Oracle® Identity Governance

Configuring the Microsoft Exchange Application

12.2.1.3.0
F22871-04
September 2020

ORACLE

Oracle Identity Governance Configuring the Microsoft Exchange Application, 12.2.1.3.0

F22871-04

Primary Author: Alankrita.Prakash

Contributors: Gowri.G.R, Vivek Garg

Contents

2 Creating an Application By Using the Microsoft Exchange Connector

3 Configuring the Microsoft Exchange Connector

4 Performing the Postconfiguration Tasks for the Microsoft Exchange Connector

List of Figures

List of Tables

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 Governance 12.2.1.3.0, visit the following Oracle Help Center page:

`https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.3/index.html`

For information about installing and using Oracle Identity Manager 11.1.2.3, visit the following Oracle Help Center page:

`http://docs.oracle.com/cd/E52734_01/index.html`

For information about Oracle Identity Governance Connectors 12.2.1.3.0 documentation, visit the following Oracle Help Center page:

`https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html`

For information about Oracle Identity Manager Connectors 11.1.1 documentation, visit the following Oracle Help Center page:

`http://docs.oracle.com/cd/E22999_01/index.htm`

Conventions

The following text conventions are used in this document:

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

What's New In This Guide?

These are the updates made to the software and documentation for release 12.2.1.3.0 of Configuring the Microsoft Exchange Application.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the Microsoft Exchange target. This helps in quicker onboarding of the applications for this target system into Oracle Identity Governance by using an intuitive UI.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following is a documentation-specific update for revision "04" of the guide:

Information about Oracle Identity Manager versions prior to 11g Release 2 PS3 (11.1.2.3.0) has been removed from the guide.

The following is a documentation-specific update for revision "03" of the guide:

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

The following is a documentation-specific update for revision "02" of the guide:

A new issue about failure in onboarding the Microsoft Exchange connector has been documented in Known Issues and Workarounds for the Microsoft Exchange Connector.

1

About the Microsoft Exchange Connector

The Microsoft Exchange connector integrates Oracle Identity Governance with the Microsoft Exchange target system.

The following topics provide a high-level overview of the Microsoft Exchange connector:

1.1 Introduction to the Connector

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premises or on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications.

The Microsoft Exchange connector lets you create and onboard Exchange applications in Oracle Identity Governance.

> **Note:**
>
> In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**. The connector that is deployed using the **Manage Connector** option in Oracle Identity System Administration is referred to as a **CI-based connector** (Connector Installer-based connector).

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Oracle Identity Self Service. This capability lets business users to onboard applications with minimum details and effort. The connector installation package includes a collection of predefined templates (XML files) that contain all the information required for provisioning and reconciling data from a given application or target system. These templates also include basic connectivity and configuration details specific to your target system. The connector

uses information from these predefined templates allowing you to onboard your applications quickly and easily using only a single and simplified UI.

Application onboarding is the process of registering or associating an application with Oracle Identity Governance and making that application available for provisioning and reconciliation of user information.

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.

> **Note:**
>
> At some places in this guide, Microsoft Exchange is sometimes 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.

1.2 Certified Components

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

Table 1-1 Certified Components

Item	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	You can use any one of the following releases: • Oracle Identity Governance release 12c PS4 (12.2.1.4.0) • Oracle Identity Governance release 12c (12.2.1.3.0)	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance release 12c PS4 (12.2.1.4.0) • Oracle Identity Governance release 12c (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)

Table 1-1 (Cont.) Certified Components

Item	Requirement for AOB Application	Requirement for CI-Based Connector
Target systems	Microsoft Exchange 2016, 2019	The target system can be any one or a combination of the following: • Microsoft Exchange 2013, 2016, 2019 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. • Microsoft Exchange 2010 RTM, SP1, SP2, SP3 (64-bit) • Microsoft Exchange 2007 SP1, SP2, SP3 (64-bit)
Connector Server	12.2.1.3.0	11.1.2.1.0 or 12.2.1.30
Connector Server JDK	JDK 1.8 or later	You can use one of the following versions: • For Connector Server 11.1.2.1.0, use JDK 1.6 or later • For Connector Server 12.2.1.3.0, use JDK 1.8 or later

Table 1-1 (Cont.) Certified Components

Item	Requirement for AOB Application	Requirement for CI-Based Connector
Other systems	You must ensure the following software are installed in your operating environment: • Microsoft Active Directory • Microsoft Active Directory User Management connector 12.2.1.3.0 or later You must create the Microsoft Active Directory User Management application before you can create and use the Microsoft Exchange application. See Creating an Application By Using the Microsoft Active Directory User Management Connector in *Oracle® Identity Governance Configuring the Microsoft Active Directory User Management Application* for instructions to create and onboard the Microsoft Active Directory User Management Application. • .NET Connector Server The Microsoft Exchange connector operates in the context of the .NET Framework. You can download the .NET connector server from the Oracle Identity Manager Connector Downloads Oracle Identity Manager Connector Downloads.	You must ensure the following software are installed in your operating environment: • Microsoft Active Directory • Microsoft Active Directory User Management connector 11.1.1.5.0 or later You must deploy the Microsoft Active Directory User Management connector before you can deploy and use the Microsoft Exchange connector. See Deploying the Connector in *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for instructions to deploy the Microsoft Active Directory connector. • .NET Connector Server The Microsoft Exchange connector operates in the context of the .NET Framework. You can download the .NET connector server from the Oracle Identity Manager Connector Downloads Oracle Identity Manager Connector Downloads.

1.3 Usage Recommendation

These are the recommendations for the Microsoft Exchange connector versions that you can deploy and use depending on the Oracle Identity Governance or Oracle Identity Manager version that you are using.

- If you are using Oracle Identity Governance release 12c (12.2.1.3.0) or later, then use the 12.2.1.3.0 version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service for a fresh installation. Otherwise, continue to manage the connector using the CI mode and Oracle Identity Manager Design Console.

- If you are using any of the Oracle Identity Manager releases listed in the "Requirement for CI-Based Connector" column of Table 1-1, then use the 11.1.1.*x* version of the Microsoft Exchange connector. If you want to use the 12.2.1.3.0 version of this connector, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12c (12.2.1.3.0) or later.

> **Note:**
>
> If you are using the 12.2.1.3.0 version of the Microsoft Exchange connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for Microsoft Exchange*, Release 11.1.1 for complete details on connector deployment, usage, and customization.

1.4 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

1.5 Supported Connector Operations

These are the list of operations that the connector supports for your target system.

Table 1-2 Supported Connector Operations

Operation	Supported?
User Management	Yes
Create User	Yes
Delete User	Yes
Update User	Yes
Enable User	Yes
Disable User	Yes
Entitlement Grant Management	Yes
Insert Distribution Group	Yes
Delete Distribution Group	Yes
Update Distribution Group	Yes

1.6 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.

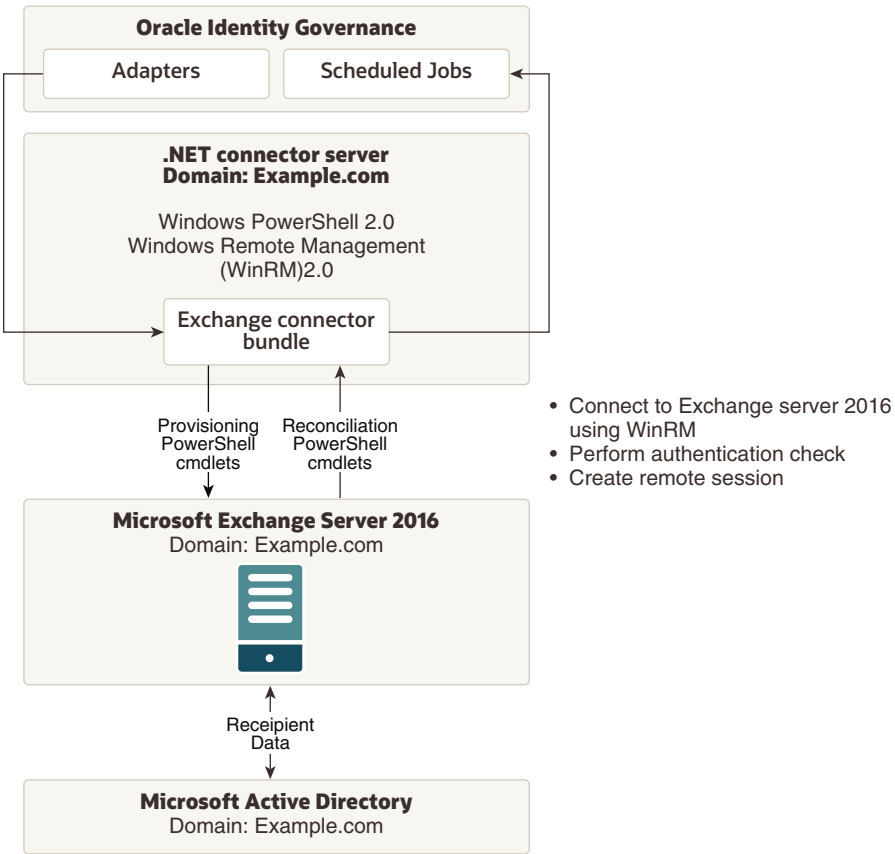
1.6.1 Architecture of the Microsoft Exchange Connector

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 the Exchange target system.

> **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 2016. 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 1-1 Architecture of the Connector Supporting Exchange Server 2016



Oracle Identity Governance (OIG) communicates with the Exchange Server 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 the Exchange Server, OIG 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 2016. 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

1.6.2 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.

1.7 Supported Connector Features Matrix

Provides the list of features supported by the AOB application and CI-based connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Full reconciliation	Yes	Yes
Incremental reconciliation	Yes	Yes
Limited reconciliation	Yes	Yes
Reconcile deleted user records	Yes	Yes
Scheduled jobs for reconciliation of distribution groups and mailbox database	Yes	Yes
Perform reconciliation and provisioning operations across multiple domains	Yes	Yes
Run custom PowerShell scripts	Yes	Yes
Connection pooling	Not applicable	Yes
Use connector server	Yes	Yes

Table 1-3 (Cont.) Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Clone applications or create new application instances	Yes	Yes
Transformation and validation of account data	Yes	Yes

1.8 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
- Support for Connector Server
- Support for Cloning Applications and Creating Instance Applications
- Transformation and Validation of Account Data

1.8.1 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.

1.8.2 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.

For detailed information about limited reconciliation, see Performing Limited Reconciliation.

1.8.3 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.

For information about the Delete User reconciliation job, see Reconciliation Jobs.

1.8.4 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 as entitlements in the lookup definitions on Oracle Identity Governance.

For detailed information about the jobs that are available for reconciling these entitlements, see Reconciliation Jobs.

1.8.5 Support for Multiple Domains

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

For more information about performing reconciliation and provisioning operations on mailboxes across multiple domains, see Reconciliation and Provisioning of Mailboxes Across Multiple Domains.

1.8.6 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.

For more information about configuring these scripts, see Configuring Action Scripts.

1.8.7 Support for Connector Server

Connector Server is a component provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Governance connector.

The Microsoft Exchange connector is written using Microsoft .NET. A .NET environment is required for the execution of this connector code. Therefore, it is mandatory for this connector to be deployed on the .NET Connector Server. The Microsoft Exchange connector operates in the context of a .NET Connector Framework, which in turn requires an application to execute. Therefore, by default, Oracle provides the .NET Connector Server to run the Microsoft Exchange connector.

For information about installing, configuring, and running the Connector Server, and installing the connector in a Connector Server, see Using an Identity Connector Server

in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

1.8.8 Support for Cloning Applications and Creating Instance Applications

You can configure this connector for multiple installations of the target system by cloning applications or by creating instance applications.

When you clone an application, all the configurations of the base application are copied into the cloned application. When you create an instance application, it shares all configurations as the base application.

For more information about these configurations, see Cloning Applications and Creating Instance Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.9 Transformation and Validation of Account Data

You can configure transformation and validation of account data that is brought into or sent from Oracle Identity Governance during reconciliation and provisioning operations by writing Groovy scripts while creating your application.

For more information, see Validation and Transformation of Provisioning and Reconciliation Attributes in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

2

Creating an Application By Using the Microsoft Exchange Connector

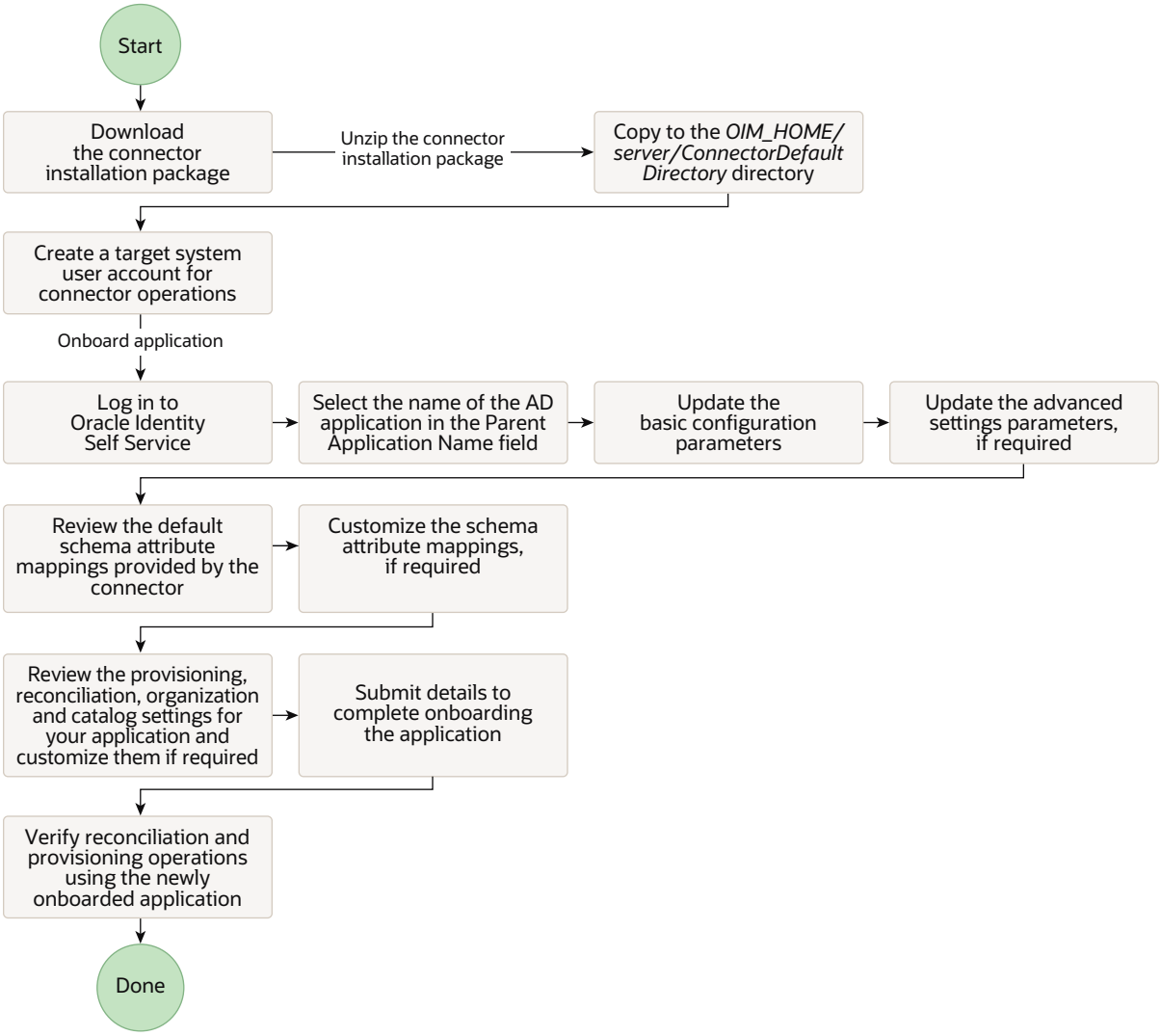
Learn about onboarding applications using the connector and the prerequisites for doing so.

2.1 Process Flow for Creating an Application By Using the Connector

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Identity Self Service.

Figure 2-1 is a flowchart depicting high-level steps for creating an application in Oracle Identity Governance by using the connector installation package.

Figure 2-1 Overall Flow of the Process for Creating an Application By Using the Connector



2.2 Prerequisites for Creating an Application By Using the Connector

Learn about the tasks that you must complete before you create the application.

- Downloading the Connector Installation Package
- Installing and Configuring the Connector Server
- Deploying the Connector Bundle on the Connector Server
- Creating a Target System User Account for Connector Operations
- Creating the Parent Application

2.2.1 Downloading the Connector Installation Package

You can obtain the installation package for your connector on the Oracle Technology Network (OTN) website.

To download the connector installation package:

1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html.
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.

   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.* For example, for this connector, the director name is activedirectory-12.2.1.3.0.
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIM_HOME*/server/ConnectorDefaultDirectory directory.

2.2.2 Installing and Configuring the 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.

This section contains the following topics:

- Prerequisites for the Connector Server
- Installing the Connector Server
- Enabling Logging
- Configuring Log File Rotation

2.2.2.1 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 4.0 or later on the same computer where you are installing the connector server.

  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.

2.2.2.2 Installing the Connector Server

You must install the .NET Connector Server by downloading the Connector Server package from the Oracle Technology Network site and running the `ServiceInstall-version.msi` file.

To install, configure, and run the Connector Server, see Using the Microsoft .NET Framework Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

2.2.2.3 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 Governance. 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.

2.2.2.4 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.VisualBasi
c,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`

2.2.3 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
- Creating the IT Resource for the Connector Server

2.2.3.1 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 the contents of the `bundle/Exchange.Connector-12.3.0.0.zip` file to the *CONNECTOR_SERVER_HOME* directory.
3. Start the Connector Server.

2.2.3.2 Creating the IT Resource for the Connector Server

Create the IT resource for the connector server from Identity System Administration.

To create the IT resource:

1. Log in to Identity System Administration, and then in the left pane, under Provisioning Configuration, click **IT Resource.**
2. On the Manage IT Resources page, click the **Create** icon.
3. On the Create IT Resource page:
   a. In the **IT Resource Name** field, enter a name for the IT resource. This is the name that you will provide in the Basic Configuration section while creating the Target application.
   b. From the **IT Resource Type** dropdown list, select **Connector Server**.

c. In the Parameter Values section, specify values for the IT resource parameters, click **Test Connectivity** to test the connection, and then click **Finish**.

Table 2-2 provides information about the parameters of the IT resource.

Table 2-2 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `RManager`
Key	Enter the key for the Java 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. Sample value: `300`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see Setting SSL for Connector Server and OIM in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

The IT resource for the Connector Server is created.

2.2.4 Creating a Target System User Account for Connector Operations

Oracle Identity Governance requires a target system user account to connect to and access the target system during reconciliation and provisioning operations. You must create this target system user account with appropriate permissions for connector operations.

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.

2.2.5 Creating the Parent Application

Before you create the application for your Exchange target system, you must create its parent application, which is the application for the Microsoft Active Directory target system, in Oracle Identity Governance.

You must specify this parent application (Microsoft Active Directory) as the value of the **Parent Application Name** dropdown on the Basic Information page while creating the

application for Exchange. By doing so, the new application (for Exchange) inherits all the properties of its parent application (Microsoft Active Directory).

To create the parent application, see Creating an Application By Using the Microsoft Active Directory User Management Connector in *Oracle® Identity Governance Configuring the Microsoft Active Directory User Management Application*.

2.3 Creating an Application By Using the Connector

You can onboard an application into Oracle Identity Governance from the connector package by creating a Target application. To do so, you must log in to Identity Self Service and then choose the **Applications** box on the **Manage** tab.

The following is the high-level procedure to create an application by using the connector:

> **Note:**
>
> For detailed information on each of the steps in this procedure, see Creating Applications of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1. Create an application in Identity Self Service. The high-level steps are as follows:
   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
   b. Ensure that the **Connector Package** option is selected when creating an application.
   c. From the **Parent Application Name** dropdown, ensure to select the application that you created for the Microsoft Active Directory target system. Specifying a value for the **Parent Application Name** dropdown is mandatory because this value links the Exchange application that you are about to create with the Microsoft Active Directory application, which is the parent application.
   d. Update the basic configuration parameters to include connectivity-related information.
   e. If required, update the advanced setting parameters to update configuration entries related to connector operations.
   f. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.

      If you want to perform Remote Mailbox provisioning, then add the **Remote Routing Address** and **Recipient Type Details** attributes to the existing list of attribute mappings.
   g. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
   h. Review the details of the application and click **Finish** to submit the application details.

      The application is created in Oracle Identity Governance.

i. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

   If you click **Yes**, then the default form is automatically created and is attached with the newly created application. The default form is created with the same name as the application. The default form cannot be modified later. Therefore, if you want to customize it, click **No** to manually create a new form and attach it with your application.

2. Log out of and log in to Identity Self Service, and then verify reconciliation and provisioning operations on the newly created application.

See Also:

- Setting Up Remote Mailbox Provisioning for an AOB Application for details on adding the **Remote Routing Address** and **Recipient Type Details** attributes to support Remote Mailbox provisioning from Oracle Identity Governance
- Configuring the Microsoft Exchange Connector for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector
- Configuring Oracle Identity Governance for details on creating a new form and associating it with your application, if you chose not to create the default form

3 Configuring the Microsoft Exchange Connector

While creating a target application, you must configure connection-related parameters that the connector uses to connect Oracle Identity Governance with your target system and perform connector operations. In addition, you can view and edit attribute mappings between the process form fields in Oracle Identity Governance and target system attributes, predefined correlation rules, situations and responses, and reconciliation jobs.

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to Microsoft Exchange.

Table 3-1 Basic Configuration Parameters for Microsoft Exchange

Parameter	Mandatory?	Description
Exchange Server Type	Yes	Enter the type of Microsoft Exchange Server. For Exchange 2016, set the value to `OnPremise2016`.
Connector Server Name	No	If you are using this connector with a .NET Connector Server, then enter the name of Connector Server IT resource.
Exchange Server Host	Yes	Enter the hostname of the computer hosting the Exchange Server.
Exchange User	Yes	User name of the service account having minimum privileges described in Creating a Target System User Account for Connector Operations. Enter the username in the following format: *DOMAIN_NAME\USER_NAME*

Table 3-1 (Cont.) Basic Configuration Parameters for Microsoft Exchange

Parameter	Mandatory?	Description
Exchange User Password	Yes	Enter the valid password for user specified for the Exchange User parameter.

3.2 Advanced Settings Parameters

These are the configuration-related entries that the connector uses during reconciliation and provisioning operations.

Table 3-2 Advanced Setting Parameters

Parameter	Mandatory ?	Description
Directory Admin Name	Yes	This parameter is used internally by the connector. Do not modify this entry. **Default value:** `UseDefault`
Directory Admin Password	Yes	This parameter is used internally by the connector. Do not modify this entry. **Default value:** `UseDefault`
Container	Yes	This parameter is used internally by the connector. Do not modify this entry. **Default value:** `UseDefault`
Use SSL For Remote PowerShell	No	This entry is used when the connector is configured against Exchange 2010 to remotely connect to the connector. **Default value:** `false` Do not modify this entry.
Authentication Mechanism	No	This entry is used when the connector is configured against Exchange to remotely connect to the Exchange Server. **Default value:** `Kerberos` Do not modify this entry.
Bundle Name	No	This entry holds the name of the connector bundle package. **Default value:** `ExchangeConnector`
Bundle Version	No	This entry holds the version of the connector bundle class. **Default value:** `12.3.0.0`
Default Incoming Message Size	No	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. Enter the appropriate default value for your organization. **Default value:** `10MB`
Connector Name	No	This entry holds the name of the connector class. **Default value:** `Org.IdentityConnectors.Exchange.ExchangeConnector`

Table 3-2 (Cont.) Advanced Setting Parameters

Parameter	Mandatory ?	Description
Mode	No	This parameter is used internally by the connector. **Default value:** `OIM`
Default Outgoing Message Size		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. Enter the appropriate default value for your organization. **Default value:** `10MB`
Domain Name	No	This parameter is used internally by the connector. Do not modify this entry. **Default value:** `UseDefault`

3.3 Attribute Mappings

The Schema page for a target application displays the default schema (provided by the connector) that maps Oracle Identity Governance attributes to target system attributes. The connector uses these mappings during reconciliation and provisioning operations.

Exchange User Attributes

Table 3-3 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Google Apps attributes. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute Mappings for a Microsoft Exchange User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive ?
User Logon Name	__NAME__	String	Yes	Yes	Yes	No	Not applicable
Alias	Alias	String	No	Yes	Yes	No	Not applicable
Display Name	DisplayName	String	No	Yes	Yes	No	Not applicable
Simple Display Name	SimpleDisplayName	String	Yes	Yes	Yes	No	Not applicable
Recipient Type	RecipientType	String	No	Yes	Yes	Yes	No

Table 3-3 (Cont.) Default Attribute Mappings for a Microsoft Exchange User Account

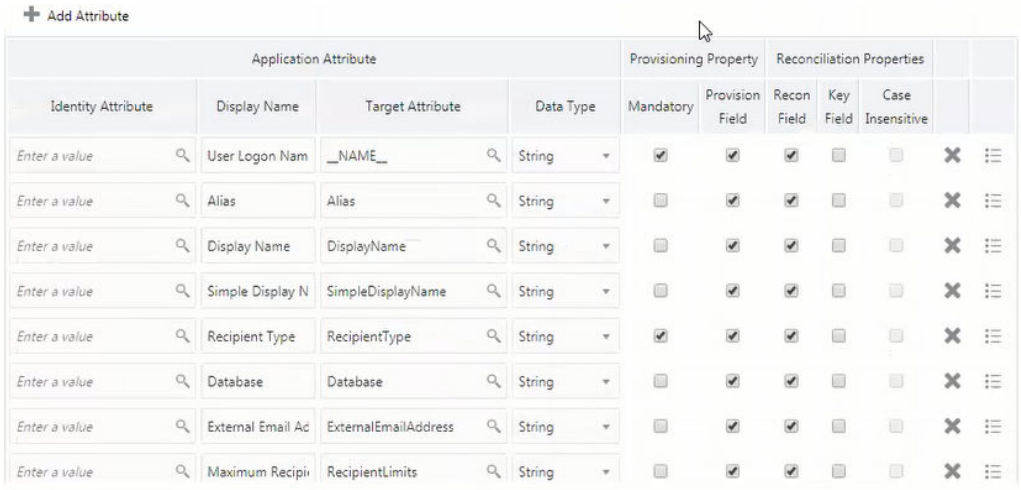
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
External Email Address	ExternalEmailAddress	String	No	Yes	Yes	No	Not applicable
Maximum Recipients	RecipientLimits	String	No	Yes	Yes	No	Not applicable
Max Incoming Message Size	MaxReceiveSize	String	No	Yes	Yes	No	Not applicable
Max Outgoing Message Size	MaxSendSize	String	No	Yes	Yes	No	Not applicable
Use Storage Defaults	UseDatabaseQuotaDefaults	Boolean	No	Yes	Yes	No	Not applicable
Mailbox Size Receipt Quota	ProhibitSendReceiveQuota	String	No	Yes	Yes	No	Not applicable
Mailbox Size Transmit Quota	ProhibitSendQuota	String	No	Yes	Yes	No	Not applicable
Mailbox Warning Size	IssueWarningQuota	String	No	Yes	Yes	No	Not applicable
Archive Mailbox Size	ArchiveQuota	String	No	Yes	No	No	Not applicable
Archive Mailbox Size Warning	ArchiveWarningQuota	String	No	Yes	No	No	Not applicable
Retain Deleted Items Defaults	UseDatabaseRetentionDefaults	Boolean	No	Yes	Yes	No	Not applicable
Retain Deleted Items For	RetainDeletedItemsFor	String	No	Yes	Yes	No	Not applicable
Retain Deleted Items Until Backup	RetainDeletedItemsUntilBackup	Boolean	No	Yes	Yes	No	Not applicable
Return Value	__UID__	String	No	Yes	Yes	Yes	No
Leave Start Date		Date	No	No	No	No	Not applicable
Leave End Date		Date	No	No	No	No	Not applicable

Table 3-3 (Cont.) Default Attribute Mappings for a Microsoft Exchange User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Hidden From Address Lists Enabled	HiddenFromAddressListsEnabled	Boolean	No	Yes	Yes	No	Not applicable
Email Address Policy Enabled	EmailAddressPolicyEnabled	Boolean	No	Yes	Yes	No	Not applicable
Primary SMTP Address	PrimarySmtpAddress	String	No	Yes	Yes	No	Not applicable
Server		Long	Yes	No	Yes	No	Not applicable
Message Format	MessageFormat	String	No	Yes	No	No	Not applicable
Message Body Format	MessageBodyFormat	String	No	Yes	No	No	Not applicable
Use Prefer Message Format	UsePreferMessageFormat	String	No	Yes	No	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable

Figure 3-1 shows some of the default User account attribute mappings.

Figure 3-1 Default Attribute Mappings for Exchange User Account



Distribution Groups Child Attributes

Table 3-4 lists the attribute mappings for distribution groups between the process form fields in Oracle Identity Governance and Exchange attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

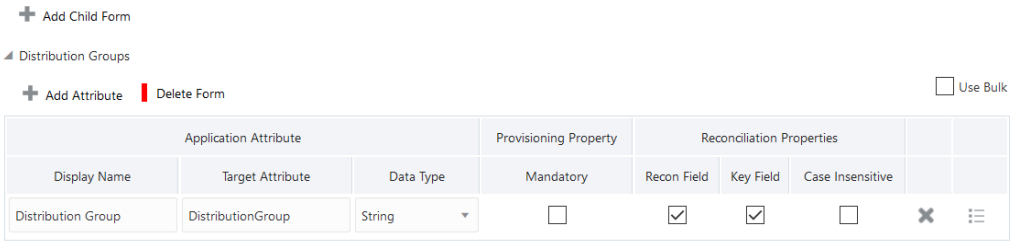
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for Exchange Distribution Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Distribution Group	DistributionGroup	String	No	Yes	Yes	No

Figure 3-2 shows the default Distribution Groups child attribute mapping.

Figure 3-2 Default Attribute Mappings for Distribution Groups



3.4 Correlation Rules

When you create a Target application, the connector uses correlation rules to determine the identity to which Oracle Identity Governance must assign a resource.

Predefined Identity Rules

By default, the Exchange connector provides a simple correlation rule when you create a Target application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Predefined Identity Correlation Rule for an Exchange Target Application

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
SamAccountName	Equals	User Login	No

In this identity rule:

- SamAccountName is a field on Microsoft Active Directory that represents the login name of the user account.
- User Login is a field on the OIM User form that holds the unique ID of the Exchange user.
- Rule operator is AND.

Predefined Situations and Responses

The Exchange connector provides a default set of situations and responses when you create a Target application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

Table 3-6 lists the default situations and responses for the Exchange application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-6 Predefined Situations and Responses for Exchange

Situation	Response
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

3.5 Reconciliation Jobs

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application.

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing these predefined jobs or creating new ones, see Updating Reconciliation Jobs in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

User Reconciliation Job

The Exchange Target Resource User Reconciliation job is used to reconcile user data from a target application.

Table 3-7 Parameters of the Exchange Target Resource User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
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.
Scheduled Task Name	This parameter holds the name of the scheduled job. **Note:** For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter. Default value: *APP_NAME* Exchange Target Resource User Reconciliation
OrganizationalUnit	Specifies the distinguished name of the OU from which you want to reconcile mailboxes.
Incremental Recon Attribute	Default value: `LastModified`
Latest Token	Time stamp at which the last reconciliation run started. Note: Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.
Filter	Enter the search filter for fetching user records from the target system during a reconciliation run. See Performing Limited Reconciliation for more information about this attribute.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` Do not change the default value.

Delete User Reconciliation Job

The Exchange Target Resource Delete User Reconciliation job is used to reconcile deleted user data from a target application.

Table 3-8 Parameters of the Exchange Target Resource Delete User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` Do not change the default value.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- Exchange User Distribution Group Lookup Reconciliation

  Use this reconciliation job to fetch all mail-enabled universal distribution groups present in the forest into Oracle Identity Governance.

- Exchange User Mailbox Database Group Lookup Reconciliation

  Use this reconciliation job to synchronize mailbox database lookup fields in Oracle Identity Governance with mailbox databases in the target system.

The parameters for both the reconciliation jobs are the same.

Table 3-9 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
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: `__NAME__` **Note:** Do not change the value of this attribute.
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: `__NAME__` **Note:** Do not change the value of this attribute.

Table 3-9 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Depending on the reconciliation job you are using, the default values are as follows: • For Exchange User Distribution Group Lookup Reconciliation - `Lookup.Exchange.DistributionGroups` • For Exchange User Mailbox Database Group Lookup Reconciliation - `Lookup.Exchange.MailboxDatabase`
Object Type	Enter the type of object whose values must be synchronized. Depending on the reconciliation job you are using, the default values are as follows: • For Exchange User Distribution Group Lookup Reconciliation - `__DISTRIBUTIONGROUP__` • For Exchange User Mailbox Database Group Lookup Reconciliation - `__MAILBOXDATABASE__` **Note:** Do not change the value of this attribute.

Leave Of Absence Reconciliation Job

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

> **Note:**
>
> This recon job is loaded into the system through the xml/Exchange-pre-config.xml file after you create your Exchange application. You can access and run this job only from the Identity System Administration console once the application is created.

To run this job, you must specify the name of the application against which reconciliation runs must be performed.

This job 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 job runs and sets the **HiddenFromAddressListsEnabled** attribute on Microsoft Exchange for that user. Otherwise, this task resets the **HiddenFromAddressListsEnabled** attribute for that user.

4

Performing the Postconfiguration Tasks for the Microsoft Exchange Connector

These are the tasks that you can perform after creating the application in Oracle Identity Governance.

- Configuring Oracle Identity Governance
- Harvesting Entitlements and Sync Catalog
- Setting Up Remote Mailbox Provisioning
- Localizing Field Labels in UI Forms
- Configuring SSL Between Oracle Identity Governance and Connector Server

4.1 Configuring Oracle Identity Governance

During application creation, if you did not choose to create a default form, then you must create a UI form for the application that you created by using the connector.

> **Note:**
>
> Perform the procedures described in this section only if you did not choose to create the default form during creating the application.

The following topics describe the procedures to configure Oracle Identity Governance:

- Creating and Activating a Sandbox
- Creating a New UI Form
- Publishing a Sandbox
- Updating an Existing Application Instance with a New Form

4.1.1 Creating and Activating a Sandbox

You must create and activate a sandbox to begin using the customization and form management features. You can then publish the sandbox to make the customizations available to other users.

See Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.1.2 Creating a New UI Form

You can use Form Designer in Oracle Identity System Administration to create and manage application instance forms.

See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

While creating the UI form, ensure that you select the resource object corresponding to the newly created application that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

4.1.3 Publishing a Sandbox

Before publishing a sandbox, perform this procedure as a best practice to validate all sandbox changes made till this stage as it is difficult to revert the changes after a sandbox is published.

1. In Identity System Administration, deactivate the sandbox.
2. Log out of Identity System Administration.
3. Log in to Identity Self Service using the xelsysadm user credentials and then activate the sandbox that you deactivated in Step 1.
4. In the Catalog, ensure that the application instance form for your resource appears with correct fields.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.1.4 Updating an Existing Application Instance with a New Form

For any changes that you do in the schema of your application in Identity Self Service, 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 and activate a sandbox.
2. Create a new UI form for the resource.
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.

See Also:

- Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
- Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*
- Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*

4.2 Harvesting Entitlements and Sync Catalog

You can populate Entitlement schema from child process form table, and harvest roles, application instances, and entitlements into catalog. You can also load catalog metadata.

To harvest entitlements and sync catalog:

1. Run the reconciliation jobs for lookup field synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

> **See Also:**
>
> - Reconciliation Jobs for a list of jobs for entitlements (lookup field synchronization)
> - Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for information about the Entitlement List and Catalog Synchronization Job scheduled jobs

4.3 Setting Up Remote Mailbox Provisioning

You can configure your Exchange application or resource to support Remote Mailbox provisioning operations.

- Setting Up Remote Mailbox Provisioning for an AOB Application
- Setting Up Remote Mailbox Provisioning for a CI-Based Resource

4.3.1 Setting Up Remote Mailbox Provisioning for an AOB Application

You can configure your Exchange application to support Remote Mailbox provisioning operation.

You can set up Remote Mailbox provisioning either during or after the creation of your Exchange application.

1. Log in to Identity Self Service.
2. Depending on whether you are setting up Remote Mailbox provisioning during or after the creation of your Exchange application, perform one of the following steps:
   - For setting up Remote mailbox provisioning during Exchange application creation, fill in all the necessary details on the Basic Information page and then navigate to the Schema page.
   - For setting up Remote mailbox provisioning after creating the Exchange application, search for and open the application you created for editing.
3. On the Schema page, add two new attributes as follows:

a. Click **Add Attribute**.

b. In the newly added row, enter values for the following fields:

- **Display Name**: `Remote Routing Address`

- **Target Attribute**: `RemoteRoutingAddress`

- Select the **Provision Field** and **Recon Field** check boxes.

- Click **Advanced Settings** denoted by three horizontal lines at the end of the row, select the **Provide old value on update** checkbox, and then click **OK**.

c. If you want to reconcile Remote Mailbox Type, then click **Add Attribute** to add a new attribute named Recipient Type Details.

d. In the newly added row, enter values for the following fields:

- **Display Name**: `Recipient Type Details`

- **Target Attribute**: `RecipientTypeDetails`

- Deselect the **Provision Field** checkbox and select the **Recon Field** check box.

4. If you are in the process of creating the Exchange application, then continue with the rest of the process for creating it.
5. If you added the attributes for Remote Mailbox provisioning to an existing application, then apply your changes. Then, log in to Identity System Administration, create a new form and associate it with your updated Exchange application.
6. Log in to Identity System Administration.
7. Search for and open the **Lookup.Exchange.RecipientType.Options** lookup.
8. Add a new entry to the lookup with both the code and decode values as `RemoteUserMailbox` and save your changes.
9. Verify that the lookup **Lookup.Exchange.RecipientType.Options** contains the newly added entry.

4.3.2 Setting Up Remote Mailbox Provisioning for a CI-Based Resource

You can configure your Exchange resource to support Remote Mailbox provisioning operations after you deploy the connector.

1. Log in to Oracle Identity Manager Design Console.
2. Update the **Lookup.Exchange.RecipientType.Options** lookup definition to include an entry for Remote User Mailbox as follows:

a. Expand **Administration**, and then double-click **Lookup Definition**.

b. Search for and open the **Lookup.Exchange.RecipientType.Options** lookup definition.

c. Add a new entry to the lookup definition with the Code Key and Decode values as **RemoteUserMailbox** and **Remote User Mailbox**, respectively.

d. Verify that the **Lookup.Exchange.RecipientType.Options** lookup definition contains the newly added entry.

3. Update the **UD_Exchange** process form by adding a new field for Remote Routing Address as follows:
   a. Expand **Development Tools**, and then double-click **Form Designer**.
   b. Search for and open the **UD_Exchange** process form.
   c. Click **Create a New Version**.
   d. Click **Add** to add the new field and enter all the required details. Ensure that you enter the form field name as `Remote Routing Address`. Enter values for form field label, length, and other properties as per your requirement.
   e. Click **Make Version Active** to activate the new version of the process form.
4. Update the **Lookup.Exchange.UM.ProvAttrMap** lookup definition for provisioning by adding a new entry with the Code Key and Decode values as **Remote Routing Address** and **RemoteRoutingAddress**, respectively.
5. Add the new field to the list of reconciliation fields in the resource object as follows:
   a. Expand **Resource Management** and then double-click **Resource Objects**.
   b. Search for and open the **Exchange User** resource object.
   c. On the Object Reconciliation tab, click **Add Field**. Then, in the Add Reconciliation Field dialog box, enter the details for the RemoteRoutingAddress field.
   d. Click **Create Reconciliation Profile** to copy changes made to the resource object into the MDS.
6. Create a reconciliation field mapping for the new field on the process form as follows:
   a. Expand **Process Management** and then double-click **Process Definition**.
   b. From the Process Definition table, select and open the **Exchange User** resource object.
   c. Click **Reconciliation Field Mappings** and then click **Add Field Map**.
   d. Enter all the details for the RemoteRoutingAddress field and then save your changes.
7. Create an entry for the field in the lookup definition for reconciliation as follows:
   a. Expand **Administration**, and then double-click **Lookup Definition**.
   b. Search for and open the **Lookup.Exchange.UM.ReconAttrMap** lookup definition.
   c. Add a new entry to the lookup definition with the Code Key and Decode values as **RemoteRoutingAddress** and **Remote Routing Address**, respectively and the save your changes.
8. On the Resource Objects form, click **Create Reconciliation Profile** to copy changes made to the resource object into the MDS.
9. If you want to reconcile Remote Mailbox Type, then you must add a new entry named "Recipient Type Details" for reconciliation as follows:

   Perform Steps 5 through 8 to add the Recipient Type Details field for reconciliation. While performing these steps ensure to replace RemoteRoutingAddress with RecipientTypeDetails.
10. Restart Oracle Identity Manager.

4.4 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. The resource bundles are available in the connector installation media.

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 (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor if you are using Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) or later:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.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.

4.5 Configuring SSL Between Oracle Identity Governance and Connector Server

You must configure SSL to secure communication between Oracle Identity Governance 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 Governance and connector server:

- Exporting the Certificate
- Configuring the Connector Server for SSL
- Configuring Oracle Identity Governance for SSL

4.5.1 Exporting the Certificate

You can export the certificate generated by CA by using the Microsoft Management Console. Ensure to export the certificate by creating a certificate file (.cer). For detailed instruction on exporting the certificate, refer to the target system documentation.

4.5.2 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.usessl" 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.

4.5.3 Configuring Oracle Identity Governance for SSL

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

1. Copy the certificate generated in Step 1 of Configuring the Connector Server for SSL to the computer on which Oracle Identity Governance is running.
2. Import the target system certificate into the JDK used by Oracle Identity Governance by running the following command:
   - For Oracle Identity Governance 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 sample_password
```

- For Oracle Identity Governance 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 sample_password
  ```

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

   - For Oracle Identity Governance 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 Governance 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 $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 sample_password
```

```
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`.

5

Using the Microsoft Exchange Connector

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

The following topics discuss information related to using the connector for performing reconciliation and provisioning operations:

- Guidelines on Using the Connector
- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Performing Provisioning Operations
- Uninstalling the Connector

5.1 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

5.1.1 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.

5.1.2 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.

5.2 Configuring Reconciliation

You can configure the connector to specify the type of reconciliation and its schedule.

This section provides information on the following topics related to configuring reconciliation:

- Performing Full Reconciliation and Incremental Reconciliation
- Performing Limited Reconciliation

5.2.1 Performing Full Reconciliation and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager.

After you create the application, 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 reconciliation job. If the value of the DomainController parameter is blank, then reconciliation is performed against a forest.

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

- Filter
- Incremental Recon Attribute
- Latest Token

5.2.2 Performing Limited Reconciliation

By default, all target system records are reconciled during the current reconciliation run. You can customize this process by specifying the subset of target system records that must be reconciled.

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

For detailed information about ICF Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

5.3 Configuring Reconciliation Jobs

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

You can apply this procedure to configure the reconciliation jobs for users and entitlements.

To configure a reconciliation job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:
   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

   In addition to modifying the job details, you can enable or disable a job.
5. On the **Job Details** tab, in the Parameters region, specify values for the attributes of the scheduled task.

> **Note:**
>
> 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.

6. Click **Apply** to save the changes.

> **Note:**
>
> You can use the Scheduler Status page in Identity System Administration to either start, stop, or reinitialize the scheduler.

5.4 Performing Provisioning Operations

You create a new user in Identity Self Service by using the Create User page. You provision or request for accounts on the Accounts tab of the User Details page.

To perform provisioning operations in Oracle Identity Governance:

1. Log in to Identity Self Service.
2. Create a user as follows:
   a. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
   b. From the Actions menu, select **Create**. Alternatively, you can click **Create** on the toolbar. The Create User page is displayed with input fields for user profile attributes.
   c. Enter details of the user in the Create User page.
3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance for the connector that you configured earlier, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.

> **See Also:**
>
> Creating a User in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for details about the fields on the Create User page

5.5 Uninstalling the Connector

Uninstalling the connector deletes all the account-related data associated with its resource objects.

If you want to uninstall the connector for any reason, then run the Uninstall Connector utility. Before you run this utility, ensure that you set values for `ObjectType` and `ObjectValues` properties in the ConnectorUninstall.properties file. For example, if you want to delete resource objects, scheduled tasks, and scheduled jobs associated with the connector, then enter `"ResourceObject", "ScheduleTask", "ScheduleJob"` as the value of the `ObjectType` property and a semicolon-separated list of object values corresponding to your connector (for

example, `ActiveDirectory User; ActiveDirectory Group`) as the value of the `ObjectValues` property.

For more information, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

6

Extending the Functionality of the Microsoft Exchange Connector

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

6.1 Adding New Multivalued Fields

You can add multivalued fields for user reconciliation and provisioning between Oracle Identity Governance and the target system.

By default, the multivalued fields listed on the Schema page for your application in Identity Self Server are mapped for provisioning and reconciliation between Oracle Identity Governance and the target system. If required, you can add new multivalued fields for provisioning and reconciliation.

To add new multivalued fields for reconciling users from a target application (or target resource reconciliation):

1. Log in to Oracle Identity System Administration and create a lookup that can hold the list of values for the multivalued field that you want to add.
2. Create a child form and add attributes as follows:
   a. Log in to Identity Self Service.
   b. Search for and open the application you created for your target system for editing.
   c. On the Schema page, add a new child form and its attributes.

      For example, enter the following values:

      - **Display Name**: `Proxy Address`
      - **Target Attribute**: `EmailAddresses`
      - Ensure that the **Recon Field** option is selected.

> **Note:**
>
> - When you add attributes to the child form, from the Advanced Settings option, ensure to mark the newly added attribute as a **Lookup**.
> - In the List of values field, enter the name of the lookup created in Step 1.

d. Apply your changes.

3. Log in to Identity System Administration, create a new form and associate it with your application.

> **See Also:**
>
> - Creating a Lookup Type in *Oracle Fusion Middleware Administering Oracle Identity Governance* for details about create lookups for your multivalued fields
> - Adding Child Forms in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for information about creating a child form and adding attributes
> - Configuring Oracle Identity Governance for information about creating a new form and associating it with your application

6.2 Configuring Transformation and Validation of Data

Configure transformation and validation of user account data by writing Groovy script logic while creating your application.

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 Governance.

Similarly, 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 transformation or validation of user account data, you must write Groovy scripts while creating your application. For more information about writing Groovy script-based validation and transformation logic, see Validation and Transformation of Provisioning and Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.3 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

6.3.1 About Configuring Action Scripts

You can configure **Action Scripts** by writing your own PowerShell scripts while creating your application.

These scripts can be configured to run before or after the create, update, or delete an account provisioning operations. For example, you can configure a script to run before every mailbox creation operation.

For information on adding or editing action scripts, see Updating the Provisioning Configuration in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

> **Note:**
>
> The scripting language used is PowerShell.

The following are some important points pertaining to 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.

  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.
- 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.

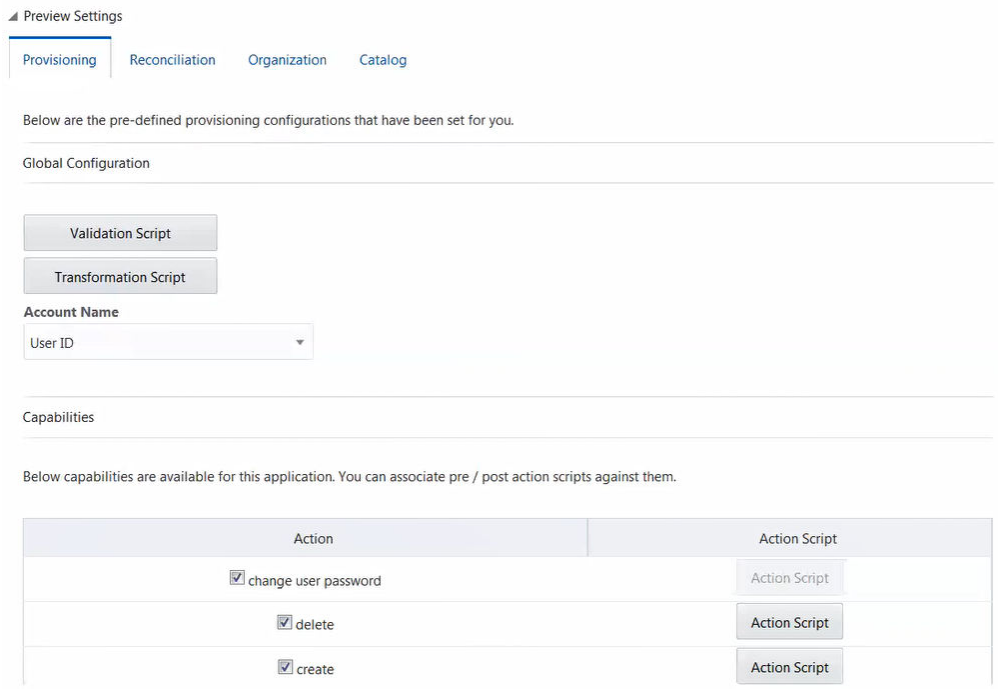
    If other attributes are also required, then you must create and use a new adapter calling `ICProvisioningManager# updateAttributeValues(String objectType, String[] labels)`. During adapter mapping in process task, add the form field labels of the dependent attributes.
  - During delete operations, only the `__UID__ (GUID)` attribute is available to the script.

6.3.2 Running a Custom PowerShell Script

As an example, the following procedure describes the steps to run a custom PowerShell script before a create operation:

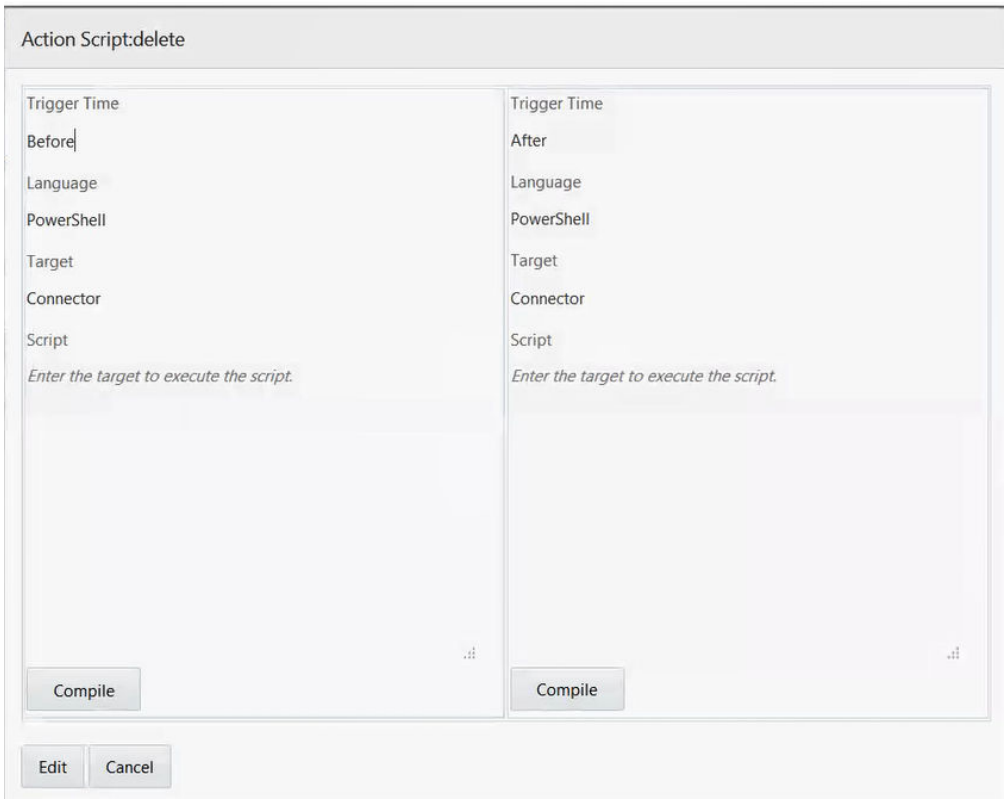
1. Select an application of your choice after creating it or while updating it.
2. Select the **Settings** tab, **User**, and then **Provisioning**. All available action scripts are displayed.

Figure 6-1 Preview Settings for Action Scripts



3. To view its contents, click any of the enabled action scripts.

Figure 6-2 Action Scripts



4. Click **Edit**, and then enter the following content in the **Script** field:

```
Powershell.exe -File NAME_AND_FULL_LOCATION_OF_THE_CUSTOM_SCRIPT %Alias% -
SimpleDisplayName %DisplayName%
Exit
```

Sample value:

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

5. Click **Compile** to check if the script is valid, and then click **Save**.
6. Log in to the computer running the connector server and create the custom script (in this example the customScript.ps1 script, located in the C:\PSScript directory) file with the following content:

Note:

Before running this script using the connector or Oracle Identity Governance, 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 the `$pw` variable with the actual password. The value `Welcome1` is specified as a sample value.
- Update the value of the `$cred` variable with the actual username. The value `Connectorse1\oim_exch_service` has been specified as a sample value.
- Update the value of the `$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

.DESCRIPTION
    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.

7

Upgrading the Microsoft Exchange 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.

7.1 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.

7.2 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.

7.3 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.
   c. Create a new UI form to view the upgraded fields.
   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.
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.

4. Update the Connector Server bundle DLLs as described in Copying and Extracting the Connector Bundle to the Connector Server.
5. Re-configure the IT resource of the source connector (an earlier release of the connector that must be upgraded).

> **See Also:**
>
> Creating a Sandbox, Activating a Sandbox, and Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* and Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance* for detailed instructions on some of the steps in this topic.

8

Troubleshooting the Microsoft Exchange Connector

These are the solutions to some issues associated with the Exchange connector.

Table 8-1 lists solutions to some commonly encountered issues associated with the Exchange connector:

Table 8-1 Troubleshooting Common Connector Issues

Problem Description	Solution
The Exchange connector throws the following error: `Could not find domain controller for user <user_name>`	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 <add name="ExchangeSwitch" value="4" /> 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 8-1 (Cont.) Troubleshooting Common Connector Issues

Problem Description	Solution
The Exchange connector throws the following error: `ConnectorServer.exe Error 0 Problem while PowerShell execution System.Management.Automation.Remoting.PSRemotingTransportException: 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_Troubleshooting Help topic.`	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 Creating the IT Resource for the Connector Server for detailed information about this parameter.

9

Known Issues and Workarounds for the Microsoft Exchange Connector

These are known issues associated with this release of the connector.

Exchange Resource Remains In Provisioning Status When It Is Provisioned Before Provisioning the AD Resource

When you provision an Exchange resource to a user, the provisioning operation remains in Waiting status if the user has not been provisioned an AD resource yet. After you provision the AD resource, the Exchange resource provisioning operation should be complete. However, the Exchange resource continues to remain in the Provisioning status. In addition, the Resource History displays the System Validation task to be in the Pending state.

Workaround: Perform the following steps before you provision the Exchange resource:

1. Ensure you created the Exchange application with the AD application as the Parent application.
2. Log in to Oracle Identity Design Console.
3. Search for and open the process form for the Exchange application and select the **Auto Save** and **Auto Prepop** checkboxes.
4. Save the changes.

Onboarding the Microsoft Exchange 12c Connector Application Fails Due to the Four Character Application Name Limitation

Installation of the Microsoft Exchange 12c Connector in the AOB mode fails as the application name exceeds four characters. The connector throws the following error message while creating the application with application name exceeding four characters:

```
Application creation failed Internal Server Error Parent
field attribute withname Retain Deleted Items Until Backup,
type CheckBox,data type Booleanfailed with exception There
is already an existing database object with thegiven name :
UD_EXCHANGE_RETAIN_DELETED_IT1.
```

Workaround: As a fix, limit the character length of the application name to four characters. For example, while creating the application, specify `EXCH` or `EXNG` as the value for the **Application Name** field instead of `EXCHANGE`.

10
Frequently Asked Questions

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

1. 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.

2. Can the 11.*x* Exchange connector co-exist with the 12c Exchange connector?

   Answer: No. A connector once managed through CI-based installation, cannot be managed through AOB.

3. Is it mandatory to install the Active Directory connector 12c before installing Exchange connector 12c?

   Answer: Yes.

4. 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.

5. 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.

6. 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.

7. I performed target resource reconciliation using filters in the reconciliation 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 OIG 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 Governance via ICF INTG. Even before data reaches ICF INTG, ICF (framework) applies a case-sensitive search against the result sent by the 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.

8. 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.

9. 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.

10. I see that the values for the Container, Directory AdminName, Directory Admin Password, and Domain Name parameters in the Advanced Settings section set to `UseDefault`. What is the significance of these parameters 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 Advanced Settings section.

11. Explain what cmdlets the connector runs during create, update, delete, disable and enable operations in Oracle Identity Governance (OIG).

    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.

12. The Distribution Group Lookup Reconciliation and Target Resource User Reconciliation jobs 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.

13. I have configured my action script to run after the 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 Governance, then open a PowerShell window and run the same commands manually to verify if there is any issue.

Note that Oracle Identity Governance does not return any exceptions or runtime errors that occur when the script is running.

A

Files and Directories in the Microsoft Exchange Connector Installation Package

These are the components of the connector installation package that comprise the Microsoft Exchange connector.

Table A-1 Files and Directories in the Connector Installation Package

File in the Installation Package Directory	Description
bundle/Exchange.Connector-12.3.0.0.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 • ModifyResourceExchange.xml • ProvisionResourceExchange.xml	These XML files specify the information to be submitted by the requester during a request-based provisioning operation. **Note:** These files are applicable only if you are using an Oracle Identity Manager release prior to 11.1.2.
Files in the javadoc directory	This directory contains information about the Java APIs used by the Exchange Leave Of Absence Update Task.
lib/Exchange-oim-integration.jar	This JAR file contains the class files that are specific to the 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 the 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. **Note:** A **resource bundle** 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. **Note:** Run this script only if you are upgrading the connector from release 9.*x* to 11.*x*.
xml/Exchange-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects such as Recipient Types and so on.
xml/Exchange-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system . It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.

Table A-1 (Cont.) Files and Directories in the Connector Installation Package

File in the Installation Package Directory	Description
xml/Exchange-ConnectorConfig.xml	This XML file contains definitions for the connector components. These components include the following: • IT resource type • Connector server IT Resource type • IT resource instance • Connector server IT resource instance • Process forms • Resource object • Process definition • Process tasks • Adapters • Reconciliation rules • Prepopulate adapters • Lookup definitions • Scheduled tasks
xml/Exchange-Datasets.xml	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. **Note:** This file is applicable only if you are using an Oracle Identity Manager release prior to 11.1.2.

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.

- AntispamBypassEnabled
- CustomAttribute1
- CustomAttribute2
- CustomAttribute3
- CustomAttribute4
- CustomAttribute5
- CustomAttribute6
- CustomAttribute7
- CustomAttribute8
- CustomAttribute9
- CustomAttribute10
- CustomAttribute11
- CustomAttribute12
- CustomAttribute13
- CustomAttribute14
- CustomAttribute15
- Work
- UserPrincipalName
- WindowsEmailAddress