www.novell.com/documentation

Office 365 Driver Implementation Guide

Identity Manager 4.0.2

January 2014

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

Contents

About This Guide

This guide explains how to install and configure the Identity Manager 4.0.2 Driver for Office 365.

Audience

This guide is for Identity Manager and Office 365 administrators who are using the Identity Manager Driver for Office 365.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, and enter your comments there.

Documentation Updates

For the most recent version of this document, see the Identity Manager 4.0.2 Drivers Documentation Web site.

Additional Documentation

For information on Identity Manager, see the Identity Manager Documentation Web site.

1 Understanding the Office 365 Driver

Identity Manager 4.0 and later offers automatic provisioning and synchronization of users to cloud applications. The new Office 365 driver for Novell Identity Manager seamlessly provisions and deprovisions users, group memberships, roles, and licenses to the Microsoft Online Services cloud application and keeps user identity information consistent across both the Identity Vault and Office 365.

Office 365 includes the hosted versions of Microsoft's Server products. The driver provisions users to the following Microsoft Online Services:

- Microsoft Exchange Online
- Microsoft SharePoint Online
- Microsoft Lync Online
- Office Professional Plus
- Office WebApps

NOTE: The Office 365 driver supports secure password synchronization between the Identity Vault and the Office 365 on the Subscriber channel only. The driver uses several protocols to enable identity provisioning and data synchronization between the Identity Vault and Office 365.

1.1 Key Features

The Office 365 driver supports the following features:

- Provisioning users, group membership, roles, and licenses from the Identity Vault. Microsoft Active Directory is not mandatory for provisioning of Office 365 users. Also, Active Directory Federation Service is not required.
- Managing users and security groups.
- Creating and managing of Exchange Distribution List and Mail-enabled security groups.
- Creating user accounts based on policies and entitlements.
- Creating and assigning custom licenses to enable or disable specific services of Office 365.
- Providing additional support for provisioning Active Directory users to Office 365.

IMPORTANT: When you configure the Office 365 driver, you can either select the default or Active Directory configuration to synchronize identities. If you choose to configure the Identity Vault as the identity provider, association to any other directory is not required. With Active Directory, you can synchronize only users and groups that have an association.

1.2 Driver Concepts

- Section 1.2.1, "Office 365 Driver Shim," on page 8
- Section 1.2.2, "Data Transfer between Systems," on page 8
- Section 1.2.3, "How the Driver Works," on page 8

1.2.1 Office 365 Driver Shim

The driver shim converts the XML-based Identity Manager command and event language (XDS) to the protocols and API calls needed to interact with Office 365. The shim for Office 365 is `DXMLMSOnlineDriver.dll`.

The shim is called by the driver to execute the PowerShell commands on the machine hosting the driver shim after the Output Transformation runs. The shim also generates events from Office 365 for the Input Transformation policy.

1.2.2 Data Transfer between Systems

The driver supports two data transfer channels, the Publisher and the Subscriber channels, between the Identity Vault and Office 365.

The Subscriber channel controls data transfer as follows:

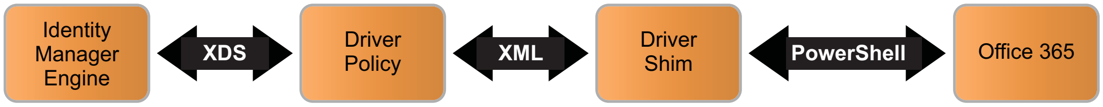
- The channel monitors the Identity Vault for new objects and changes to the existing objects.
- The channel sends the relevant changes to the driver shim to be executed in Office 365.

With filters and policies, you can configure the driver to control and manage the changes that are detected and sent to Office 365.

1.2.3 How the Driver Works

Figure 1-1 illustrates the data flow between Identity Manager and Office 365:

Figure 1-1 *Office 365 Driver Data Flow*



The Identity Manager engine uses XDS, a specialized form of XML, to represent events in the Identity Vault. Identity Manager engine passes the XDS to the driver policy, which can consist of basic policies, DirXML Script, and XSLT style sheets.

The driver shim receives XML from the Identity Manager engine. Based on the input XML, the driver uses Microsoft PowerShell infrastructure and Microsoft Online Services cmdlets for transferring data into and out of Office 365.

The cmdlets apply functions to manage users and groups in Office 365. When the driver receives an add, modify, or delete event from the Identity Vault, it executes the PowerShell cmdlets to provision, modify, or deprovision users to Office 365. The Subscriber channel synchronizes users, groups, and licenses.

On a successful Add, Modify, or Delete operation, the driver stores the XDS events into a change cache. Passwords are not stored in the change cache. By default, the change cache is located in the `C:\Temp` folder on the Remote Loader server.

The driver uses the change cache to prevent loopback of events on the Publisher channel. The Publisher channel periodically polls the change cache for additions and modifications to users and groups. The user attributes returned by the query are based on the Sync Filter settings of the driver. By default, the Publisher channel checks the change cache every 60 seconds. Ensure that the change cache is encrypted. Change cache can be encrypted by specifying the Database Password in the Driver Properties.

Each user entry returned by the query is compared with the user data in the Publisher database. Depending on the query results, the Publisher channel sends one of the following notifications to the Identity Vault:

- If a user is not present in the database, the Publisher channel sends an Add operation request to the Identity Vault.
- If you modify one or more attributes of a user, the Publisher channel sends a Modify operation request to the Identity Vault.
- If the database contains users that are not returned by the query, the Publisher channel sends a Delete operation request to the Identity Vault.

The driver provides a configurable option, *Confirm Publisher Deletes,* to query Office 365 for revalidating a delete request for a specific object. This option is enabled by default, which means the driver queries Office 365 to ensure that a specific user or a group is deleted from Office 365 before the Publisher channel can send a delete request to the Identity Vault.

1.3 Support for Standard Driver Features

The following sections provide information about the ways in which Office 365 driver supports standard driver features:

1.3.1 Supported Operations

The Office 365 driver performs the following operations on the Publisher and Subscriber channels:

- **Publisher Channel:** Add, Modify, Delete, Migrate, and Query operations on User and Group objects.
- **Subscriber Channel:** Add, Modify, Delete, Migrate, and Query operations on User and Group objects, and Password Set/Reset operations only on User objects. Based on the access entitlements to Office 365 services, specific License Assignments are set on the users. A License Assignment is required by the users to access specific services in Office 365. The driver has the capability to selectively provision users to specific services in Office 365.

1.3.2 Password Synchronization

The Subscriber channel sets the password. Passwords are not synchronized on the Publisher channel. This means that passwords are synchronized from the Identity Vault to Office 365, but not from Office 365 to the Identity Vault.

1.3.3 Object Synchronization

The Office 365 driver synchronizes users and groups.

1.3.4 Exchange Distribution Lists and Mail-Enabled Security Groups Synchronization

The driver supports creation and management of Distribution and Mail-enabled Security Groups. It supports multiple group attributes to enable creation and management of these groups. You must use the GroupType attribute in the Office 365 schema to synchronize the desired groups.

- If the GroupType contains *DistributionList*, it creates an Exchange Distribution List.
- If the GroupType contains *MailEnabledSecurity*, it creates an Exchange Security Group.
- If the GroupType contains *Security*, it creates an Office 365 Security Group.

The local variables are initialized at the driver scope in the Output Transformation Policy of the default configuration package. Use an appropriate local variable value for the GroupType attribute in the XDS document to synchronize on the Subscriber channel.

Memberships to the groups are granted via entitlements.

1.3.5 Entitlements

The Office 365 driver implements entitlements. You should enable entitlements for the driver only if you plan to use the User Application or Role-Based Entitlements with the driver. For more information about entitlements, see the *Identity Manager 4.0.2 Entitlements Guide*.

Entitlements make it easier to integrate Identity Manager with the Identity Manager User Application and Role-Based Services in the Identity Vault. In the User Application, an action such as provisioning an account in Office 365 is delayed until the proper approvals are made. In Role-Based Services, rights are assigned based on attributes of a user object and not by regular group membership. Both of these services offer a challenge to Identity Manager, because it is not obvious from the attributes of an object whether an approval is granted or the user matches a role. Entitlements standardize a method of recording this information on objects in the Identity Vault.

From the driver perspective, an entitlement grants or revokes the right to resources in Office 365. You can use entitlements to grant the right to an account in Office 365 or to control group membership. The driver is unaware of the User Application or Role-Based Entitlements. It depends on the User Application server or the Entitlements driver to grant or revoke the entitlement for a user based on its own rules.

NOTE: License entitlement is configured as a single-valued resource in User Application. Therefore to assign multiple Office 365 driver licenses, you must create resources for each value that needs be assigned in the User Application. The driver supports only one license assignment per operation.

You can also configure the driver without using entitlements. In such scenarios, Active Directory could be the authoritative source for both users and group membership. After the Active Directory driver synchronizes identities and group memberships from Active Directory into the Identity Vault, the Office 365 driver synchronizes those objects from the Identity Vault into Office 365. However, you can also configure the driver without Active Directory and entitlements.

1.4 Checklist for Enabling User Synchronization

Use the following checklist to verify that you complete the following tasks in order to have a complete solution with the driver.

- Ensure that you have installed the software mentioned in Section 2.1, "Prerequisites," on page 13.
- Install the driver object. For more information, see Chapter 2, "Installing the Driver Files," on page 13.
- Create and configure the driver object. For more information, see Chapter 3, "Creating a New Driver Object," on page 15.

2 Installing the Driver Files

Unlike most Identity Manager drivers, the Identity Manager engine cannot directly load the Office 365 driver. The Office 365 driver can only be run from the .NET Remote Loader that has been modified to support it. For information about the supported operating systems, see "Remote Loader" in "System Requirements" in the *Identity Manager 4.0.2 Framework Installation Guide*.

You must install the Office 365 driver on a server that has HTTP access to the Office 365 Web service with which the driver communicates.

2.1 Prerequisites

To provision the Identity Vault users with Office 365, you need the following software:

- Novell Identity Manager 4.0.2 and its prerequisites, as listed in "System Requirements" in the *Identity Manager 4.0.2 Framework Installation Guide*.
- Microsoft Windows Server 2008 R2 (64-bit), Microsoft Windows Server 2012, and Microsoft Windows Server 2012 R2.

  Note that Office 365 driver supports .NET Remote Loader running on these Windows platforms.
- Microsoft Windows PowerShell Version 2.0 or later.
- Microsoft .NET Framework Version 3.5 SP1.
- Microsoft Online Services Sign-In Assistant version 7.250.4209.0 64-bit (http://www.microsoft.com/enin/download/details.aspx?id=39267) and Microsoft Online Services Module for Windows PowerShell version 1.0.0 32-bit (http://g.microsoftonline.com/0BX10EN/230) or 64-bit (http://g.microsoftonline.com/0BX10EN/423) on the same computer where you want to install Office 365 driver. For installation instructions, see the Microsoft Online Services page.

2.2 Installing The Driver Files

The driver files are bundled in the `NIdM_Driver_4.0.2_Office365.zip` file. The zip file contains the following:

- **Driver Shim:** Contains the driver files: `DXMLMSOnlinedriver.dll`, `DXMLBase.dll`, `SQLiteInterop.dll`, and `System.Data.SQLite.dll`.

Ensure that you perform the following tasks before installing the Office 365 driver:

- Create an Office 365 user administrator account through which the driver can authenticate to Office 365 and perform administrative functions, such as creating users and groups. The driver must log in to Office 365 using an Office 365 account with administrative privileges.
- Install the Microsoft Online Services Sign-In Assistant version 7.250.4209.0 and Microsoft Online Services Module for Windows PowerShell version 1.0.0. For installation instructions, see the Microsoft Online Services page. The Microsoft Online module is installed in the default Windows PowerShell path of your Windows computer.

Run the following steps to install the driver:

1. Download and unzip the `NIdM_Driver_4.0.2_Office365.zip` file to a local folder on your system.
2. Copy the `DXMLMSOnlinedriver.dll`, `SQLiteInterop.dll`, `DXMLBase.dll`, and `System.Data.SQLite.dll` files to the `<IDM__RL_Install_Dir>\RemoteLoader.NET\` folder on your machine.
3. Download and unzip the Identity Manager 4.0.2 Engine Patch 1a from the Novell Downloads Web Site.
4. Unzip the Identity Manager 4.0.2 Engine Patch 1a or later to work with Office 365.
5. Apply the .NET Remote Loader patch using the patch installer.

2.2.1 Creating Driver Instance in the .NET Remote Loader Console

To create a driver instance in the .NET Remote Loader Console, do the following:

1. Launch the Remote Loader Console.
2. Specify the Driver description.
3. In the *Driver* field, browse to the .NET Remote Loader installation folder `<IDM__RL_Install_Dir>\RemoteLoader.NET\`,then select the `DXMLMSOnlineDriver.dll` file.
4. (Optional) Specify the SSL details.

3 Creating a New Driver Object

After you install the Office 365 driver files on the server where you want to run the driver, you can create the driver in the Identity Vault. You do so by installing the driver packages or importing the basic driver configuration file and then modifying the driver configuration to suit your environment.

The following sections provide instructions:

- Section 3.1, "Creating the Driver Object in Designer," on page 15
- Section 3.2, "Activating the Driver," on page 21

3.1 Creating the Driver Object in Designer

You create the Office 365 driver by importing the driver's packages and then modifying the configuration to suit your environment. After you have created and configured the driver, you need to start it.

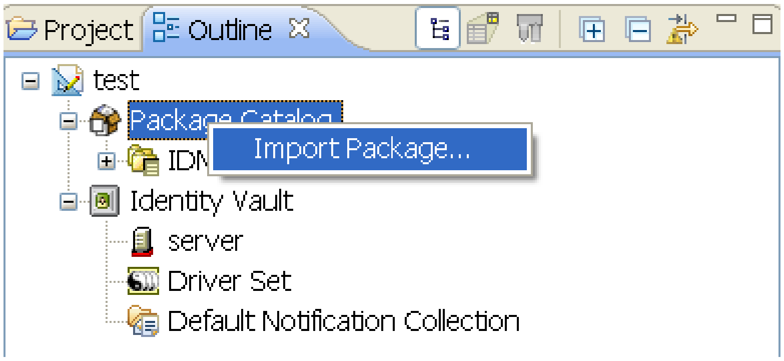
- Section 3.1.1, "Importing the Driver Packages in Designer," on page 15
- Section 3.1.2, "Installing the Driver Packages," on page 16
- Section 3.1.3, "Configuring the Driver Object," on page 19
- Section 3.1.4, "Deploying the Driver Object," on page 20
- Section 3.1.5, "Starting the Driver," on page 20

3.1.1 Importing the Driver Packages in Designer

The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package Catalog before you can create a new driver object.

To verify that you have the most recent version of the driver packages in the Package Catalog:

1. Open Designer.
2. In the toolbar, click *Help* > *Check for Package Updates*.
3. Click *OK* to update the packages or click *OK* if the packages are up-to-date.
4. In the Outline view, right-click *Package Catalog*.
5. Click *Import Package*.



6 Select any Office 365 driver packages.

or

Click *Select All* to import all of the packages displayed.

By default, only the base packages are displayed. Deselect *Show Base Packages Only* to display all packages.

7 Click *OK* to import the selected packages, then click *OK* in the successfully imported packages message.

8 After the current packages are imported, continue with Section 3.1.2, "Installing the Driver Packages," on page 16.

3.1.2 Installing the Driver Packages

1 In Designer, open your project.

2 In the Modeler, right-click the driver set where you want to create the driver, then click *New* > *Driver*.

3 Select *Office365 Base*, then click *Next*.

4 Select the optional features to install for the Office 365 driver, then click *Next*. The options are:

Office 365 Configuration: This package contains the default policies required to enable the driver to create user and group accounts. Leave this option selected.

Office 365 Driver Entitlements: This package contains configuration information and policies for synchronizing user accounts, group membership, roles and licenses. If you want account creation and auditing enabled through entitlements, verify that this option is selected. For more information, see the *Identity Manager 4.0.2 Entitlements Guide*.

Office 365 Password Synchronization: This packages contains the policies that enable the Office 365 driver to synchronize passwords. If you want to synchronize passwords, verify that this option is selected. For more information, see the *Identity Manager 4.0.2 Password Management Guide*.

Office 365 Managed System Information: This package contains the policies that enable the driver to collect data for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the *Identity Reporting Module Guide*.

Office 365 Account Tracking: This package contains the policies that enable you to track accounts for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the *Identity Reporting Module Guide*.

Office 365 Audit Entitlements: This package contains the policies that enable account creation and auditing for the Office 365 driver. If you want account creation and auditing enabled, verify that this option is selected. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the *Identity Manager 4.0.2 Entitlements Guide*.

Office 365 Optional Policies: This package contains the policies that enable the driver to handle multivalued CN (Common Name) attribute conversions between the Identity Vault and Office 365.

By default, the *Show Only Applicable Packages Versions* option is selected.

5. (Conditional) If there are package dependencies for the packages you selected to install, you must install these dependencies to install the selected package. Click *OK* to install the package dependencies listed.

6. (Conditional) The Common Settings page is only displayed if the Common Settings package is installed as a dependency. On the Install Common Settings page, fill in the following fields, then click *Next*:

   User Container: Select the Identity Vault container where Office 365 users will be added if they don't already exist in the vault. This value becomes the default for all drivers in the driver set.

   Group Container: Select the Identity Vault container where Office 365 groups will be added if they don't already exist in the vault. This value becomes the default for all drivers in the driver set.

7. On the Install Office 365 Base page, specify a name for the driver that is unique within the driver set, and then click *Next*.

8. On the new Install Office 365 Base page, fill in the following fields, then click *Next*:

   Subscriber Options: Fill in the following fields to define Office 365:

   - **Driver Name:** Specify the name for the driver.
   - **User Name:** Specify the name of the Office 365 administrator user. The driver shim requires this name to access Office 365. For example, `username@domain.onmicrosoft.com`.
   - **User Password:** Specify the password of the site administrator user. The driver shim requires this password to access Office 365.
   - **Office 365 Custom Licenses:** Click the ➕ icon to create custom Office 365 licenses by disabling specific services. You must use License Entitlements to assign licenses to the Office 365 users.
     - **Custom License Name:** Specify the name with which a custom license should be created. This will appear as `[domainname]:[license name (service to be disabled)]` in the License Entitlements. If the name you entered contains spaces or a hyphen "-", the driver cannot create a custom license.
     - **Service Name to be Disabled:** Specify the service names to be disabled. To disable more than one service, use a comma to separate the service names. For example, to disable Microsoft Exchange and Microsoft Sharepoint services from your enterprise plan, use this string: EXCHANGE_S_ENTERPRISE,SHAREPOINTENTERPRISE.

   Publisher Options: Select *True* to enable the Publisher connection. The following options are displayed to configure the Publisher channel:

   - **Working Directory:** Specify the full path of a directory on the local file system where publisher state information for the driver can be stored. The driver process must have write access to the directory.
   - **Office 365 Polling Interval:** Specify the number of seconds the Publisher channel waits after polling the Office 365 system for new changes before polling again.
   - **Database Password:** Specify the database password. This password is used to encrypt and connect to the Publisher cache. Ensure that the same password is used to reconnect to the cache at the later time.
   - **Confirm Publisher Deletes:** This means that the Publisher channel reconfirms the delete operations by polling Office 365. If the value of this option is set to *False*, the channel does not reconfirm the operations.

- **Clear Current Cached Events:** Set this option to *True* if you want to clear the current events stored in the Publisher cache.

Heart Beat Interval: Specify the number of seconds that the Publisher channel waits after running the polling script and sending Office 365 events from the change cache to the Identity Manager engine.

9 Fill in the following fields to configure the .NET Remote Loader, then click *Next*:

Host Name: Specify the hostname or IP address of the server where the .NET Remote Loader Service is installed and running for this driver.

Port: Specify the port number where the .NET Remote Loader Service is installed and is running for this driver. The default port is 8090.

KMO: Specify the Key Name of the Key Material Object (KMO) containing the keys and certificate to be used for SSL. For example, kmo=remotecert.

If you use spaces in the certificate name, you need to enclose the KMO object nickname in single quotation marks.

Remote Password: Specify the Remote Loader' password, as defined on the Remote Loader service. The Identity Manager engine (or Remote Loader shim) requires this password to authenticate to the Remote Loader.

Driver Password: Specify the driver object password that is defined on the Remote Loader service. The Remote Loader requires this password to authenticate to the Identity Manager server.

10 On the Office 365 Base page, fill in the following fields, then click *Next*:

- **Office 365 Domain Name**: Specify your Office 365 domain name, using the *Domain-name*.onmicrosoft.com format.
- **Usage Location**: Specify a two-letter country code that needs to be set in Office 365. For example, if the Office 365 service is hosted in different location and you select your country, the servers hosted in your country are used to make the service available to you.

11 (Conditional) On the Install Office 365 Account Tracking page, fill in the following fields, then click *Next*:

Realm: Specify the name of the realm, security domain, or namespace in which the account name is unique. You must set the *Realm* to the Office 365 Domain Name.

12 (Conditional) On the Install Office 365 Password Synchronization page, fill in the following fields, then click *Next*:

- **Set Password Never Expires:** If you set this option to *True* on the newly created users, the password does not expire for them.
- **Disable Force Change Password at First Login:** If *True*, disables forced password change when a user logs into Office 365 for first time.

13 (Conditional) On the Install Office 365 Managed System Information page, fill in the following fields to define the ownership of the Office 365 system, then click *Next*:

General Information

- **Name**: Specify a descriptive name for the managed system.
- **Description**: Specify a brief description of the managed system.
- **Location**: Specify the physical location of the managed system.
- **Version**: Specify the version of the managed system.

System Ownership

- **Business Owner** - Select a user object in the Identity Vault that is the business owner of the Office 365 system. This can only be a user object, not a role, group, or container.

- **Application Owner**: Select a user object in the Identity Vault that is the application owner of the Office 365 system. This can only be a user object, not a role, group, or container.

  This page is only displayed if you selected to install the Data Collection packages and the Account Tracking packages.

System Classification

- **Classification**: Select the classification of the Office 365 system. This information is displayed in the reports. The options are as follows:
  - Mission-Critical
  - Vital
  - Not-Critical
  - Other

    If you select Other, you must specify a custom classification for the Office 365 system
- Environment: Select the type of environment the Office 365 system provides. The options are as follows:
  - Development
  - Test
  - Staging
  - Production
  - Other

    If you select *Other*, you must specify a custom environment for the Office 365 system.

14 Review the summary of tasks that will be completed to create the driver, then click *Finish*.

The driver is now created. You can modify the configuration settings, by continuing with the next section, Configuring the Driver Object. If you don't need to configure the driver, continue with Deploying the Driver Object.

3.1.3 Configuring the Driver Object

Configuring the Driver Parameters: There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to review the Driver Properties located on the Driver Configuration page. The Driver Parameters and the Global Configuration Values let you configure the Office 365 login information and other parameters associated with the Publisher channel. These settings must be configured properly for the driver to start and function correctly. The driver requires an account with Office 365 that is an administrator for your Office 365 subscription. You should create a new account in your Office 365 specifically for this purpose. Make sure that this new account is set to administer your Office 365. These values are set during the default import of the driver

Customizing the Driver Policies and Filter: The driver policies and filter control data flow between the Identity Vault and the application. You should ensure that the policies and filters reflect your business needs.

Specifying Authentication Information: The Authentication information contains the Remote Loader configuration information.

If you do not have the Driver Properties page displayed in Designer, configure the driver properties:

1. Open your project.
2. In the Modeler, right-click the driver icon or the driver connection, then select Properties.
3. Make any desired changes, then click *OK* to save the changes.
4. After the driver is created in Designer, it must be deployed to the Identity Vault. Proceed to Section 3.1.4, "Deploying the Driver Object," on page 20.

After completing the configuration tasks, continue with Section 3.1.4, "Deploying the Driver Object," on page 20.

3.1.4 Deploying the Driver Object

After the driver is created in Designer, it must be deployed into the Identity Vault.

1. In Designer, open your project.
2. In the Modeler, right-click the driver icon or the driver connection, then select *Live* > *Deploy*.
3. Read through the deployment summary, then click *Deploy*.
4. Read the success message, and then click *OK*.
5. Click *Define Security Equivalence* to assign rights to the driver.

   The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights.

   5a Click *Add*, then browse to and select the object with the correct rights.

   5b Click *OK* twice.
6. Click *Exclude Administrative Roles* to exclude users that should not be synchronized.

   6a Click *Add*, then browse to and select the user object you want to exclude, then click *OK*.

   6b Repeat Step 6a for each object you want to exclude, then click *OK*.
7. Click *OK*.

3.1.5 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver by using Designer:

1. In Designer, open your project.
2. In the Modeler, right-click the driver icon or the driver line, then select *Live* > *Start Driver*.

   NOTE: The driver cannot initialize completely unless it successfully connects to the .NET Remote Loader and loads the Office 365 driver shim.

To start the driver using iManager:

1. In iManager, click to display the Identity Manager Administration page.
2. Click *Identity Manager Overview*.
3. Browse to and select the driver set object that contains the driver you want to start.

4 Click the driver set name to access the Driver Set Overview page.

5 Click the upper right corner of the driver, then click *Start driver*.

For information about performing management tasks with the driver, see Chapter 5, “Managing the Driver,” on page 25.

IMPORTANT: When you start the driver for the first time, don't add new users to the Publisher channel until the first polling interval completes because the driver treats all users as existing users and stores them in the change cache without sending them to the Identity Manager engine. It sends the new users to the Identity Manager engine from the next polling interval. Therefore, ensure that new users are added to the Publisher channel after the first polling cycle completes.

3.2 Activating the Driver

To activate the Office 365 driver, activate the Identity Manager engine, then activate the driver by using the separate Office 365 activation key. If you created the driver in a driver set that has not been activated, you must activate the Identity Manager engine and the driver within 90 days. Otherwise, the driver stops working.

If driver activation has expired, ndstrace displays the following error message:

```
DirXML Log Event -------------------
Driver: \META-RHEL6\system\DriverSet\eDirDriver-BulkOperations
Channel: Subscriber
Status: Error
Message: Code(-9075) Shutting down because DirXML engine evaluation period
has expired. Activation is required for further use.
```

To use the driver, you must reactivate it.

For information on activation, refer to “Activating Novell Identity Manager Products” in the *Identity Manager 4.0.2 Framework Installation Guide*.

4 Securing Communication

The Office 365 driver uses the Microsoft Online Services module for Windows Powershell to communicate with Office 365. The Powershell modules use the HTTPS protocol to communicate with Office 365. The connecting user is securely authenticated to Office 365 using the *Select Windows Security Groups* setting defined on the Office 365 cloud. A security certificate is used by the Microsoft Online Services cmdlets to identify the Office 365 service.

SSL is used for default communication between the .NET Remote Loader and the Identity Manager engine.

You can store the Publisher change cache in an embedded database provided by the .NET Framework. If this option is not viable, you can encrypt the change cache XML and store it in the DIB directory.

5 Managing the Driver

As you work with the Office 365 driver, there are several management tasks you might need to perform, including the following:

- Starting, stopping, and restarting the driver
- Viewing driver version information
- Using Named Passwords to securely store passwords associated with the driver
- Monitoring the driver's health status
- Backing up the driver
- Inspecting the driver's cache files
- Viewing the driver's statistics
- Using the DirXML Command Line utility to perform management tasks through scripts
- Securing the driver and its information

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *NetIQ Identity Manager 4.0.2 Common Driver Administration Guide*.

6 Troubleshooting the Driver

This section contains potential problems and error codes you might encounter while configuring or using the driver.

- Section 6.1, "Troubleshooting Driver Processes," on page 27
- Section 6.2, "Troubleshooting Office 365 Driver Issues," on page 27

6.1 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. You can use DSTrace to view the driver processing events. You should only use DSTrace during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see "Viewing Identity Manager Processes" in the *NetIQ Identity Manager 4.0.2 Common Driver Administration Guide*.

6.2 Troubleshooting Office 365 Driver Issues

- Section 6.2.1, "Deleting the Last Name attribute value of users is not synchronized to the Identity Manager," on page 27
- Section 6.2.2, "Adding a user with a long value of Display Name attribute fails on the Publisher channel," on page 28
- Section 6.2.3, "Adding a user with a long value of First Name attribute fails on the Publisher channel," on page 28
- Section 6.2.4, "The EmailAddress attribute sync triggers a loopback on the Publisher channel," on page 28
- Section 6.2.5, "Not all the synced attributes are supported by the cmdlet," on page 28
- Section 6.2.6, "Setting the set-executionPolicy to RemoteSigned in the Powershell," on page 28
- Section 6.2.7, "Changing the driver settings for allowing certain operations," on page 28

6.2.1 Deleting the Last Name attribute value of users is not synchronized to the Identity Manager

The LastName attribute of Office 365 is mapped to the Surname attribute of the Identity Vault. If the value of LastName is removed from Office 365, the Identity Vault does now allow empty field to be synchronized.

6.2.2 Adding a user with a long value of Display Name attribute fails on the Publisher channel

The Display Name attribute of Office 365 is mapped to the Full Name attribute of the Identity Vault. The Identity Vault does not allow a Full Name value with more than 64 characters. The Identity Vault sends a SYNTAX_VIOLATION exception.

6.2.3 Adding a user with a long value of First Name attribute fails on the Publisher channel

The First Name attribute of Office 365 is mapped to the Given Name attribute of the Identity Vault. The Identity Vault does not allow a Given Name value with more than 32 characters. The Identity Vault sends a SYNTAX_VIOLATION exception.

6.2.4 The EmailAddress attribute sync triggers a loopback on the Publisher channel

This occurs because only the primary e-mail address is received during Office 365 polling. The driver removes any additional e-mail addresses.

6.2.5 Not all the synced attributes are supported by the cmdlet

For some operations, traces might appear with this message:

```
Disallowed attribute Sync : <attr>.
```

It occurs for the attribute that are either irrelevant to the type of group that is being synced or unsupported by the commandlet.

6.2.6 Setting the set-executionPolicy to RemoteSigned in the Powershell

To start the Office 365 driver, change the set-executionPolicy to *RemoteSigned* in the Powershell. By default, it is set to *Restricted*. If you don't change the setting, the driver fails to start and displays the following error message:

```
Error Connecting to Office 365. File <file>.psm1 cannot be loaded because the
execution of scripts is disabled on this system.
```

6.2.7 Changing the driver settings for allowing certain operations

The Office 365 driver does not allow some of the Distribution or Security Group settings for specific groups. For example, it doesn't allow you to set *Member Depart Restriction* to *Open* for a Security Group. It doesn't allow you to set *Member Join Restriction* to *Approval Required* for some Distribution Groups.

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the Office 365 driver. These are the only unique properties for this driver. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *NetIQ Identity Manager 4.0.2 Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with an icon.

- Section A.1, "Driver Configuration," on page 29
- Section A.2, "Global Configuration Values," on page 33

A.1 Driver Configuration

In iManager:

1 Click to display the Identity Manager Administration page.

2 Open the driver set that contains the driver whose properties you want to edit:

2a In the *Administration* list, click *Identity Manager Overview*.

2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.

2c Click the driver set to open the Driver Set Overview page.

3 Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.

4 Click *Edit Properties* to display the driver's properties page.

By default, the Driver Configuration page is displayed.

In Designer:

1 Open a project in the Modeler.

2 Right-click the driver icon or line, then select click *Properties* > *Driver Configuration.*

The Driver Configuration options are divided into the following sections:

- Section A.1.1, "Driver Module," on page 30
- Section A.1.2, "Driver Object Password," on page 30
- Section A.1.3, "Authentication," on page 30
- Section A.1.4, "Startup Option," on page 31
- Section A.1.5, "Driver Parameters," on page 31

- Section A.1.6, “ECMAScript,” on page 33
- Section A.1.7, “Global Configurations,” on page 33

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Java: This option is not used with the Office 365 driver.

Native: This option is not used with the Office 365 driver.

Connect to Remote Loader: This option is always used with the Office 365 driver to connect to Office 365.

The driver .dll is: `DXMLMSOnlineDriver.dll`.

A.1.2 Driver Object Password

Driver Object Password: Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page, or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

A.1.3 Authentication

The Authentication section stores the information required to authenticate to the connected system. For the Office 365 driver, it stores the information required to authenticate to the Office 365 server with which the driver is associated.

Authentication ID: Specify the DN of the LDAP account that the driver will use to authenticate to connected Office 365 server.

Connection Context: Specify the hostname or IP address of the Office 365 server, as well as the decimal port number. For example, 187.168.1.1:389.

The driver uses SSL to secure communication with Office 365.

Remote Loader Connection Parameters: This option is always used with the Office 365 driver. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, where the hostname is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090.

The `kmo` is used because the driver uses an SSL connection between the Remote Loader and the Identity Manager engine. For example, `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`.

Driver Cache Limit (KB): Specify the maximum event cache file size (in KB). If the value is set to zero, the file size is unlimited. In Designer, click *Unlimited* to set the file size to unlimited in Designer.

Application Password: Specify the password for the user object listed in the *Authentication ID* option.

Remote Loader Password: Specify the password for the driver when it is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

A.1.4 Startup Option

The Startup Option section enables you to set the driver state when the Identity Manager server is started.

Auto start: The driver starts every time the Identity Manager server is started.

Manual: The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.

Disabled: The driver has a cache file that stores all of the events. When the driver is set to *Disabled*, this file is deleted, and no new events are stored in the file until the driver state is changed to *Manual* or *Auto Start*.

If the driver is *Disabled* and then changed to *Auto start* or *Manual*, you can select the *Do Not Automatically Synchronize the Driver* check box. This prevents the driver from synchronizing objects automatically when it loads. To synchronize objects manually, use the *Synchronize* button on the Driver Overview page.

A.1.5 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment.

The parameters are divided into the following categories:

- "Driver Settings" on page 31
- "Subscriber Settings" on page 31
- "Publisher Settings" on page 32

Driver Settings

- **User Name:** Specify the name of the Office 365 user. The driver shim requires this name to access the Office 365 site using the `username@domain.onmicrosoft.com` format.
- **User Password:** Specify the password of the Office 365 user. The driver shim requires this password to access the Office 365 site collection.

Subscriber Settings

- **Office 365 Domain Name:** Specify the Office 365 site context. For example, stidm.onmicrosoft.com (*Domain-name*.onmicrosoft.com).
- **Office 365 Custom Licenses:** Click the ✚ icon to create custom Office 365 licenses by disabling specific services. You must use the License Entitlements to assign licenses to the Office 365 users.
    - **Custom License Name:** Specify the name for the license. This will appear as `[domainname]:[license name (service to be disabled)]` in the License Entitlements.
    - **Service Name to be Disabled:** Specify the service names to be disabled. To disable more than one service, use a comma to separate the service names. For example, to disable services, such as Microsoft Exchange and Microsoft Sharepoint in your enterprise plan, use this string: EXCHANGE_S_ENTERPRISE,SHAREPOINTENTERPRISE.

- **Exchange Distribution/Security Group Configuration:** Select *Show* to enable the security group configuration. The following options are displayed to configure the Subscriber channel:
    - **Make Group Owner Member of the Group:** Select *True* to specify that the manager of the group is also a member of the distribution group.
    - **Member Join Restriction:** Specifies the restrictions on recipients who want to join the group membership. Set it to Open if no restriction applies. Set it to *Closed* if restrictions apply. Otherwise, set it to *Approval Required* if it requires approval from the moderator. This is a default configuration setting that the driver will use. To change it for a particular group, set the relevant attributes using the driver policies.
    - **Member Depart Restriction:** Specifies the restrictions on recipients who want to leave the group membership. Set it to Open if no restriction applies. Set it to *Closed* if restrictions apply. Otherwise, set it to *Approval Required* if it requires approval from the moderator. This is a default configuration setting that the driver will use. To change it for a particular group, set the relevant attributes using the driver policies.

      NOTE: The Office 365 driver does not allow some of the Distribution or Security Group settings for specific groups. For example, it doesn't allow you to set *Member Depart Restriction* to *Open* for a Security Group. It doesn't allow you to set *Member Join Restriction* to *Approval Required* for some Distribution Groups.
    - **Moderation Enabled:** Specifies whether to enable moderation for the distribution group. To ensure moderation, set it to *True*. Otherwise, set it to *False*. This is a default configuration setting that the driver will use. To change it for a particular group, set the relevant attributes using the driver policies.
    - **Bypass Nested Moderation:** Specifies whether to allow the parent group moderators to provide approval for any nested groups that are also moderated. If it is set to *True*, after a moderator approves a message sent to this distribution group, the message is automatically approved for any other moderated recipients that are members of this distribution group. The default value is *False*.
    - **Send Moderation:** Specifies whether status notifications are sent to users when they send a message to the moderated distribution group. Set it to *Always* for sending the notifications to all senders. Set it to *Internal* for sending the notifications only to the senders who are internal to the organization. The senders are always notified if their message is rejected by the moderators, regardless of the listed values for this option. The default value is *Never*, which disables all status notifications.

Publisher Settings

Enable/Disable Publisher Connection: Select *True* to enable the Publisher connection. The following options are displayed to configure the Publisher channel.

- **Working Directory:** Specify the full path to a directory on the local file system where Publisher state information for the driver can be stored. The information is stored in the SQLite database. The driver process must have write access to the directory. The default location is `C:\temp` folder on the Remote Loader server.
- **Office 365 Polling Interval:** Specifies the number of seconds that the Publisher channel waits after running the polling script and sending Office 365 events from the change cache to the Identity Manager engine.
- **Database Password:** Specify the database password. This driver shim uses this password to encrypt the database that stores the Publisher cache/state information.
- **Remove Existing Password:** Select this option to remove the existing password.

- **Confirm Publisher Deletes:** When this option is set to *True*, the Publisher channel reconfirms the delete operations by polling Office 365. If the value is set to *False*, reconfirmation is not done. By default, the value is set to *True*.
- **Clear Current Cached Events:** When this option is set to *True*, the current events stored in the Publisher cache are cleared.
- **Heartbeat Interval:** Specifies how often, in seconds, the driver shim contacts the Identity Manager engine when there has not been any traffic during the interval time. Specify 0 to disable the heartbeat.

A.1.6 ECMAScript

The ECMAScript section enables you to add ECMAScript resource files. The resources extend the driver's functionality when Identity Manager starts the driver.

A.1.7 Global Configurations

The Global Configurations section displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads when the driver is started. You can add or remove the Global Configuration objects, and you can change the order in which the objects are executed.

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The Office 365 driver includes several GCVs that are created from information supplied during importing the driver configuration file. For more information, see Chapter 3, "Creating a New Driver Object," on page 15.

The driver also includes the GCVs that are used with password synchronization. In Designer, you can click the icon next to a password synchronization GCV to edit the object. This displays the Password Synchronization Options dialog box, which displays a better view of the relationship between the different settings. In iManager, you should edit the password synchronization settings on the *Server Variables* tab rather than under the GCVs. The Server Variables page has a better view of the relationship between the different GCVs.

You can add your own GCVs if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in iManager:

1 Click to display the Identity Manager Administration page.

2 Open the driver set that contains the driver whose properties you want to edit:

   2a In the *Administration* list, click *Identity Manager Overview*.

   2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.

   2c Click the driver set to open the Driver Set Overview page.

3 Locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.

or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver's GCVs in Designer:

1. Open a project in the Modeler.
2. Right-click the driver icon or line, then select *Properties* > *Global Configuration Values.*

   or

   To add a GCV to the driver set, right-clickthe driver set icon , then click *Properties* > *GCVs*.

The driver Global Configuration Values are divided into following categories:

- Section A.2.1, "Password Synchronization," on page 34
- Section A.2.2, "Driver Configuration," on page 35
- Section A.2.3, "Entitlements," on page 35
- Section A.2.4, "Account Tracking," on page 38
- Section A.2.5, "Managed System Information," on page 38

A.2.1 Password Synchronization

The following GCVs control password synchronization for the Office 365 driver. For more information, see the *Identity Manager 4.0.2 Password Management Guide*.

Connected System or Driver Name: Specifies the name of the connected system, application or Identity Manager driver. This value is used by the e-mail notification templates to identify the source of notification messages.

Set Password Never Expires: If you set this option to *True* on the newly created users, the password does not expire for them.

Disable Force Change Password at First Login: If you set the option to *True*, it disables a forced password change when a user logs into Office 365 for first time.

Set Strong Password Required: Set this option to *True* to enforce strong password requirement for user passwords.

Application Accepts Passwords from Identity Manager: If this option is set to *True*, the driver allows passwords to flow from the Identity Manager data store to the connected Office 365 server.

Identity Manager Accepts Passwords from the Application: If this option is set to *True*, it allows passwords to flow from the connected system to Identity Manager.

Publish Passwords to NDS Password: Use the password from the connected system to set the non-reversible NDS password in the Identity Vault.

Publish Passwords to Distribution Password: Use the password from the connected system to set the NMAS Distribution Password used for Identity Manager password synchronization.

Reset user's external system password to the Identity Manager password on failure: If this option is set to *True*, and the Distribution Password fails to distribute, attempt to reset the password in the connected system by using the Distribution Password from the Identity Manager data store.

Notify the user of password synchronization failure via e-mail: If this option is set to *True*, notify the user by e-mail of any password synchronization failures.

In Designer, you must click the icon next to a GCV to edit it. This displays the Password Synchronization Options dialog box for a better view of the relationship between the different GCVs.

In iManager, you should edit the Password Management Options on the *Server Variables* tab rather than under the GCVs. The Server Variables page has a better view of the relationship between the different GCVs.

A.2.2 Driver Configuration

Use the following GCVs to control how the driver is configured:

Office 365 Domain Name: Specify the Office 365 site context suing the `admincentral.onmicrosoft.com` format.

Identities to be Synchronized: Specify if the driver should synchronize identities from Active Directory or configure the Identity Vault to act as the identity provider. If you choose to configure the Identity Vault as the identity provider, no association to any other directory is required. With Active Directory as the identity provider, you can synchronize only users that have an association with Active Directory. If you selected Active Directory, fill in the following fields, then click *Next*:

- **AD Driver**: Specify the Active Directory driver that synchronizes users to the Active Directory domain that Office 365 uses for authentication. If a driver is specified here, a valid association from that driver on the user is a required to synchronize users to Office 365. The new users will synchronize to Active Directory before synchronizing to Office 365.
- **AD Domain Name**: Specify the Active Directory domain name of the domain used to authenticate users to Office 365 portal.

Usage Location: Specify a two-letter country code that needs to be set in Office 365. For example, if the Office 365 service is hosted in different location and you select your country, the servers hosted in your country are used to make the service available to you.

A.2.3 Entitlements

There are multiple sections in the *Entitlements* tab. Depending on which packages you installed, different options are enabled or displayed.

- "Entitlements Configuration" on page 35
- "Data Collection" on page 36
- "Role Mapping" on page 37
- "Resource Mapping" on page 37
- "Entitlement Extensions" on page 37

Entitlements Configuration

For more information about entitlements, see Section 1.3.5, "Entitlements," on page 10.

Use User Account Entitlement: Select *True* to enable the driver to manage user accounts based on the driver's defined entitlements. Select *Fals*e to disable management of user accounts based on the entitlements.

Enable Login Disabled Attribute Sync: Select *True* if the changes made to the LoginDisabled attribute in the Identity Vault should be synchronized even if the User Account entitlement (Account) is enabled.

When Account Entitlement Revoked: Select the action to take when a user account entitlement is revoked. The options are *Disable Account or Delete Account*. By default, *Disable Account* is selected.

Parameter Format: Specify the parameter format the entitlement agent must use. Under the *Identity Manager 4* option, the entitlement parameters are parsed as a JSON string arranged in a `"name":"value"` format.

Use Group Entitlement: Select *True* to enable the driver to manage group membership based on the driver's defined entitlements.

Parameter Format: Select the parameter format the entitlement agent must use. The options are *Identity Manager 4* or *Legacy*. Under the *Identity Manager 4* option, the entitlement parameters are parsed as a JSON string arranged in a `"name":"value"` format.

Select *False* to disable management of group membership based on entitlements.

Use License Entitlement: Select *True* to enable the driver to manage user licenses based on the driver's defined entitlements.

Parameter Format: Select the parameter format the entitlement agent must use. The options are *Identity Manager 4* or *Legacy*. Under the *Identity Manager 4* option, the entitlement parameters are parsed as a JSON string arranged in a `"name":"value"` format.

Select *False* to disable management of license assignments based on the entitlements.

Use Roles Entitlement: Select *True* to enable the driver to manage user roles based on the driver's defined entitlements.

Parameter Format: Select the parameter format the entitlement agent must use. The options are *Identity Manager 4* or *Legacy*. Under the *Identity Manager 4* option, the entitlement parameters are parsed as a JSON string arranged in a `"name":"value"` format.

Select *False* to disable management of role assignments for users based on the entitlements.

Advanced Settings: Select show to display the entitlement options that allow or deny additional functionality like data collection and others. These settings should rarely be changed.

Data Collection

Data collection enables the Identity Report Module to gather information to generate reports. For more information, see the *Identity Reporting Module Guide*.

Enable data collection: Select *Yes* to enable data collection for the driver through the Data Collection Service by the Managed System Gateway driver. If you are not going to run reports on data collected by this driver, select *No*.

Allow data collection from user accounts: Select *Yes* to allow data collection by the Data Collection Service for the user accounts.

Allow data collection from groups: Select *Yes* to allow data collection by the Data Collection Service for groups.

Allow data collection from licenses: Select *Yes* to allow data collection by the Data Collection Service for licenses.

Allow data collection from roles: Select *Yes* to allow data collection by the Data Collection Service for roles.

Role Mapping

The Role Mapping Administrator allows you to map business roles with IT roles. For more information, see the *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide*.

Enable role mapping: Select *Yes* to make this driver visible to the Role Mapping Administrator.

Allow mapping of user accounts: Select *Yes* if you want to allow mapping of user accounts in the Role Mapping Administrator. An account is required before a role, profile, or license can be granted through the Role Mapping Administrator.

Allow mapping of groups: Select *Yes* if you want to allow mapping of groups in the Role Mapping Administrator.

Allow mapping of licenses: Select *Yes* if you want to allow mapping of licenses in the Role Mapping Administrator.

Allow mapping of roles: Select *Yes* if you want to allow mapping of roles in the Role Mapping Administrator.

Resource Mapping

The Roles Based Provisioning Module allows you to map resources to users. For more information, see the *User Application: User Guide*.

Enables resource mapping: Select *Yes* to make this driver visible to the Roles Based Provisioning Module.

Allow mapping of user accounts: Select Yes if you want to allow mapping of user accounts in the Roles Based Provisioning Module. An account is required before a role, profile, or license can be granted.

Allow mapping of groups: Select *Yes* if you want to allow mapping of groups in the Roles Based Provisioning Module.

Allow mapping of licenses: Select *Yes* if you want to allow mapping of licenses in the Roles Based Provisioning Module.

Allow mapping of roles: Select *Yes* if you want to allow mapping of roles in the Roles Based Provisioning Module.

Entitlement Extensions

User account extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

Group extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

License extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

Role extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

A.2.4 Account Tracking

Account tracking is part of the Identity Reporting Module. For more information, see the *Identity Reporting Module Guide*.

Enable account tracking: Set this to *True* to enable account tracking policies. Set it to *False* if you do not want to execute account tracking policies.

Realm: Specify the name of the realm, security domain, or namespace in which the account name is unique. You must set the *Realm* to the Office 365 Domain Name.

A.2.5 Managed System Information

These settings help the Identity Reporting Module function to generate reports. There are different sections in the *Managed System Information* tab.

- "General Information" on page 38
- "System Ownership" on page 38
- "System Classification" on page 38
- "Connection and Miscellaneous Information" on page 39

General Information

Name: Specify a descriptive name for the managed system.

Description: Specify a brief description of the managed system.

Location: Specify the physical location of the managed system.

Vendor: Specify Microsoft as the vendor of the managed system.

Version: Specify the version of the managed system.

System Ownership

Business Owner: Browse to and select the business owner in the Identity Vault for the connected application. You must select a user object, not a role, group, or container.

Application Owner: Browse to and select the application owner in the Identity Vault for the connected application. You must select a user object, not a role, group, or container.

System Classification

Classification: Select the classification of the connected application. This information is displayed in the reports. The options are:

- Mission-Critical
- Vital
- Not-Critical
- Other

  If you select *Other*, you must specify a custom classification for the connected application.

Environment: Select the type of environment the connected application provides. The options are:

- Development
- Test
- Staging
- Production
- Other

  If you select *Other*, you must specify a custom classification for the connected application.

Connection and Miscellaneous Information

Connection and miscellaneous information: This set of options is always set to *hide*, so that you don't make changes to these options. These options are system options that are necessary for reporting to work.

B Schema Mapping

The Schema Mapping policy is referenced by the driver object and applies to both the Subscriber and the Publisher channel. The purpose of the Schema Mapping policy is to map schema names (particularly attribute names and class names) between the Identity Vault and Office 365. Any modification or removal of existing entries in the Schema Mapping policy could destroy the default configuration and policies processing behavior.

Adding new attribute mappings is discretionary. Table B-1 lists Identity Vault user and group attributes that are mapped to Office 365 user and group attributes.

Table B-1 *Mapped User Attributes*

Identity Vault	Office 365
User	**MSolUser**
city	City
CN	UserPrincipalName
Facsimile Telephone Number	Fax
Full Name	DisplayName
homePhone	Office
S	State
Given Name	FirstName
GUID	ImmutableId
Internet EMail Address	AlternateEmailAddresses
L	Country
Login Disabled	BlockCredential
mobile	MobilePhone
Password Allow Change	ForceChangePassword
Postal Address	StreetAddress
Postal Code	PostalCode
nspmDistributionPassword	Password
OU	Department
Owner	ManagedBy
Member	Member

Identity Vault	Office 365
Surname	LastName
Telephone Number	PhoneNumber
Title	Title
workforceID	Office
Group	**MSolGroup**
businessCategory	Group Type
CN	DisplayName
Description	Description
EMail Address	EMailAddress
	NOTE: The events loopback into the Publisher channel if the EMail Address attribute is synchronized for distribution and security groups because the driver considers only the primary EMail address and removes any additional Email addresses in the subsequent poll cycles.
Member	Member
Owner	ManagedBy