore.

The following is a sample command:

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/  
DemoTrust.jks -file /home/ExchangeSSLCer.cer -storepass  
DemoTrustKeyStorePassPhrase
```

- For Oracle Identity Manager running on IBM WebSphere Application Server:

In a terminal window, change to the *WEBSHERE\_HOME*\AppServer\java\jre\bin directory and run the following command:

```
keytool -import -alias ALIAS_NAME -keystore $WAS_PROFILE_HOME/  
config/cells/DefaultCell01/trust.p12 -storetype PKCS12 -file  
CERT_FILE_NAME -storepass PASSWORD
```

In this command:

- *ALIAS\_NAME* is the alias for the certificate store.

- *MY\_CACERTS* is the full path and name of the certificate store (the default is cacerts).

- *CERT\_FILE\_NAME* is the full path and name of the certificate file.

- *PASSWORD* is the password of the keystore.

The following is a sample command:

```
keytool -import -alias exchange_cert -keystore /scratch/jdoe/r2was/  
was9461/java/jre/lib/security/cacerts -file /scratch/jdoe/first/  
CS.cer -storepass changeit
```

```
keytool -import -alias exchange_cert -keystore /scratch/jdoe/r2was/  
was9461/profiles/Custom01/config/cells/DefaultCell01/trust.p12 -  
storetype PKCS12 -file /scratch/jdoe/first/CS.cer -storepass WebAS
```

4. Set the value of the UseSSL parameter of the connector server IT resource to true.

## 2.3.7 Setting up the Lookup Definition for Connection Pooling

By default, this connector uses the ICF connection pooling. Learn about the connection pooling properties for this connector, their description, and default values set in ICF:

**Table 2-5 Connection Pooling Properties**

Property	Description
Pool Max Idle	Maximum number of idle objects in a pool. Default value: 10
Pool Max Size	Maximum number of connections that the pool can create. Default value: 10
Pool Max Wait	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: 150000
Pool Min Evict Idle Time	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: 120000
Pool Min Idle	Minimum number of idle objects in a pool. Default value: 1

If you want to modify the connection pooling properties to use values that suit requirements in your environment, then:

1. Log in to the Design Console.
2. Expand **Administration**, and then double-click **Lookup Definition**.
3. Search for and open the **Lookup.Exchange.Configuration** lookup definition.  
See [Lookup.Exchange.Configuration](#) for more information about this lookup.
4. On the Lookup Code Information tab, click **Add**.  
A new row is added.
5. In the **Code Key** column of the new row, enter `Pool Max Idle`.
6. In the **Decode** column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in [Table 2-5](#).
8. Click the save icon.

## 2.4 Upgrading the Connector

If you have already deployed an earlier release of this connector, then upgrade the connector to the current release.

The following sections discuss the procedure to upgrade the connector:

- [Preupgrade Steps](#)

- [Upgrade Steps](#)
- [Postupgrade Steps](#)

 **Note:**

Before you perform the upgrade procedure:

- It is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- Upgrade the Microsoft Active Directory connector.
- As a best practice, first perform the upgrade procedure in a test environment.

## 2.4.1 Preupgrade Steps

Preupgrade involves performing certain procedures such as performing a reconciliation run to fetch all the latest updates to Oracle Identity Manager and then disabling the scheduled tasks, defining the source connector and so on.

Perform the following preupgrade steps:

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Perform the preupgrade procedure documented in *Managing Connector Lifecycle of Oracle Fusion Middleware Administering Oracle Identity Manager*.
3. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector. See *Managing Connector Lifecycle in Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.

## 2.4.2 Upgrade Steps

This is a summary of the procedure to upgrade the connector for both staging and production environments.

Depending on the environment in which you are upgrading the connector, perform one of the following steps:

- **Staging Environment**  
Perform the upgrade procedure by using the wizard mode.
- **Production Environment**  
Perform the upgrade procedure by using the silent mode.

See *Managing Connector Lifecycle in Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the wizard and silent modes.

## 2.4.3 Postupgrade Steps

Postupgrade involves copying connector code files, configuring the IT resource and scheduled tasks, running the FVC utility and so on.

Perform the following procedure:

1. Perform the postupgrade procedure documented in *Managing Connector Lifecycle of Oracle Fusion Middleware Administering Oracle Identity Manager*.
2. If you are using Oracle Identity Manager release 11.1.2.x or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
  - a. Log in to Oracle Identity System Administration.
  - b. Create and activate a sandbox. See [Creating and Activating a Sandbox](#) for more information.
  - c. Create a new UI form to view the upgraded fields. See [Creating a New UI Form](#) for more information about creating a UI form.
  - d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 2.c), and then save the application instance.
  - e. Publish the sandbox. See [Publishing a Sandbox](#) for more information.
3. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so:
  - a. In a text editor, open the `fvc.properties` file located in the `OIM_DC_HOME` directory and include the following entries:

```
ResourceObject;Exchange User
FormName;UD_MSEXCHG
FromVersion;v1
ToVersion;v_11.1.1.6.0
Parent;UD_MSEXCHG_RECIPIENTTYPE;UserMailbox
ParentParent;UD_MSEXCHG_EXCHANGEITRESOURCE;UD_MSEXCHG_SERVER
```

- b. Run the FVC utility. This utility is copied into the following directory when you install the design console:

**For Microsoft Windows:**

`OIM_DC_HOME/fvcutil.bat`

**For UNIX:**

`OIM_DC_HOME/fvcutil.sh`

When you run this utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, and the logger level and log file location.

- b.
4. If you are upgrading the connector from release 9.x to 11.x, then run the `PostUpgradeScript.sql` script as follows:

 **Note:**

Skip performing this step if you are upgrading the connector from release 11.1.1.5.0 to 11.1.1.6.0.

- a. Connect to the Oracle Identity Manager database by using the OIM User credentials.
- b. Run the PostUpgradeScript.sql located in the `OIM_HOME/server/ConnectorDefaultDirectory/EXCHANGE_PACKAGE/upgrade` directory.
5. Deploy the connector server. See [Installing, Configuring, and Running the Connector Server](#) for more information.
6. Re-configure the IT resource of the source connector (an earlier release of the connector that must be upgraded). See [Configuring the IT Resource for the Target System](#) for information about configuring the IT resource.

## 2.5 About Cloning the Connector

You can clone the Exchange connector by setting new names for some of the objects that comprise the connector.

The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

 **See Also:**

Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about cloning connectors and the steps mentioned in this section

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- **Lookup Definition**

If the lookup definition contains the old lookup definition details, then you must modify it to provide the new cloned lookup definition names. If the Code Key and Decode values are referring the base connector attribute references, then replace these with new cloned attributes.
- **Scheduled Task**

You must replace the base connector resource object name in the scheduled task with the cloned resource object name. If the scheduled task parameter has any data referring to the base connector artifacts or attributes, then these must be replaced with the new cloned connector artifacts or attributes.

- Child Table

You must reassign the adapter and add a new literal value to the `childTableName` variable of a child table after cloning the connector.

To update a child table, such as Distribution Group Insert and Distribution Group Update process tasks of the Exchange connector:

1. Log in to Design Console.
2. Open the process task and click Integrations tab.
3. Click **Remove** to unassign the adapter to the process task.
4. Click **Add** to assign the same adapter to the process task.
5. Assign a new literal value to the `childTableName` variable.
6. Map the other adapter variables as per the previous mappings.

- Localization Properties

You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

For example, the process form attributes are referenced in the Japanese properties file, `Exchange_ja.properties`, as `global.udf.UD_EXCHANGE_ALIASNAME`. During cloning, if you change the process form name from `UD_EXCHANGE` to `UD_EXCHANG1`, then you must update the process form attributes to `global.udf.UD_EXCHANG1_ALIASNAME`.

# 3

## Using the Connector

You can use the connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.

This chapter contains the following sections:

- [Guidelines on Using the Connector](#)
- [Scheduled Tasks for Lookup Field Synchronization](#)
- [Configuring Reconciliation](#)
- [Configuring Scheduled Tasks](#)
- [Configuring Provisioning in Oracle Identity Manager Release 11.1.1](#)
- [Configuring Provisioning in Oracle Identity Manager Release 11.1.2](#)
- [Configuring Action Scripts](#)

### 3.1 Guidelines on Using the Connector

These are the guidelines that you must apply while using the connector for reconciliation and provisioning operations.

- [Guidelines on Configuring Reconciliation](#)
- [Guidelines on Performing Provisioning Operations](#)

#### 3.1.1 Guidelines on Configuring Reconciliation

Apply these guidelines while configuring reconciliation.

- Before a target resource reconciliation run is performed, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before user reconciliation runs.

If you are using Oracle Identity Manager 11.1.2.x or later, then you must also run the Entitlement List and Catalog Synchronization Job scheduled jobs.

- The scheduled task for user reconciliation must be run before the scheduled task for reconciliation of deleted user data.

#### 3.1.2 Guidelines on Performing Provisioning Operations

Apply these guidelines while performing provisioning operations.

- Before performing provisioning operations, you must reconcile all lookup definitions.
- Before provisioning Exchange User, you must provision AD User.
- If you select the user type as UserMailbox, then the Database field on the process form is mandatory. If you select the user type as MailUser, then External E-mail Address field on the process form is mandatory.

- Specifying multibyte values for fields

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.

## 3.2 Scheduled Tasks for Lookup Field Synchronization

Scheduled tasks for lookup field synchronization fetch the most recent values from specific fields in the target system to lookup definitions in Oracle Identity Manager. These lookup definitions are used as an input source for lookup fields in Oracle Identity Manager.

The following are the scheduled tasks for lookup field synchronization:



### Note:

The procedure to configure these scheduled tasks is described later in the guide.

- Exchange User Distribution Group Lookup Reconciliation

This scheduled task fetches all mail-enabled universal distribution groups present in the forest into the Lookup.Exchange.DistributionGroups lookup definition.

- Exchange User Mailbox Database Group Lookup Reconciliation

This scheduled task is used to synchronize mailbox database lookup fields in Oracle Identity Manager with mailbox databases in the target system.

[Table 3-1](#) describes the attributes of both scheduled tasks.

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

Attribute	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: <code>__NAME__</code> <b>Note:</b> Do <i>not</i> change the value of this attribute.

**Table 3-1 (Cont.) Attributes of the Scheduled Tasks for Lookup Field Synchronization**

Attribute	Description
Decode Attribute	Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: <code>__NAME__</code> <b>Note:</b> Do <i>not</i> change the value of this attribute.
IT Resource Name	Name of the IT resource for the target system installation from which you want to reconcile records. Default value: <code>Exchange IT Resource</code>
Lookup Name	Name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled task you are using, the default values are as follows: <ul style="list-style-type: none"> <li>For Exchange User Distribution Group Lookup Reconciliation: <code>Lookup.Exchange.DistributionGroups</code></li> <li>For Exchange User Mailbox Database Group Lookup Reconciliation: <code>Lookup.Exchange.MailboxDatabase</code></li> </ul>
Object Type	Name of the type of object you want to reconcile. Depending on the scheduled task you are using, the default values are as follows: <ul style="list-style-type: none"> <li>For Exchange User Distribution Group Lookup Reconciliation: <code>__DISTRIBUTIONGROUP__</code></li> <li>For Exchange User Mailbox Database Group Lookup Reconciliation: <code>__MAILBOXDATABASE__</code></li> </ul>
Resource Object Name	Name of the resource object for the target system installation from which you want to reconcile records. Default value: <code>Exchange User</code>

## 3.3 Configuring Reconciliation

When you run the Connector Installer, scheduled tasks for user reconciliation are automatically created in Oracle Identity Manager. Configuring reconciliation involves providing values for the attributes of these scheduled tasks.

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

- [Performing Full Reconciliation and Incremental Reconciliation](#)
- [Limited Reconciliation By Using Filters](#)
- [Reconciliation Scheduled Tasks](#)

### 3.3.1 Performing Full Reconciliation and Incremental Reconciliation

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

full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

You can perform a full and incremental reconciliation against a single domain by providing a value for the `DomainController` parameter of the scheduled task. If the `DomainController` parameter is blank, reconciliation is performed against a forest.

To perform a full reconciliation run, ensure that no values are specified for the following attributes of the scheduled tasks for reconciling user records:

- Filter
- Incremental Recon Attribute
- Latest Token

### 3.3.2 Limited Reconciliation By Using Filters

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a `Filter` attribute (a scheduled task attribute) that allows you to use Exchange resource attributes to filter the target system records.

[Table 3-2](#) lists the filter syntax that you can use and the corresponding description and sample values.



#### Note:

Filters with wildcard characters are not supported.

**Table 3-2 Keywords and Syntax for the Filter Attribute**

Filter Syntax	Description
<b>String Filters</b>	
<code>startsWith('ATTRIBUTE_NAME','PREFIX')</code>	Records whose attribute value starts with the specified prefix are reconciled. <b>Example:</b> <code>startsWith('DisplayName','John')</code> In this example, all records whose display name begins with 'John' are reconciled.
<code>endsWith('ATTRIBUTE_NAME','SUFFIX')</code>	Records whose attribute value ends with the specified suffix are reconciled. <b>Example:</b> <code>endsWith('DisplayName','Doe')</code> In this example, all records whose display name ends with 'Doe' are reconciled.
<code>contains('ATTRIBUTE_NAME','STRING')</code>	Records where the specified string is contained in the attribute's value are reconciled. <b>Example:</b> <code>contains('DisplayName','Smith')</code> In this example, all records whose display name contains 'Smith' are reconciled.
<b>Equality and Inequality Filters</b>	

Table 3-2 (Cont.) Keywords and Syntax for the Filter Attribute

Filter Syntax	Description
<code>equalTo('ATTRIBUTE_NAME','VALUE')</code>	Records whose attribute value is equal to the value specified in the syntax are reconciled. <b>Example:</b> <code>equalTo('DisplayName','Sales Organization')</code> In this example, all records whose display name is Sales Organization are reconciled.
<code>greaterThan('ATTRIBUTE_NAME','VALUE')</code>	Records whose attribute value (string or numeric) is greater than (in lexicographical or numerical order) the value specified in the syntax are reconciled. <b>Example:</b> <code>greaterThan('DisplayName','bob')</code> In this example, all records whose display name is present after the common name 'bob' in the lexicographical order (or alphabetical order) are reconciled.
<code>greaterThanOrEqualTo('ATTRIBUTE_NAME','VALUE')</code>	Records whose attribute value (string or number) is lexicographically or numerically greater than or equal to the value specified in the syntax are reconciled. <b>Example:</b> <code>greaterThanOrEqualTo('DisplayName','S')</code> In this example, all records whose display name is equal to 'S' or greater than 'S' in lexicographical order are reconciled.
<code>lessThan('ATTRIBUTE_NAME','VALUE')</code>	Records whose attribute value (string or numeric) is less than (in lexicographical or numerical order) the value specified in the syntax are reconciled. <b>Example:</b> <code>lessThan('DisplayName','Smith')</code> In this example, all records whose display name is present after the last name 'Smith' in the lexicographical order (or alphabetical order) are reconciled.
<code>lessThanOrEqualTo('ATTRIBUTE_NAME','VALUE')</code>	Records whose attribute value (string or numeric) is lexicographically or numerically less than or equal to the value specified in the syntax are reconciled. <b>Example:</b> <code>lessThanOrEqualTo('DisplayName','A')</code> In this example, all records whose display name is equal to 'A' or less than 'A' in lexicographical order are reconciled.
<b>Complex Filters</b>	
<code>&lt;FILTER1&gt; &amp; &lt;FILTER2&gt;</code>	Records that satisfy conditions in both filter1 and filter2 are reconciled. In this syntax, the logical operator & (ampersand symbol) is used to combine both filters. <b>Example:</b> <code>startsWith('DisplayName','John') &amp; endsWith('DisplayName','Doe')</code> In this example, all records whose display name starts with John and ends with Doe are reconciled.
<code>&lt;FILTER1&gt;   &lt;FILTER2&gt;</code>	Records that satisfy either the condition in filter1 or filter2 are reconciled. In this syntax, the logical operator   (vertical bar) is used to combine both filters. <b>Example:</b> <code>contains('DisplayName','Andy')   contains('DisplayName','Brown')</code> In this example, all records that contain 'Andy' in the display name attribute or records that contain 'Brown' in the display name are reconciled.

Table 3-2 (Cont.) Keywords and Syntax for the Filter Attribute

Filter Syntax	Description
not(<FILTER>)	Records that do not satisfy the given filter condition are reconciled. <b>Example:</b> not(contains('DisplayName', 'Mark')) In this example, all records that does not contain the display name 'Mark' are reconciled.

The following attributes are supported in the filters:

- ArchiveQuota
- ProhibitSendQuota
- ArchiveWarningQuota
- Database
- IssueWarningQuota
- ProhibitSendQuota
- ProhibitSendReceiveQuota
- UseDatabaseQuotaDefaults
- ExternalEmailAddress
- DisplayName
- SimpleDisplayName
- EmailAddressPolicyEnabled
- HiddenFromAddressListsEnabled
- MaxSendSize
- MaxReceiveSize
- Name
- Alias
- PrimarySmtpAddress
- RecipientLimits
- RecipientType
- WhenChanged
- CustomAttribute1, CustomAttribute2, and so on up to CustomAttribute15

### 3.3.3 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:

 **See Also:**

[Scheduled Tasks for Lookup Field Synchronization](#) for information about the Exchange User Distribution Group Lookup Reconciliation and the Exchange User Mailbox Database Group Lookup Reconciliation scheduled tasks

- [Exchange Target Resource User Reconciliation](#)
- [Exchange Target Resource Delete User Reconciliation](#)
- [Exchange Leave Of Absence Update Task](#)

### 3.3.3.1 Exchange Target Resource User Reconciliation

The Exchange Target Resource User Reconciliation scheduled task is used to reconcile data from active mailboxes and mail users. [Table 3-3](#) lists the attributes of this scheduled task.

**Table 3-3 Attributes of the Exchange Target Resource User Reconciliation Scheduled Task**

Attribute	Description
Database	Specifies distinguished name of the database. <b>Note:</b> Distinguished name of the database is available in the Lookup.Exchange.MailboxDatabase lookup definition.
DomainController	This attribute indicates if you want to reconcile from a particular domain. If no domain controller is provided, then a reconciliation run fetches users from all the domains in the forest. By default, this value is blank.
Filter	Expression for filtering records that must be reconciled by the scheduled task. See <a href="#">Table 3-2</a> for the syntax. Default value: None For example, if you set the <code>equalTo('DisplayName', 'john')</code> filter, only the records with <code>DisplayName = john</code> will be reconciled.
Incremental Recon Attribute	Name of the target system attribute that holds last update-related number, non-decreasing value. For example, <code>numeric</code> or <code>strings</code> . The value in this attribute is used during incremental reconciliation to determine the newest or most youngest record reconciled from the target system. Default value: <code>LastModified</code> <b>Note:</b> Do <i>not</i> change the value of this attribute.
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Default value: <code>Exchange IT Resource</code>
Latest Token	Time stamp at which the last reconciliation run started. <b>Note:</b> Do <i>not</i> enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.
Object Type	Type of object you want to reconcile. Default value: <code>User</code>

**Table 3-3 (Cont.) Attributes of the Exchange Target Resource User Reconciliation Scheduled Task**

Attribute	Description
OrganizationalUnit	Specifies the distinguished name of the OU from which you want to reconcile mailboxes.
Resource Object Name	Name of the resource object against which reconciliation runs must be performed. Default value: Exchange User <b>Note:</b> 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.
Scheduled Task Name	Name of the scheduled task. Default value: Exchange Target Resource User Reconciliation <b>Note:</b> For the scheduled task shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the task, then you can enter the unique name for that scheduled task as the value of this attribute.

If there are large number of mailboxes on the target system, it is recommended that you specify values for the following parameters to improve performance of the connector:

- Database
- DomainController
- OrganizationalUnit

 **Note:**

When an Exchange user is disabled from Oracle Identity Manager, the Max Incoming Size and Max Outgoing Size parameters of the mailbox are set to zero in the target system as Exchange does not support enable/disable operations. Similarly, during reconciliation when the Exchange user's MaxSendSize and MaxReceiveSize parameters are set to zero in the target system, the status in Oracle Identity Manager account can be configured to be disabled.

To achieve this behavior during reconciliation:

1. In the Design Console, under Administration, click **Lookup Definition**.
2. Add the following entries in Lookup.Exchange.UM.ReconTransformation:

Code Key: Status

Decode:

```
oracle.iam.connectors.exchange.extension.StatusReconTransformer
```

### 3.3.3.2 Exchange Target Resource Delete User Reconciliation

The Exchange Target Resource Delete User Reconciliation scheduled task is used to reconcile data about deleted mailboxes and mail users. [Table 3-4](#) lists the attributes of this scheduled task.

**Table 3-4 Attributes of the Exchange Target Resource Delete User Reconciliation Scheduled Task**

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Default value: Exchange IT Resource
Object Type	This attribute holds the type of object you want to reconcile. Default value: User
Resource Object Name	Name of the resource object against which reconciliation runs must be performed. Default value: Exchange User  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.

### 3.3.3.3 Exchange Leave Of Absence Update Task

The Exchange Leave Of Absence Update Task sets the HiddenFromAddressListsEnabled attribute on Microsoft Exchange for a user.

To run this task, you must specify the name of the resource object against which reconciliation runs must be performed.

This task runs only if the Leave Start Date and Leave End Date values are provided on the process form. For example, if the date falls between the Leave Start Date and the Leave End Date, then this task runs and sets the HiddenFromAddressListsEnabled attribute on Microsoft Exchange for that user. Otherwise, this task resets the HiddenFromAddressListsEnabled attribute for that user.

## 3.4 Configuring Scheduled Tasks

Configure scheduled jobs to perform reconciliation runs that check for new information on your target system periodically and replicates the data in Oracle Identity Manager.

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

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:

- a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
  - b. On the left pane, in the Search field, enter the name of the scheduled task as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
  - c. In the search results table on the left pane, click the scheduled task in the Job Name column.
4. Modify the details of the scheduled task. To do so:
    - a. On the Job Details tab, you can modify the following parameters:
      - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the task before assigning the Stopped status to the task.
      - **Schedule Type:** Depending on the frequency at which you want the task to run, select the appropriate schedule type.

 **See Also:**

See *Creating Jobs in Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

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

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

 **Note:**

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
  - 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 `Filter` scheduled task attribute.
- On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.
6. After specifying the attributes, click **Apply** to save the changes.

 **Note:**

Depending on the Oracle Identity Manager release that you are using, you can use the Scheduler Status page in the Administrative and User Console or Identity System Administration to either start, stop, or reinitialize the scheduler.

## 3.5 Configuring Provisioning in Oracle Identity Manager Release 11.1.1

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

This section discusses the following topics:

- [Using the Connector for Provisioning](#)
- [Performing Provisioning Operations](#)
- [Switching Between Request-Based Provisioning and Direct Provisioning](#) .

### 3.5.1 Using the Connector for Provisioning

Apply this 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 provision the Microsoft Active Directory resource object to the user in Oracle Identity Manager.

 **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.

### 3.5.2 Performing Provisioning Operations

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

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

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you

want to revert to direct provisioning, then perform the steps described in [Switching Between Request-Based Provisioning and Direct Provisioning](#) .

The following are types of provisioning operations:

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

This section discusses the following topics:

- [Direct Provisioning](#)
- [Request-Based Provisioning](#)

### 3.5.2.1 Direct 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. On the Welcome to Identity Administration page, from the Users region, click **Create User**.
3. On the Create User page, enter values for the OIM User fields, and then click **Save**.
4. If you want to provision a Microsoft Exchange mailbox to an existing OIM User, then:
  - a. On the Welcome to Identity Administration page, search for the OIM User by selecting Users from the list on the left pane.
  - b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
5. On the user details page, click the **Resources** tab.
6. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
7. On the Step 1: Select a Resource page, select **Exchange** from the list, and then click **Continue**.
8. On the Step 2: Verify Resource Selection page, click **Continue**.
9. On the Step 5: Provide Process Data page, enter the details of the mailbox that you want to create on the target system and then click **Continue**.

10. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
11. Close the window displaying the "Provisioning has been initiated" message.
12. On the Resources tab, click **Refresh** to view the newly provisioned resource.

## 3.5.2.2 Request-Based Provisioning

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

### Note:

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

- [End User's Role in Request-Based Provisioning](#)
- [Approver's Role in Request-Based Provisioning](#)

### 3.5.2.2.1 End User's Role in Request-Based Provisioning

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

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.  
The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account..  
  
If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.

10. From the Available Resources list, select **Exchange**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
  - Effective Date
  - Justification

On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

#### 3.5.2.2 Approver's Role in Request-Based Provisioning

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

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

A message confirming that the task was approved is displayed.

### 3.5.3 Switching Between Request-Based Provisioning and Direct Provisioning

If you have configured the connector for request-based provisioning, you can always switch to direct provisioning. Similarly, you can always switch back to request-based provisioning any time.

This section discusses the following topics:

- [Switching From Request-Based Provisioning to Direct Provisioning](#)
- [Switching From Direct Provisioning to Request-Based Provisioning](#)

### 3.5.3.1 Switching From Request-Based Provisioning to Direct Provisioning

 **Note:**

It is assumed that you have performed the procedure described in [Configuring Oracle Identity Manager for Request-Based Provisioning](#).

If you want to switch from request-based provisioning to direct provisioning, then:

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

### 3.5.3.2 Switching From Direct Provisioning to Request-Based Provisioning

If you want to switch from direct provisioning back to request-based provisioning, then:

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

## 3.6 Configuring Provisioning in Oracle Identity Manager Release 11.1.2

You can configure provisioning in Oracle Identity Manager release 11.1.2 by using the Oracle Identity Administrative and User console.

To configure provisioning operations in Oracle Identity Manager release 11.1.2.x:



### Note:

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

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See *Creating a User in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance, and then click **Checkout**.
5. Specify values for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.
7. If you want to provision a Microsoft Exchange mailbox to an existing OIM User, then:
  - a. On the Users page, search for the required user.
  - b. On the user details page, click **Accounts**.
  - c. Click the **Request Accounts** button.
  - d. Search for the Exchange application instance in the catalog search box and select it.
  - e. Click **Add to Cart**.
  - f. Click **Checkout**.
  - g. Specify values for fields in the application form and then click **Ready to Submit**.
  - h. Click **Submit**.

## 3.7 Configuring Action Scripts

Actions are scripts that you can configure to run before or after any provisioning operation. For example, you can run custom PowerShell scripts before or after creating, updating, or deleting a mailbox.

The following are topics pertaining to action scripts:

- [About Configuring Action Scripts.](#)
- [Running a Custom PowerShell Script.](#)

### 3.7.1 About Configuring Action Scripts

This is a summary of the procedure to configure action scripts:

- On the computer hosting the connector server, create the custom PowerShell script in a directory. This script should be self-sufficient, that is, it should be able to create, maintain, and delete sessions with the target Exchange server and complete all actions against it.
- On the computer hosting Oracle Identity Manager, create a batch (.bat) file. This batch file runs on the computer hosting the connector server, which in turn calls custom PowerShell script available on the connector server host computer. Even if Oracle Identity Manager is installed on a UNIX-based computer, create a batch file.

The batch file runs custom PowerShell script using the Powershell.exe program. For more information on Powershell.exe, see <http://technet.microsoft.com/en-us/library/hh847736.aspx>.

- Open Oracle Identity Manager Design Console and add the following entries to the Lookup.Exchange.UM.Configuration lookup definition. The entries specified in italics are generic, which need actual entries based on when the scripts need to be run.

Code Key	Decode
<i>TIMING Action Language</i>	Shell <b>Note:</b> Do not change this value.
<i>TIMING Action File</i>	Enter full path to the batch file on the computer hosting Oracle Identity Manager.
<i>TIMING Action Target</i>	Resource <b>Note:</b> Do not change this value.

Based on when the script needs to run, you can update actual entry for *TIMING Action* in the preceding table as per the following table:

When the Script Needs to Run	Actual value for <i>TIMING Action</i>
Before the create operation	Before Create Action
After the create operation	After Create Action
Before the update operation	Before Update Action
After the update operation	After Update Action
Before the delete operation	Before Delete Action
After the delete operation	After Delete Action

During various operations, there is a difference in terms of what data is available:

- During create operations, all attributes part of the process form are available to the script.

- During update operations, only the attribute that is being updated is available to the script.

If other attributes are also required, then a new adapter calling `ICProvisioningManager# updateAttributeValues(String objectType, String[] labels)` should be created and used. During adapter mapping in process task, add the form field labels of the dependent attributes.

- During delete operations, only the `__UID__` (GUID) attribute is available to the script.

## 3.7.2 Running a Custom PowerShell Script

As an example, this procedure describes the steps to run a custom PowerShell script after a create operation.

1. Log in to the Design Console.
2. Search for and open the **Lookup.Exchange.UM.Configuration** lookup definition.
3. Add the following new values:
  - **Code Key:** After Create Action File
  - **Decode:** Enter the full path of batch file that invokes the script (Oracle Identity Manager must be able to access this file).
  - **Example:** `/home/Scripts/CustomCreateScript.bat`
4. Add the following new values:
  - **Code Key:** After Create Action Language
  - **Decode:** Enter the scripting language of the script you want to run
  - **Example:** Shell (do *not* modify this value)
5. Add the following new values:
  - **Code Key:** After Create Action Target
  - **Decode:** Resource (do *not* modify this value)
6. Save the lookup definition.
7. On the computer running Oracle Identity Manager, create the **/home/Scripts/CustomCreateScript.bat** file with the following content:

```
Powershell.exe -File C:\PSScript\CustomCreateScript.ps1 %Alias% -  
SimpleDisplayName %DisplayName%  
Exit
```

### Note:

The parameters in the process form are available to the batch file and hence to the script. To include additional parameters, you can specify the entries in the Decode column of the provisioning attribute map (Lookup.Exchange.UM.ProvAttrMap).

8. Log in to the computer running the connector server and create the **C:\PSScript\CustomCreateScript.ps1** file with the following content:

 **Note:**

Before running this script using the connector or Oracle Identity Manager, verify the following on the computer running the connector server:

- Connect manually to Exchange server with the values specified in the script using the PowerShell window without any issues.
- Run the `Set-Mailbox` command against any existing mailbox and verify if it runs without any issues.
- From a command prompt, navigate to the directory containing the batch file. Then, run the batch file with appropriate parameters and ensure that the PowerShell script runs on Exchange server without any issues.

If there are any issues, update the batch file or the script appropriately.

Provide appropriate values for username, password, and Exchange server in the following sample script. In the following script:

- Update the value of `$pw` variable with the actual password. The value `Welcome1` is specified as a sample value.
- Update the value of `$cred` variable with the actual username. The value `Connectorse1\oim_exch_service` has been specified as a sample value.
- Update the value of `$Session` variable with the actual Exchange server. The value `http://example.com/PowerShell/` has been specified as a sample value.

```
<#
.SYNOPSIS
    Updates a mailbox property

.DESRIPTION
    This script assumes the first parameter as the identity value, second
    paramater as a the property name to be updated and thrid parameter as the
    new
    value.
.NOTES
    File Name      : CustomCreateScript.ps1

#>

#Accept parameters
$Identity = $args[0]
$ParameterName = $args[1]
$ParameterValue = $args[2]

#Remove "[" and "]"
$Identity = $Identity.Replace("[","")
$Identity = $Identity.Replace("]", "")

#Replace "[" with "-" and remove "]"
$ParameterName = $ParameterName.Replace("[","-")
$ParameterName = $ParameterName.Replace("]", "")
```

```
#Remove "[" and "]"
$ParameterValue = $ParameterValue.Replace("[","")
$ParameterValue = $ParameterValue.Replace("]", "")

#Create password
$pw = convertto-securestring -AsPlainText -Force -String Welcome1

#Create credential
$cred = new-object -typename System.Management.Automation.PSCredential -
argumentlist "Connectorse1\oim_exch_service",$pw

#Create session
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri http://example.com/PowerShell/ -Authentication Kerberos -
Credential $cred

#Import session
Import-PSSession $Session

#Create command variable
$Command = "Set-Mailbox -Identity $Identity $ParameterName $ParameterValue"

#Just to check if proper command is created, dump it to a file.
$Command >> "c:\command.txt"

#Invoke it
Invoke-Expression $Command

#Remove session
Remove-PSSession -Session $Session
```

This script runs after every create operation. It updates the **SimpleDisplayName** property of the newly created mailbox with its **DisplayName** property value.

# 4

## Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.

 **Note:**

From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See *Managing Lookups in Oracle Fusion Middleware Administering Oracle Identity Manager* for information about managing lookups by using the Form Designer in the Oracle Identity Manager System Administration console.

This chapter contains the following sections:

- [Adding New Fields for Target Resource Reconciliation](#)
- [Adding New Multivalued Fields for Target Resource Reconciliation](#)
- [Adding New Fields for Provisioning](#)
- [Adding New Multivalued Fields for Provisioning](#)
- [Configuring Validation of Data During Reconciliation and Provisioning](#)
- [Configuring Transformation of Data During User Reconciliation](#)

### 4.1 Adding New Fields for Target Resource Reconciliation

By default, a few fields are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional fields for reconciliation.

 **Note:**

This section describes an optional procedure. Perform this procedure only if you want to add new single-valued fields for target resource reconciliation. [Table C-1](#) lists the single-valued fields supported by Microsoft Exchange.

To add a new single-valued field for target resource reconciliation:

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\_EXCHANGE** 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.
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 CustomAttribute1 field, enter UD\_EXCHANGE\_CUSTOM1 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 4-1 is a sample screenshot of the new version of process form.

**Figure 4-1 Adding a New Version of Process Form**

Additional Columns	Child Table(s)	Object Permissions	Properties			
Add	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value
	1 UD_EXCHANGE_SERVER	long		Server	ITResourceLo	
Delete	2 UD_EXCHANGE_LOGONNAME	String	150	User Logon Name	TextField	
	3 UD_EXCHANGE_ALIASNAME	String	64	Alias	TextField	
	4 UD_EXCHANGE_CUSTOM1	String	150	CustomAttribute1	TextField	
	5 UD_EXCHANGE_DISPLAYNAME	String	100	Display Name	TextField	
	6 UD_EXCHANGE_SIMPLEDISPLAYNAME	String	64	Simple Display Nar	TextField	
	7 UD_EXCHANGE_RECIPIENTTYPE	String	48	Recipient Type	LookupField	
	8 UD_EXCHANGE_DATABASE	String	300	Database	LookupField	
	9 UD_EXCHANGE_EXTERNALEMAILADDR	String	150	External Email Add	TextField	
	10 UD_EXCHANGE_RECIPIENTLIMITS	String	150	Maximum Recipient	TextField	
	11 UD_EXCHANGE_MAXRECEIVESIZE	String	150	Max Incoming Mes	TextField	
	12 UD_EXCHANGE_MAXSENDSIZE	String	150	Max Outgoing Mes	TextField	
	13 UD_EXCHANGE_DBDEFAULTQUOTAS	boolean	1	Use Storage Defau	CheckBox	
	14 UD_EXCHANGE_MAILBOXQUOTA	String	150	Mailbox Size Defau	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 `CustomAttribute1` 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 Code Key value of the entry that you create in the `Lookup.Exchange.UM.ReconAttrMap` lookup definition.

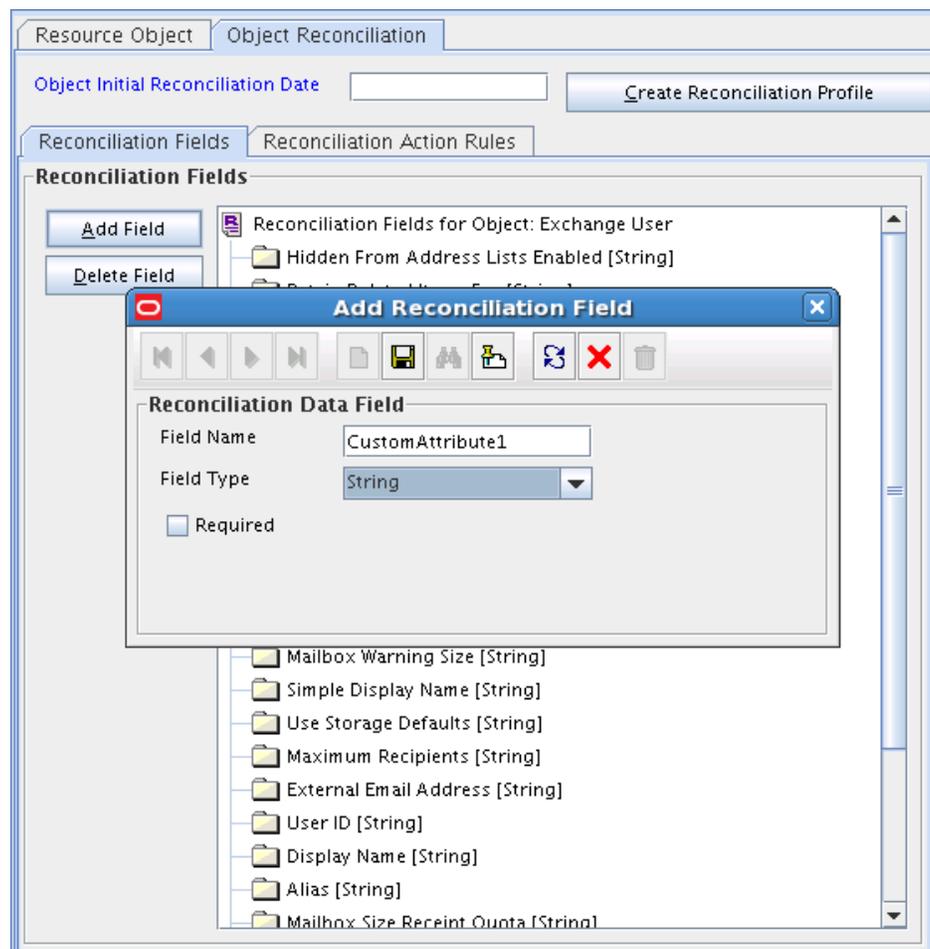
- f. Click **Create Reconciliation Profile**.

This copies changes made to the resource object into the MDS.

- g. Click **Save**.

Figure 4-2 is a sample screenshot of the newly added reconciliation field.

**Figure 4-2 Adding a New Reconciliation Field**



- 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**.

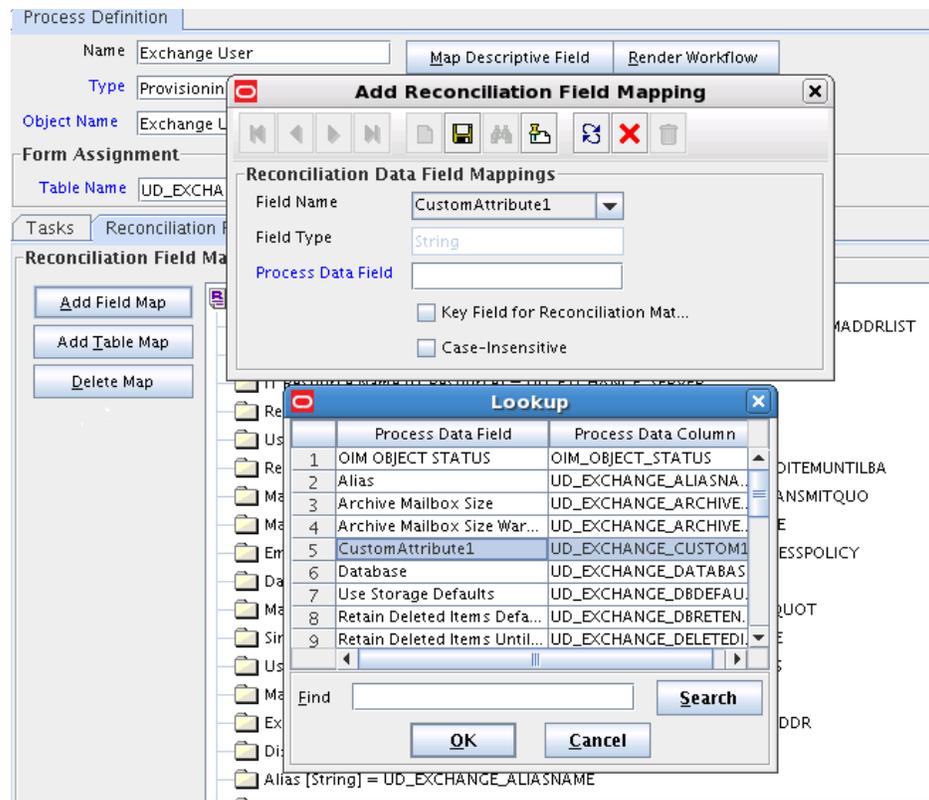
- e. In the Field Name field, select the value for the field that you want to add.  
 For example, select CustomAttribute1.
- f. In the **Field Type** field, select the type of the field that is prepopulated.
- g. Double-click the **Process Data Field** field.

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 CustomAttribute1 = UD\_EXCHANGE\_CUSTOM1.

Figure 4-3 is a sample screenshot of the newly added reconciliation field mapping.

**Figure 4-3 Adding a Reconciliation Field Mapping**



- h. Click the save icon.

Figure 4-4 is a sample screenshot of the reconciliation field mappings.

**Figure 4-4 Reconciliation Field Mappings**

The screenshot displays the 'Process Definition' interface for 'Exchange User'. It includes sections for 'Process Definition' (Name, Type, Object Name, Map Descriptive Field, Render Workflow, Default Process, Auto Pre-populate, Auto Save Form), 'Form Assignment' (Table Name: UD\_EXCHANGE), and 'Reconciliation Field Mappings'. The 'Reconciliation Field Mappings' section shows a list of fields and their corresponding UD\_EXCHANGE attributes, such as 'Hidden From Address Lists Enabled [String] = UD\_EXCHANGE\_HIDDENFROMADDRLIST' and 'CustomAttribute1 [String] = UD\_EXCHANGE\_CUSTOM1'.

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 **Lookup.Exchange.UM.ReconAttrMap** lookup definition.
  - d. Click **Add** and enter the Code Key and Decode values for the field.

The Code Key value must be the form field name. The Decode value must be the attribute name on the target system.

For example, enter `Custom Attribute 1` in the **Code Key** field and then enter `CustomAttribute1` in the **Decode** field.

- e. Click the save icon.

Figure 4-5 is a sample screenshot of the new entry added to the reconciliation lookup definition.

Figure 4-5 Adding an Entry to Reconciliation Lookup

**Lookup Definition**

Code:

Field:

Lookup Type  Field Type

Required:

Group:

**Lookup Code Information**

	Code Key ▼	Decode
<input type="button" value="Add"/>	1 Alias	Alias
<input type="button" value="Delete"/>	2 Archive Mailbox Size	ArchiveQuota
	3 Archive Mailbox Size Warning	ArchiveWarningQuota
	4 Custom Attribute 1	CustomAttribute1
	5 Database[LOOKUP]	Database
	6 Display Name	DisplayName
	7 Distribution Groups~Distribution Group	DistributionGroup
	8 Email Address Policy Enabled	EmailAddressPolicyEnabled
	9 External Email Address	ExternalEmailAddress
	10 Hidden From Address Lists Enabled	HiddenFromAddressListsEnabled
	11 Mailbox Size Receipt Quota	ProhibitSendReceiveQuota
	12 Mailbox Size Transmit Quota	ProhibitSendQuota
	13 Mailbox Warning Size	IssueWarningQuota
	14 Maximum Recipients	RecipientLimits
	15 Max Incoming Message Size	MaxReceiveSize
	16 Max Outgoing Message Size	MaxSendSize
	17 Message Body Format	MessageBodyFormat
	18 Message Format	MessageFormat
	19 Primary SMTP Address	PrimarySmtpAddress
	20 Recipient Type	RecipientType
	21 Retain Deleted Items Defaults	UseDatabaseRetentionDefaults
	22 Retain Deleted Items For	RetainDeletedItemsFor

- On the Resource Objects form, click **Create Reconciliation Profile**.  
This copies changes made to the resource object into the MDS.
- If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

## 4.2 Adding New Multivalued Fields for Target Resource Reconciliation

By default, a few fields are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional fields for reconciliation.

 **Note:**

This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for target resource reconciliation. [Table C-2](#) and [Table C-3](#) list the multivalued fields supported by Microsoft Exchange.

See [Adding New Fields for Target Resource Reconciliation](#) for sample screenshots of some of the following steps.

If you are using Oracle Identity Manager 11.1.2, see [Defining Lookup Definition for Custom Multivalued Attributes in Oracle Identity Manager 11.1.2](#) for related procedure.

- [Adding New Multivalued Fields.](#)
- [Adding Secondary Email Addresses as Multivalued Fields.](#)
- [Defining Lookup Definition for Custom Multivalued Attributes in Oracle Identity Manager 11.1.2.](#)

## 4.2.1 Adding New Multivalued Fields

You can add new multivalued fields by creating new fields on the process form and assigning child tables, adding these new fields to the resource object and creating reconciliation field mapping. Then, create an entry for this new field in the lookup definition for reconciliation.

To add a new multivalued field for target resource reconciliation:

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. Create a new form, for example, UD\_EX\_CH1.
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 AcceptMessagesOnlyFrom field, enter UD\_EX\_CH1\_ACCEPT 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**.
4. Assign UD\_EX\_CH1 as a child table to the UD\_EXCHANGE form as follows:
  - a. Search for and open the **UD\_EXCHANGE** process form.
  - b. 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.

- c. Select the new version created from the **Current Version** dropdown.
  - d. Click the Child Table(s) tab.
  - e. Click **Assign** and select the newly created (active) version of the UD\_EX\_CH1 form.
  - f. Click **Make Version Active**.
  - g. Click the save icon.
5. 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 `MultiValuedForm` in the **Field Name** field and select **MultiValued Attribute** from the Field Type list.
  - f. Right-click **MultiValuedForm [MultiValued]** and select **Define Property Fields**.
  - g. Enter the details of this field.  
For example, enter `AcceptMessagesOnlyFrom` 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 Code Key value of the entry that you create in the Lookup.Exchange.UM.ReconAttrMap lookup definition.
  - h. Click **Create Reconciliation Profile**.  
This copies changes made to the resource object into the MDS.
  - i. Click **Save**.
6. 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**.
  - e. Right-click **MultiValuedForm [MultiValued]** and select **Edit Table Map**.
  - f. Select **Field Name** and **Table Name**.  
For example, select `MultiValuedForm` as Field Name and `UD_EX_CH1` as Table Name.
  - g. Right-click **MultiValuedForm [MultiValued]** and select **Define Property Field Map**.



For example, if you are adding the ProxyAddressForm field, enter UD\_EX\_PROXY\_ADDRESS in the **Name** field and then enter the following details of this field:

**Variant Type:** String

**Length:** 129

**Field Label:** Proxy Address

**Field Type:** textField

**Order:** 1

- c. Click **Save**.
  - d. To activate the newly created form, click **Make Version Active**.
4. Assign the UD\_EX\_PROXY form as a child table to the UD\_EXCHANGE form as follows:
- a. Expand **Development Tools**.
  - b. Double-click **Form Designer**.
  - c. Search for and open the **UD\_EXCHANGE** process form.
  - d. Click **Create New Version**.  
In the Create a new version dialog box, enter a new version in the Label field, and then click the Save icon.
  - e. Select the new version created from the **Current Version** drop-down list.
  - f. On the Child Table(s) tab, click **Assign** and select the newly created (active) version of the UD\_EX\_PROXY form.
  - g. Click **Make Version Active**.
  - h. Click the Save icon.
5. 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.  
Enter `MultiValuedForm` in the **Field Name** field and select **MultiValued Attribute** from the Field Type list.
  - f. Right-click **MultiValuedForm [Multivalued]** and select **Define Property Fields**.
  - g. Enter the details of this field.  
Enter `ProxyAddressForm` 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 Code Key value of the entry that you create in the Lookup.Exchange.UM.ReconAttrMap lookup definition.
  - h. Click **Create Reconciliation Profile**.

This copies changes made to the resource object into the MDS.

- i. Click **Save**.
6. 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**.
  - e. Right-click **MultiValuedForm [MultiValued]** and select **Edit Table Map**.
  - f. Select **Field Name** and **Table Name**.  
Select `MultiValuedForm` as Field Name and `UD_EX_PROXY` as Table Name.
  - g. Right-click **MultiValuedForm [MultiValued]** and select **Define Property Field Map**.
  - h. Select **Field Name** and **Process Data Field**.  
Select `ProxyAddressForm` as Field Name and `UD_EX_PROXY_ADDRESS` as Process Data Field.
  - i. Click the save icon.
7. 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 **Lookup.Exchange.UM.ReconAttrMap** lookup definition.
  - d. Click **Add** and enter the Code Key and Decode values for the field.  
The Code Key value must be the reconciliation field name as entered in the resource object. The Decode value must be the attribute name on the target system.  
Enter `MultiValuedForm~ProxyAddressForm` in the **Code Key** field. This value indicates that `ProxyAddressForm` is a field added to the child form represented by `MultiValuedForm = UD_EX_PROXY`.  
Then, enter `EmailAddresses` in the **Decode** field.
  - e. Click the save icon.
8. On the Resource Objects form, click **Create Reconciliation Profile**.  
This copies changes made to the resource object into the MDS.
9. If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

## 4.2.3 Defining Lookup Definition for Custom Multivalued Attributes in Oracle Identity Manager 11.1.2

For every new custom multivalued attribute added in the connector on Oracle Identity Manager release 11.1.2.x or later, you must define a lookup definition to enable the attribute to be used as entitlements.

 **Note:**

If custom multivalued attributes need to be handled as entitlements, then perform the following procedure. Otherwise, you can use child forms to directly to specify values for these attributes.

As there are no scheduled tasks to populate values into these lookup definitions, they need to be added manually. To do so:

1. Add a custom multivalued attribute, such as `AcceptMessagesOnlyFrom`, as described earlier.
2. Define a new lookup definition, such as `Lookup.Exchange.AcceptMessages`. Then, add some values manually. For example:

Code Key: `23~CN=exch21_exch21L,OU=samarth,DC=extest,DC=com`

Decode Key: `exchblr~CN=exch21_exch21L,OU=samarth,DC=extest,DC=com`

3. In the Form Designer, while adding the new child form, select the field type as **LookupField** instead of `TextField`.
4. On the new form, click the **Properties** tab and click **Add Property**.

Then, add the following values:

Property Name = `Lookup Code`

Property Value = `"Lookup.Exchange.AcceptMessages"`

5. Click **Add Property** and add the following values:

Property Name = `Entitlement`

Property value = `true`

6. Run the Entitlement List and Catalog Synchronization Jobs.

You can now manage the new child form data from entitlements.

7. Create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

## 4.3 Adding New Fields for Provisioning

By default, a few fields are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional fields for provisioning.

### Note:

This section describes an optional procedure. Perform this procedure only if you want to add new single-valued fields for provisioning. [Table C-1](#) lists the single-valued fields supported by Microsoft Exchange.

See [Adding New Fields for Target Resource Reconciliation](#) for sample screenshots of some of the following steps.

To add a new single-valued field for provisioning:

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\_EXCHANGE** 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.

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](#)", 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 CustomAttribute1 field, enter UD\_EXCHANGE\_CUSTOM1 in the **Name** field and then enter the rest of the details of this field.

- b. Click **Save** and then click **Make Version Active**.

4. Create an entry for the field in the lookup definition for provisioning as follows:

- a. Expand **Administration**.
- b. Double-click **Lookup Definition**.
- c. Search for and open the **Lookup.Exchange.UM.ProvAttrMap** lookup definition.
- d. Click **Add** and enter the Code Key and Decode values for the field.

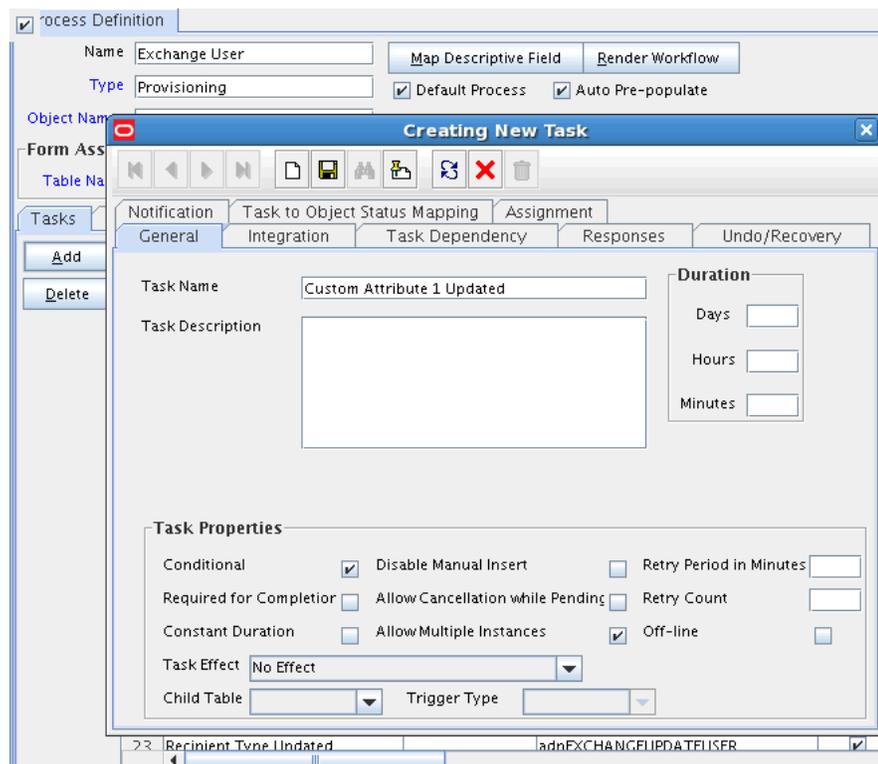
The Code Key value must be the form field name. The Decode value must be the attribute name on the target system.

For example, enter `Custom Attribute 1` in the **Code Key** field and then enter `CustomAttribute1` in the **Decode** field.

- e. Click the save icon.
5. Create a process task to update the new field `Custom Attribute 1` as follows:
    - a. Expand **Process Management**.
    - b. Double-click **Process Definition** and open the **Exchange User** process definition.
    - c. In the process definition, add a new task for updating the field as follows:
      - Click **Add** and enter the task name, for example, `Custom Attribute 1 Updated`, and the task description.
      - In the Task Properties section, select the following fields:  
Conditional  
Allow Multiple Instances
      - Click on the Save icon.

Figure 4-6 is a sample screenshot of the new process task.

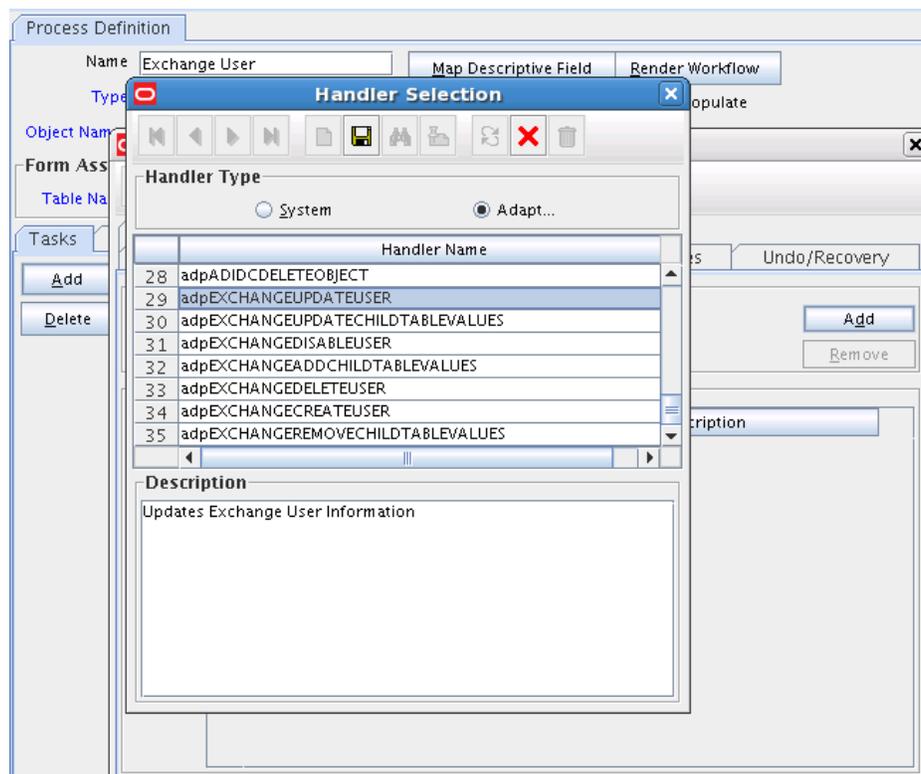
**Figure 4-6 Adding a New Process Task**



- d. On the Integration tab, click **Add**, and then click **Adapter**.
- e. Select the **adpExchangeUpdateUser** adapter, click **Save**, and then click **OK** in the message that is displayed.

Figure 4-7 is a sample screenshot of the selecting the adapter for the new process task.

**Figure 4-7** Selecting an Adapter for New Process Task

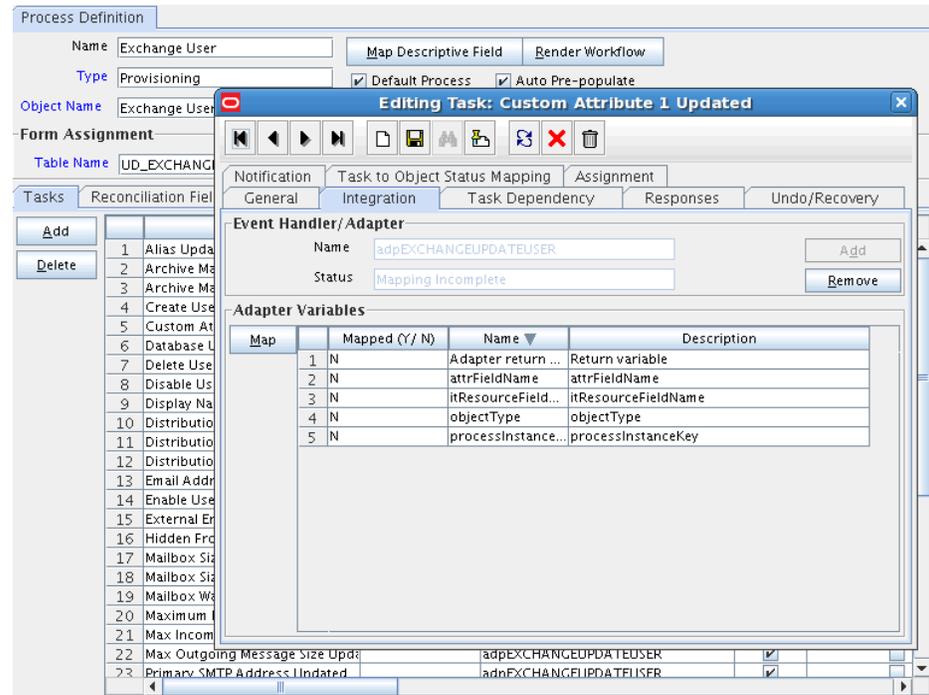


- f. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify values similar to values in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
Adapter return value	Object	Response code	NA	NA
attrFieldName	String	Literal	String	Custom Attribute 1
itResourceFieldName	String	Literal	String	UD_EXCHANGE_SERVER
objectType	String	Literal	String	User
processInstanceKey	Long	Process Data	Process Instance	NA

Figure 4-8 is a sample screenshot of the adapter variables for the new process task.

**Figure 4-8 Mapping Adapter Variables for New Process Task**



- g. On the Responses tab, click **Add** to add the following response codes:

Code Name	Description	Status
ERROR	Error Occurred	R
UNKNOWN	An unknown response was received	R
SUCCESS	Operation Completed	C

- h. Click the Save icon and then close the dialog box.
6. If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

## 4.4 Adding New Multivalued Fields for Provisioning

By default, a few fields are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional fields for provisioning.

### Note:

This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for provisioning. [Table C-2](#) and [Table C-3](#) list the multivalued fields supported by Microsoft Exchange.

See [Adding New Fields for Target Resource Reconciliation](#) and [Adding New Fields for Provisioning](#) for sample screenshots of some of the following steps.

If you are using Oracle Identity Manager 11.1.2, see [Defining Lookup Definition for Custom Multivalued Attributes in Oracle Identity Manager 11.1.2](#) for related procedure.

To add a new multivalued field for provisioning:

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. Create a new form, for example, UD\_EX\_CH1.
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 AcceptMessagesOnlyFrom field, enter UD\_EX\_CH1\_ACCEPT 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**.
4. Assign UD\_EX\_CH1 as a child table to the UD\_EXCHANGE form as follows:
  - a. Search for and open the **UD\_EXCHANGE** process form.
  - b. 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.
  - c. Select the new version created from the **Current Version** dropdown.
  - d. Click the Child Table(s) tab.
  - e. Click **Assign** and select the newly created (active) version of the UD\_EX\_CH1 form.



Variable Name	Data Type	Map To	Qualifier	Literal Value
Adapter return value	Object	Response code	NA	NA
childPrimaryKey	Long	Process Data	Child Primary Key	Exchange User Distribution Group Form
childTableName	String	Literal	String	UD_EX_CH1
objectType	String	Literal	String	User
itResourceFieldName	String	Literal	String	UD_EXCHANGE_SERVER
processInstanceKey	Long	Process Data	Process Instance	NA

- h. On the Responses tab, click **Add** to add the following response codes:

Code Name	Description	Status
CONFIGURATION_ERROR	Connector configuration is wrong	R
CONNECTION_FAILED	Cannot connect to the resource	R
CONNECTOR_EXCEPTION	Child table insertion failed	R
ERROR	Error occurred	R
OBJECT_ALREADY_EXISTS	Object with the same ID already exists	R
UNKNOWN	An unknown response was received	R
UNKNOWN_UID	Object does not exist	R
VALIDATION_FAILED	Custom data validation failed	R
SUCCESS	Operation completed	C

- i. Click the Save icon and then close the dialog box.
7. If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

The following is a sample procedure for adding secondary email addresses as multivalued fields for provisioning:

1. Log in to 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. Create a new form by entering the following values:
 

**Table Name:** UD\_EX\_PROXY

**Description:** Exchange proxy addresses
  - d. Click **Save**.
3. Add the new field on the process form as follows:
  - a. On the Additional Columns tab, **Add**.
  - b. In the newly added row, enter the details of the field.

For example, if you are adding the ProxyAddressForm field, enter UD\_EX\_PROXY in the **Name** field and then enter the following details of this field:

**Variant Type:** String

**Length:** 129

**Field Label:** Proxy Address

**Field Type:** textField

**Order:** 1

- c. Click **Save**.
- d. To activate the newly created form, click **Make Version Active**.
4. Assign the UD\_EX\_PROXY form as a child table to the UD\_EXCHANGE form as follows:

- a. Expand **Development Tools**.
- b. Double-click **Form Designer**.
- c. Search for and open the **UD\_EXCHANGE** process form.
- d. Click **Create New Version**.

In the Create a new version dialog box, enter a new version in the Label field, and then click the Save icon.

- e. Select the new version created from the **Current Version** drop-down list.
- f. On the Child Table(s) tab, click **Assign** and select the newly created (active) version of the UD\_EX\_PROXY form.
- g. Click **Make Version Active**.
- h. Click the Save icon.

5. Create an entry for the field in the lookup definition for provisioning as follows:

- a. Expand **Administration**.
- b. Double-click **Lookup Definition**.
- c. Search for and open the **Lookup.Exchange.UM.ProvAttrMap** lookup definition.
- d. Click **Add** and enter the Code Key and Decode values for the field.

The Code Key format is UD\_EX\_PROXY~Proxy Address. The Decode value is taken from [Table C-3](#) of Exchange Connector Guide.

**Code Key:** UD\_EX\_PROXY~Proxy Address

**Decode:** EmailAddresses

- e. Click the Save icon.
6. Create process tasks to perform insert, update, and delete provisioning operations for the newly created child form, UD\_EX\_PROXY as follows:

 **Note:**

The steps in this section must be performed 3 times for the following insert, update, and delete provisioning operations:

- Add task: Proxy Address Insert
- Add task: Proxy Address Update
- Add task: Proxy Address Delete

- a. Expand **Process Management**.
- b. Double-click **Process Definition**.
- c. Search for and open the **Exchange User** process definition.
- d. On the tasks tab, click **Add** to add the Proxy Address Insert task for an insert provisioning operation.  
A Creating New Task dialog box opens.
- e. Click the **General** tab, and enter the following values:  
**Task Name:** Proxy Address Insert  
**Description:** Add a new Exchange proxy address value
- f. In the Task Properties section, perform the following steps:
  - Select the following options:  
Conditional  
Allow cancellation while Pending  
Allow Multiple Instances
  - From the Child Table list, select **UD\_EX\_PROXY**.
  - From the Trigger Type list, select **Insert**.
- g. Click **Save**.
- h. On the Integration tab, click **Add**.
- i. From the Handler Selection dialog box that is displayed, click **Adapter**.  
A list of adapters which can be assigned to the process task is displayed in the Handler Name region.
- j. Select the **adpEXCHANGEADDCHILDTABLEVALUES** adapter to configure the Proxy Address Insert provisioning operation.
- k. Click **Save**.
- l. In the message that is displayed, click **OK** and close the dialog box.
- m. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify values similar to values in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
Adapter return value	Object	Response Code	NA	NA

Variable Name	Data Type	Map To	Qualifier	Literal Value
childPrimaryKey	Long	Process Data	Child primary Key	Exchange Proxy Address
childTableName	String	Literal	String	UD_EX_PROXY
objectType	String	Literal	String	User
itResourceFieldName	String	Literal	String	UD_EXCHANGE_SERVER
processInstanceKey	Long	Process Data	Process Instance	NA

- n. On the Responses tab, click **Add** to add the following response codes:

 **Note:**

The values specified in the following table are the same for Insert, Update, and Delete process tasks.

Code Name	Description	Status
CONFIGURATION_ERROR	Connector configuration is wrong	R
CONNECTION_FAILED	Cannot connect to the resource	R
CONNECTOR_EXCEPTION	Child table insertion failed	R
ERROR	Error occurred	R
OBJECT_ALREADY_EXISTS	Object with the same ID already exists	R
UNKNOWN	An unknown response was received	R
UNKNOWN_UID	Object does not exist	R
VALIDATION_FAILED	Custom data validation failed	R
SUCCESS	Operation complete	C

- o. Click **Save** and close the Creating New Task dialog box.
- p. In the process definition, to add the Proxy Address Update task for an update provisioning operation, perform Steps 6.d through 6.k with the following differences:
- While performing Step 6.d, in the Creating New Task dialog box, enter the following values:  
**Task Name:** Proxy Address Update  
**Description:** Update an existing Exchange proxy address value
  - While performing Step 6.e, in the Task Properties section, from the Trigger Type list, select **Update** instead of Insert.
  - While performing Step 6.h, in the Handler Name region, select the **adpEXCHANGEUPDATECHILDTABLEVALUES** adapter instead of the **adpEXCHANGEADDCHILDTABLEVALUES** adapter.

- q. In the process definition, to add the Proxy Address Delete task for a delete provisioning operation, perform Steps 6.d through 6.k with the following differences:
  - While performing Step 6.d, in the Creating New Task dialog box, enter the following values:
 

**Task Name:** Proxy Address Delete

**Description:** Delete an Exchange proxy address value
  - While performing Step 6.e, in the Task Properties section, from the Trigger Type list, select **Delete** instead of Insert.
  - While performing Step 6.h, in the Handler Name region, select the **adpEXCHANGEREMOVECHILDTABLEVALUES** adapter instead of the adpEXCHANGEADDCHILDTABLEVALUES adapter.
7. Create a new UI form for the Exchange User resource and attach it to the application instance to make the new Proxy Address field visible in the request form as follows:
  - a. Create a sandbox and activate it as described in [Creating and Activating a Sandbox](#).
  - b. Create a new UI form for the Exchange User resource as described in [Creating a New UI Form](#).
 

While creating a new UI form, select **Exchange User** for the **Resource Type** field, and enter `ExchangeUser2` in the **Form Name** field.
  - c. Open the existing application instance.
  - d. In the **Form** field, select the new UI form that you created.
  - e. Save the application instance.
  - f. Publish the sandbox as described in [Publishing a Sandbox](#).

## 4.5 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class with a fully qualified domain name (FQDN), such as `org.identityconnectors.exchange.extension.ExchangeValidator`.

This validation class must implement the `validate` method. The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
package com.validationexample;

import java.util.HashMap;
```

```

public class MyValidator {
    public boolean validate(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {

        /* You must write code to validate attributes. Parent
        * data values can be fetched by using
hmUserDetails.get(field)
        * For child data values, loop through the
        * ArrayList/Vector fetched by
hmEntitlementDetails.get("Child Table")
        * Depending on the outcome of the validation operation,
        * the code must return true or false.
        */

        /*
        * In this sample code, the value "false" is returned if the field
        * contains the number sign (#). Otherwise, the value "true" is
        * returned.
        */
        boolean valid = true;
        String sFirstName = (String) hmUserDetails.get(sField);
        for (int i = 0; i < sFirstName.length(); i++) {
            if (sFirstName.charAt(i) == '#') {
                valid = false;
                break;
            }
        }
        return valid;
    }
}

```

2. Log in to the Design Console.
3. Search for and open one of the following lookup definitions (or create a new lookup):
  - To configure validation of data for reconciliation:  
Lookup.Exchange.UM.ReconValidation
  - To configure validation of data for provisioning:  
Lookup.Exchange.UM.ProvValidation

 **Note:**

If you cannot find these lookup definitions, create new lookup definitions.

4. In the **Code Key** column, enter the resource object field name that you want to validate. For example, SimpleDisplayName.
5. In the **Decode** column, enter the class name. For example, org.identityconnectors.exchange.extension.ExchangeValidator.
6. Save the changes to the lookup definition.
7. Search for and open the **Lookup.Exchange.UM.Configuration** lookup definition.
8. In the **Code Key** column, enter one of the following entries:
  - To configure validation of data for reconciliation:

Recon Validation Lookup

- To configure validation of data for provisioning:

Provisioning Validation Lookup

9. In the **Decode** column, enter one of the following entries (or enter the name of the lookup you created in step 3):
  - To configure validation of data for reconciliation:
 

Lookup.Exchange.UM.ReconValidation
  - To configure validation of data for provisioning:
 

Lookup.Exchange.UM.ProvValidation
10. Save the changes to the lookup definition.
11. Create a JAR with the class and upload it to the Oracle Identity Manager database using the UpdateJars utility.
12. Run the PurgeCache utility to clear content related to request datasets from the server cache.
13. Perform reconciliation or provisioning to verify validation for the field, for example, SimpleDisplayName.

## 4.6 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

To configure transformation of single-valued user data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class with a fully qualified domain name (FQDN), such as `org.identityconnectors.exchange.extension.ExchangeTransformation`.

This transformation class must implement the transform method. The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

```
package com.transformationexample;

import java.util.HashMap;

public class MyTransformer {
    public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {
        /*
         * You must write code to transform the attributes.
         * Parent data attribute values can be fetched by
         * using hmUserDetails.get("Field Name").
         * To fetch child data values, loop through the
         * ArrayList/Vector fetched by
         hmEntitlementDetails.get("Child      Table")
         * Return the transformed attribute.
         */
    }
}
```

```

        String sFirstName = (String) hmUserDetails.get("First Name");
        String sLastName = (String) hmUserDetails.get("Last Name");
        return sFirstName + "." + sLastName;
    }
}

```

2. Log in to the Design Console.
3. Search for and open the **Lookup.Exchange.UM.ReconTransformation** (or create another custom name) lookup definition.

 **Note:**

If you cannot find the Lookup.Exchange.UM.ReconTransformation lookup definition, create a new lookup definition.

4. In the **Code Key** column, enter the resource object field name you want to transform. For example, `SimpleDisplayName`.
5. In the **Decode** column, enter the class name. For example, `org.identityconnectors.exchange.extension.ExchangeTransformation`.
6. Save the changes to the lookup definition.
7. Search for and open the **Lookup.Exchange.UM.Configuration** lookup definition.
8. In the **Code Key** column, enter `Recon Transformation Lookup`.
9. In the **Decode** column, enter `Lookup.Exchange.UM.ReconTransformation` or enter the name of the lookup you created in step 3.
10. Save the changes to the lookup definition.
11. Create a JAR with the class and upload it to the Oracle Identity Manager database using the UpdateJars utility.
12. Run the PurgeCache utility to clear content related to request datasets from the server cache.
13. Perform reconciliation to verify transformation of the field, for example, `SimpleDisplayName`.

# 5

## Troubleshooting

These tables list solutions to some issues associated with the Exchange connector.

- [Table 5-1](#)
- [Table 5-2](#)
- [Table 5-3](#)

[Table 5-1](#) lists solutions to some commonly encountered issues associated with the Exchange connector:

**Table 5-1 Troubleshooting Common Connector Issues**

Problem Description	Solution
The Exchange connector throws the following error: <code>Could not find domain controller for user &lt;user_name&gt;</code>	The connector tries to get the domain controller where the Active Directory (AD) user was created using the value provided in the User Logon Name field.  This value must be same as the value provided for the User Principal Name field during AD provisioning. If there is any mismatch, the connector throws this error. Ensure the values provided for these two fields are same.
The Exchange connector does not log any information. Logging is enabled for the connector in ConnectorServer.exe.Config file. The line <code>&lt;add name="ExchangeSwitch" value="4" /&gt;</code> has been added and connector server has been restarted.	Ensure the log file location and name as specified in the ConnectorServer.exe.Config file is valid.  Also, ensure the user who is running the connector server has write permission on the log file.  Then, restart the connector server.

**Table 5-1 (Cont.) Troubleshooting Common Connector Issues**

Problem Description	Solution
<p>The Exchange connector throws the following error:</p> <pre>ConnectorServer.exe Error 0 Problem while PowerShell execution System.Management.Aut omation.Remoting.PSRe motingTransportExcept ion: Starting a command on remote server failed with the following error message : The Windows Remote Shell cannot process the request; the selector value 93523BF3-968A-47AA- BCE9-8DD59CFD53E9 specified in the request was not found. For more information, see the about_Remote_Troubles hooting Help topic.</pre>	<p>The problem is caused by the Timeout setting of the "Exchange Connector Server" IT resource. To troubleshoot this problem, increase the value specified for the Timeout parameter in the "Exchange Connector Server" IT resource. See <a href="#">Table 2-3</a> for detailed information about this parameter.</p>

[Table 5-2](#) lists solution to commonly encountered issue associated with the connector when using Exchange 2010:

**Table 5-2 Troubleshooting Connector Issues with Exchange 2010**

Problem Description	Solution
The Exchange connector throws the following error: ConnectorServer.exe Error: 0 : System.Management.Automation.Remoting.PSRemotingTransportException: Connecting to remote server failed with the following error message : Logon failure: unknown username or bad password. For more information, see the about_Remote_Troubleshooting Help topic.	<p>Ensure the username and password specified are correct. The username must be in the format DomainName\UserName.</p> <p>User distinguished name (DN) must <b>not</b> be mentioned as a value for the ExchangeUser IT resource parameter.</p> <p>If this does not solve the issue, verify if you can connect to Exchange Server from the computer hosting the connector server using a remote PowerShell window using the same credentials by following below commands:</p> <pre>\$cred = Get-Credential //provide same credentials as specified in the IT resource</pre> <pre>\$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri http://&lt;ExchangeServerHostName&gt;/PowerShell/ -Authentication Kerberos -Credential \$cred //provide same Exchange Server host name as provided in the IT resource parameter</pre> <pre>Import-PSSession \$session //this should import Exchange cmdlets without any issues. Ideally by this step, you should encounter the issue.</pre> <pre>Remove-PSSession -Session \$Session // remove newly created test session</pre> <p>If the above steps complete without any error, then check Windows event logs for more information.</p> <p><b>Alternate Solution:</b></p> <p>Run the <b>Enable-PSRemoting</b> cmdlet to configure the Exchange Server computer to receive Windows PowerShell remote commands that are sent by using the WS-Management technology. For more information about the Enable-PSRemoting cmdlet, see:</p> <p><a href="http://technet.microsoft.com/en-us/library/hh849694.aspx">http://technet.microsoft.com/en-us/library/hh849694.aspx</a></p>

Table 5-3 lists solution to commonly encountered issue associated with the connector when using Exchange 2007:

**Table 5-3 Troubleshooting Connector Issues with Exchange 2007**

Problem Description	Solution
The Exchange connector throws the following error while adding a user to a distribution group: ConnectorServer.exe Error: 0 : Org.IdentityConnectors.Framework.Common.Exceptions.ConnectorException: Problem while PowerShell execution Org.IdentityConnectors.Framework.Common.Exceptions.ConnectorException: Active Directory operation failed on MachineName.connectordevroot1.com. This error is not retrievable. Additional information: Insufficient access rights to perform the operation. Active directory response: 00002098: SecErr: DSID-03150BB9, problem 4003 (INSUFF_ACCESS_RIGHTS)	<p>For Exchange 2007, the service account must be a member of the Exchange Recipient Administrator role and the Account Operator role in every domain where the distribution group exists.</p> <p>Add the user to the Account Operator role of the domain where the distribution group exists and restart the connector server.</p>

# 6

## Frequently Asked Questions

Use these Frequently Asked Questions (FAQs) as guidelines and to troubleshoot connector issues.

The following topics are discussed in this section:

- [FAQs Related to Exchange 2007 or Later](#)
- [FAQs Related to Exchange 2010 or Later](#)
- [FAQs Related to Exchange 2007](#)

### 6.1 FAQs Related to Exchange 2007 or Later

These are FAQs on connector issues related to Exchange 2007 or later.

1. What is the recommended system configuration for the computer hosting and running the connector server?

**Answer:** The computer hosting and running the connector server must have Intel Dual-Core Processor, 2 GHz with 4 GB RAM or a computer with similar configuration. If you have a computer dedicated to the connector server, then 2 GB RAM is sufficient.

2. Where should I install the connector server for the Exchange connector?

**Answer:** Install the connector server on a computer that belongs to the same domain as that of the target Exchange server.

3. Can 9.x Exchange connector co-exist with Exchange connector 11.x?

**Answer:** Yes, 9.x Exchange connector can co-exist with Exchange connector 11.x. This can be achieved by cloning the Exchange 11.x connector XML and using it for installing the connector with the new name.

4. Is it mandatory to install Active Directory connector 11.x before installing Exchange connector 11.x?

**Answer:** Yes.

5. If I use Oracle Internet Directory (OID) 11.x connector to manage Active Directory, can I use 11.x Exchange connector to manage mailboxes?

**Answer:** No, this is not supported.

6. Why cannot I see the log files corresponding to the connector operations in the computer hosting Oracle Identity Manager?

**Answer:** The Exchange connector uses the built-in logging mechanism of the .NET framework. Therefore, all connector logs are generated on the computer hosting the connector server. See [Enabling Logging](#) for more information.

7. All connector operations are performed by using the ICFINTG layer. What is the logger name used for enabling logging for ICFINTG?

**Answer:** The logger name used to enable logging for ICFINTG is ORACLE.IAM.CONNECTORS.ICFCOMMON. Note that the logger name is case-sensitive.

8. I performed target resource reconciliation using filters in the scheduled job. Connector server logs confirm that the connector was able to get the mailbox based on search criteria. However, reconciliation events are not getting generated. There is no error in the connector server logs and in the OIM server logs. What is wrong here?

**Answer:** When you perform filter-based search, the connector internally converts them to Exchange PowerShell cmdlets. The Exchange server returns data. Note that this search is not case-sensitive. The connector returns the same data to Oracle Identity Manager via ICF INTG. Even before data reaches ICF INTG, ICF (framework) applies a case-sensitive search against the result sent by connector. It is possible that this user record might be dropped.

For example, suppose that in the scheduled task, there is a filter such as `equalTo('DisplayName', 'JOHN')` and on the target Exchange server, there is a mailbox whose display name is John. The connector runs PowerShell cmdlet, `Get-Mailbox -Filter {DisplayName -eq 'JOHN'}`, and gets the result. However, ICF applies a case-sensitive search for which the condition fails and reconciliation events are created.

9. Is Remote Manager required for the Exchange 11.x connector?

**Answer:** No.

10. After extracting the contents of the connector bundle into the `CONNECTOR_SERVER_HOME` directory, I observed some DLLs. Does it matter whether the computer hosting the connector server is 32-bit or 64-bit?

**Answer:** No, you can use the same DLLs on both 32-bit and 64-bit computers.

11. Can a single connector server be used to deploy the Active Directory User Management connector bundle and the Exchange connector bundle?

**Answer:** Yes, a single connector server can host both the Active Directory User Management and the Exchange connector bundles.

While deploying the Exchange connector, ensure not to replace the existing `ActiveDirectory.Connector.dll` file on the connector server.

12. I see `Container`, `DirectoryAdminName`, `DirectoryAdminPassword`, `DomainName` entries in `Lookup.Exchange.Configuration` with `Decode` values set to `UseDefault`. What is the significance of these entries and can I provide any value to it?

**Answer:** These properties are internally used by the connector. Do *not* modify or remove them from this lookup definition.

13. Explain what cmdlets the connector runs during create, update, delete, disable and enable operations in Oracle Identity Manager (OIM).

**Answer:**

- During a create operation, the connector enables a mailbox for an already existing AD user. It first runs `Enable-Mailbox/Enable-MailUser` cmdlet with required attributes and then runs the `Set-Mailbox/Set-MailUser` cmdlet to update rest of the attributes.
- During an update operation, it updates the `Mailbox/MailUser` attribute using the `Set-Mailbox` cmdlet.

- During a delete operation, connector just removes the mailbox and does NOT delete the AD user. It runs the Disable-Mailbox/Disable-MailUser cmdlet.
  - During a disable operation, connector just sets MaxReceiveSize and MaxSendSize to 0 KB.
  - During an enable operation, connector gets the correct value of MaxReceiveSize and MaxSendSize on process form and then sets them in the target system.
14. The Distribution Group Lookup Reconciliation and Target Resource User Reconciliation scheduled tasks obtain distribution groups of type MailUniversalDistributionGroup. Our target system has security groups that are mail-enabled. Why are they not reconciled by the Exchange connector? We would like to manage them as well.

**Answer:** The Exchange connector manages distribution groups that can only be used with e-mail applications (such as Exchange) to send e-mails to collections of users. To manage security groups (mail-enabled or otherwise), use the Active Directory connector.

15. I have configured my action script to run after Create, Update, and Delete operations as per steps mentioned in [Configuring Action Scripts](#). However, the script does not run. I want to debug and check what is happening. Where do I add my debug statements?

**Answer:** The sample script in the above section has the following line:

```
#Just to check if proper command is created, dump it to a file.  
$Command >> "c:\command.txt"
```

This line shows how to dump the command being created to a temporary file. You can use this file to add all your debug statements. You can echo all the things you need to this file.

If the commands that were dumped to this file were correct and yet, you are not getting the desired result when running the script from Oracle Identity Manager, then open a PowerShell window and run the same commands manually to verify if there is any issue.

Note that Oracle Identity Manager does not return any exceptions or runtime errors that occur when the script is running.

## 6.2 FAQs Related to Exchange 2010 or Later

These are FAQs on connector issues specific to Exchange 2010 or later.

1. In what format should the IT resource parameter ExchangeUser be specified?

**Answer:** It should be in the *DOMAIN\_NAME\USER\_NAME* format.

2. How do I ensure that the username and password provided in the IT resource are correct?

**Answer:** Follow the steps mentioned in [Table 5-2](#) for error "unknown user name or bad password."

3. What is the minimum permission/role that the user provided in IT resource should have?

**Answer:** The user should be part of the Recipient Management group.

4. What are Exchange 2010 specific requirements that must be met by the computer hosting connector server?

**Answer:** The host computer should meet all the prerequisites of Remote PowerShell. For more information, see the topic on Connect Remote Exchange Management Shell to an Exchange Server at:

<http://technet.microsoft.com/en-in/library/dd297932%28v=exchg.141%29.aspx>

5. Does the computer hosting the connector server need to have Exchange Management Tools installed?

**Answer:** No.

6. How to avoid overwriting Active Directory's account email address with an auto generated email address?

**Answer:** When you provision the Exchange account with the **Email Address Policy Enabled** option deselected, and without providing any value for the primary SMTP address, the provisioning operation overwrites the Active Directory's account email address with an auto generated email address in the *userlogonname@domain.com* format. To avoid this, perform the following steps:

- a. Change the default value of the **Email Address Policy Enabled** check box as follows:
  - i. Open the Design Console.
  - ii. Open the **Exchange User Form** and navigate to the **Additional Columns** tab.
  - iii. Change the default value of the **Email Address Policy Enabled** check box from 1 to 0 as 1 denotes **True** and 0 denotes **False**.
  - iv. Click **Save**.
- b. Provision the Exchange account by providing a value for the **Primary SMTP Address** which is same as the Active Directory's account email address present in the Exchange user form.

## 6.3 FAQs Related to Exchange 2007

These are FAQs on connector issues specific to Exchange 2007.

1. Does the connector support RTM version of Exchange 2007?

**Answer:** No.

2. What values do I have to provide for ExchangeUser, ExchangeUserPassword, and ExchangeServerHost in the Exchange IT resource?

**Answer:** No values are required for these attributes. You can leave them blank. As the connector communicates to Exchange 2007 via local runspace, the connector does not use username or password provided in IT resource to connect to Exchange server. It uses the username and password of the user who starts the connector server.

3. Does the computer hosting the connector server need to have Exchange Management Tools installed?

**Answer:** Yes.

4. What is the minimum permission/role of the user who starts the connector server?

**Answer:**

- User should be part of the Exchange Recipient Administrators group.
  - User should be part of the Account Operators group in the domain where the distribution group exists.
5. What are Exchange 2007 specific requirements that need to be met by the computer hosting the connector server?

**Answer:** The host computer needs to have Exchange Management Tools installed.

# A

## Files and Directories On the Connector Installation Media

These are the list of files and directories in the connector installation media and their descriptions.

**Table A-1 Files and Directories On the Connector Installation Media**

File in the Installation Media Directory	Description
bundle/Exchange.Connector-2.0.0.1.zip	This ZIP file contains the connector bundle.
configuration/Exchange-CI.xml	This XML file contains configuration information that is used during the connector installation process.
Files in the DataSet directory <ul style="list-style-type: none"> <li>• ModifyResourceExchange.xml</li> <li>• ProvisionResourceExchange.xml</li> </ul>	These XML files specify the information to be submitted by the requester during a request-based provisioning operation. <b>Note:</b> These files are applicable to Oracle Identity Manager releases prior to 11.1.2.
Files in the javadoc directory	This directory contains information about the Java APIs used by Exchange Leave Of Absence Update Task.
lib/Exchange-oim-integration.jar	This JAR file contains the class files that are specific to integration of the connector with the target systems. During connector deployment, this file is copied to the Oracle Identity Manager database.
owglue/ExchangeConnector-idmglue-1.0.8.zip	This ZIP file contains connector integration code for Oracle Waveset.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to Oracle Identity Manager database. <b>Note:</b> A <b>resource bundle</b> is a file containing localized versions of the text strings that include GUI element labels and messages.
upgrade/PostUpgradeScript.sql	This script file is run after upgrading a connector. <b>Note:</b> Run this script only if you are upgrading the connector from release 9.x to 11.x.

**Table A-1 (Cont.) Files and Directories On the Connector Installation Media**

File in the Installation Media Directory	Description
xml/Exchange-ConnectorConfig.xml	<p>This XML file contains definitions for the connector components. These components include the following:</p> <ul style="list-style-type: none"><li>• IT resource type</li><li>• Connector server IT Resource type</li><li>• IT resource instance</li><li>• Connector server IT resource instance</li><li>• Process forms</li><li>• Resource object</li><li>• Process definition</li><li>• Process tasks</li><li>• Adapters</li><li>• Reconciliation rules</li><li>• Prepopulate adapters</li><li>• Lookup definitions</li><li>• Scheduled tasks</li></ul>
xml/Exchange-Datasets.xml	<p>This XML file contains the dataset related definitions for the create and modify user provisioning operations. This file is used if you want to enable request-based provisioning by using the deployment manager.</p> <p><b>Note:</b> This file is applicable to Oracle Identity Manager releases prior to 11.1.2.</p>

# B

## Special Characters Supported for Alias Name

These are the special characters supported by Oracle Identity Manager and Microsoft Exchange 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.

**Table B-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	%
single quotation mark	'
asterisk	*
plus sign	+
dash	-
slash	/
equal to sign	=
question mark	?
caret	^
underscore	_
left brace	{
vertical bar	
right brace	}
tilde	~

# C

## Microsoft Exchange Fields Supported for Reconciliation and Provisioning

These are the single-valued fields supported by Microsoft Exchange that you can add for target resource reconciliation and provisioning.

**Table C-1 Single-valued Fields Supported by Microsoft Exchange**

Field
AntispamBypassEnabled
CustomAttribute1
CustomAttribute2
CustomAttribute3
CustomAttribute4
CustomAttribute5
CustomAttribute6
CustomAttribute7
CustomAttribute8
CustomAttribute9
CustomAttribute10
CustomAttribute11
CustomAttribute12
CustomAttribute13
CustomAttribute14
CustomAttribute15
Name
UserPrincipalName
WindowsEmailAddress

[Table C-2](#) lists the multi-valued fields supported by Microsoft Exchange 2010 that you can add for target resource reconciliation and provisioning.

**Table C-2 Multi-valued Fields Supported by Exchange 2010**

Field
AcceptMessagesOnlyFrom
<b>Note:</b> Provide distinguished name of the recipients.
AcceptMessagesOnlyFromDLMembers
<b>Note:</b> Provide distinguished name of the recipients.

**Table C-2 (Cont.) Multi-valued Fields Supported by Exchange 2010**

Field
AcceptMessagesOnlyFromSendersOrMembers
ArchiveName
AuditAdmin
AuditDelegate
AuditOwner
BypassModerationFromSendersOrMembers
EmailAddresses
ExtensionCustomAttribute1
ExtensionCustomAttribute2
ExtensionCustomAttribute3
ExtensionCustomAttribute4
ExtensionCustomAttribute5
GrantSendOnBehalfTo
Languages
MailTipTranslations
ModeratedBy
RejectMessagesFrom
<b>Note:</b> Provide distinguished name of the recipients.
RejectMessagesFromDLMembers
<b>Note:</b> Provide distinguished name of the recipients.
RejectMessagesFromSendersOrMembers
ResourceCustom
UMDtmfMap
UserCertificate
UserSMimeCertificate

[Table C-3](#) lists the multi-valued fields supported by Microsoft Exchange 2007 that you can add for target resource reconciliation and provisioning.

**Table C-3 Multi-valued Fields Supported by Exchange 2007**

Field
AcceptMessagesOnlyFrom
<b>Note:</b> Provide distinguished name of the recipients.
AcceptMessagesOnlyFromDLMembers
<b>Note:</b> Provide distinguished name of the recipients.
EmailAddresses
Extensions
ForwardingAddress

**Table C-3 (Cont.) Multi-valued Fields Supported by Exchange 2007**

<b>Field</b>
GrantSendOnBehalfTo
Languages
RejectMessagesFrom
<b>Note:</b> Provide distinguished name of the recipients.
RejectMessagesFromDLMembers
<b>Note:</b> Provide distinguished name of the recipients.
ResourceCustom
UMDtmfMap