NetIQ® Identity Manager™
Driver for Office 365 Implementation Guide

February 2017

NetIQ.

Legal Notices

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

About this Book and the Library

The *Identity Manager Driver for Office 365 Implementation Guide* explains how to install and configure the Identity Manager Driver for Office 365.

Intended Audience

This book provides information for individuals responsible for using the Identity Manager Driver for Office 365.

Other Information in the Library

The library provides the following information resources:

Identity Manager Setup Guide

Provides overview of Identity Manager and its components. This book also provides detailed planning and installation information for Identity Manager.

Designer Administration Guide

Provides information about designing, testing, documenting, and deploying Identity Manager solutions in a highly productive environment.

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

User Application: User Guide

Describes the user interface of the Identity Manager User Application and how you can use the features it offers, including identity self-service, the Work Dashboard, role and resource management, and compliance management.

User Application: Design Guide

Describes how to use the Designer to create User Application components, including how to work with the Provisioning view, the directory abstraction layer editor, the provisioning request definition editor, the provisioning team editor, and the role catalog.

Identity Reporting Module Guide

Describes the Identity Reporting Module for Identity Manager and how you can use the features it offers, including the Reporting Module user interface and custom report definitions, as well as providing installation instructions.

Analyzer Administration Guide

Describes how to administer Analyzer for Identity Manager.

Identity Manager Common Driver Administration Guide

Provides information about administration tasks that are common to all Identity Manager drivers.

Identity Manager Driver Guides

Provides implementation information about Identity Manager drivers.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Understanding the Office 365 Driver

The Office 365 driver offers automatic provisioning and synchronization of users to cloud applications. The driver 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: Although NetIQ remains committed to support Office 365 driver for critical issues, we recommend you to migrate to the new Azure AD Driver. The Azure AD Driver is the intended replacement for the Office 365 driver providing the same and additional functionality through an improved design that is more efficient and easier to configure. For more information, see Understanding How the Driver Works section of the NetIQ Office 365 and Azure Active Directory Driver Implementation Guide. In addition, the Azure AD driver provides a mechanism to migrate from the Office 365 driver. To plan your migration, see the Transitioning from Existing Office 365 Driver to New Azure AD Driver section of the NetIQ Office 365 and Azure Active Directory Driver Implementation Guide.

1.1 Key Features

The Office 365 driver supports the following features:

 * Supports provisioning users, group membership, roles, and licenses from the Identity Vault. Microsoft Active Directory is not mandatory for provisioning Office 365 users. Also, Active Directory Federation Service is not required.
 * Supports provisioning of MsolUsers and Exchange Online Mailboxes.
 * Creates and manages MsolGroups, Exchange Distribution Lists, and Mail-enabled security groups.
 * Creates user accounts based on policies and entitlements.
 * Creates and assigns custom licenses to enable or disable specific services of Office 365.
 * Provides additional support for provisioning Active Directory users to Office 365.
 * Provides support for executing PowerShell Cmdlets.
 * Provides support for Exchange Online Hybrid mode.
 * Synchronizes **EmailAddresses** and other Exchange Online attributes.

IMPORTANT: To synchronize identities, you can either select the default (Identity Vault) or Active Directory while configuring the Office 365 driver. If you choose to configure 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

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.

The Publisher channel controls data transfer as follows:

- The channel monitors the connected system for new objects and changes to the existing objects.
- The channel publishes the relevant changes to the driver shim to be synchronized with the Identity Vault.

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 maintains a database cache to prevent loopback of events on the Publisher channel and to identify changes in Office 365. The Publisher channel periodically polls the Office 365 for additions and modifications for users and groups.

The changes returned by the driver are based on Sync Filter settings configured for the driver. By default, the Publisher channel checks the database cache every five minutes. Database cache can be encrypted by specifying the Database Password in the Driver Properties.

Each user entry returned by the query to Office 365 is compared with the user data in the Publisher database cache. 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 Synchronizing Passwords

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 Synchronizing Users and Groups

The Office 365 driver synchronizes users and groups as MsolUser and MsolGroup. A MsolUser is a collection of exchange mailbox, mail user, and Azure attributes. A MsolGroup represent groups created on Azure Active Directory, Exchange Online Distribution Groups, and Mail-Enabled Security Groups.

You can deploy the Office 365 driver in an ADFS or non-ADFS environment. In a non-ADFS environment, the driver uses exchange online cmdlets, `create-mailbox` and `create-mailuser`, to create mailbox users and mail users.

For a federated environment (ADFS), perform the following actions:

1 Add MsolUserType to the Publisher filter and set it to **Notify** or **Sync**.

2 Create a MsolUser user and assign an Office 365 Exchange based license to the user.

  The Publisher channel modify event changes the MsolUserType from **User** to **UserMailbox**.

3 Perform the required exchange operation on **UserMailbox**.

NOTE: The Publisher channel receives the modify event only after a couple of poll cycles depending on the time taken by the Office 365 portal to provision the mailbox.

1.3.4 Synchronizing Exchange Online Mailbox and Mail Users

Exchange Online is the hosted version of Microsoft's messaging and Exchange platform. With Office 365 driver, you can create and manage Exchange Online user mailboxes and mail users. The driver uses the MsolUserType attribute of the Office 365 schema to synchronize Exchange-based user attributes.

- If the MsolUserType contains **UserMailbox**, the driver creates an Exchange Mailbox User.
- If the MsolUserType contains **MailUser**, the driver creates an Exchange Mail User.

By default, the driver creates a MsolUser if the MSolUSerType attribute is not specified.

The driver also supports synchronizing of several exchange online based attributes for the user, such as *MicrosoftOnlineServicesID*, *EmailAddresses*, *Manager*, and *Custom* attributes.

By default, the *AlternateEmailAddresses* attribute of the Office 365 driver is mapped with the *Internet EMail Address* attribute in the Identity Vault. After configuring the driver, you can update this default Office 365 attribute to **EmailAddresses** in the schema mapping. The filter options for the **EmailAddresses** attribute on both the Publisher and Subscriber channels are set to **Synchronize** by default. When you define the **EmailAddresses** attribute, you can control the protocol of the email address by prefixing the protocol name with the email address. Otherwise, the drives uses the default `smtp` protocol.

For example, *smtp:thomas.wagnor@example.com* creates a secondary email address. The same email address with `SMTP` creates a primary email address *as SMTP:thomas.wagnor@example.com*. Another example of an email address using `SIP` protocol is *SIP:thomas.wagnor@example.com*.

IMPORTANT

- If the EmailAddresses attribute filter options are set to **Ignore**, **Notify**, or **Reset**, the driver overwrites the primary SMTP address in the Identity Vault during a merge operation.
- The driver synchronizes the email address along with the prefixes on the Publisher channel. To synchronize the email text only without prefix, write specific policies that suits your deployment scenario.

The attributes are case-sensitive. Ensure that you add them during the XDS Add event.

1.3.5 Synchronizing Exchange Online Distribution Groups and Mail-Enabled Security Groups

To create and manage Distribution and Mail-enabled Security Groups, the driver uses multiple exchange-based group attributes. You must use the GroupType attribute in the Office 365 schema to synchronize the desired groups.

- If the GroupType contains *DistributionList*, the driver creates an Exchange Distribution List.
- If the GroupType contains *MailEnabledSecurity*, the driver creates an Exchange Security Group.
- If the GroupType contains *Security*, the driver 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. To synchronize on the Subscriber channel, use an appropriate local variable value for the GroupType attribute in the XDS document.

Identity Manager grants memberships to the groups via entitlements.

NOTE: The attributes are case sensitive. Ensure that you add them during the XDS Add event.

1.3.6 Supporting Exchange Online in Hybrid Mode

In a hybrid mode, Office 365 provides seamless integration between an On-Premises Exchange Server organization and Exchange Online in Microsoft Office 365. The Office 365 driver now supports hybrid deployment by allowing Publisher synchronization of Exchange Online attributes to an On-Premise Active Directory. The driver reads the Exchange Online attributes and publishes them to the

Identity Vault. You can then synchronize them with On-Premise Active Directory by using the NetIQ Identity Manager Active Directory driver. Refer to Table B-3 to understand the synced attributes used in an Exchange hybrid deployment scenario.

Below is a sample query to retrieve all the attributes required for exchange hybrid mode synchronization using the PowerShell cmdlet:

```
<nds dtdversion="4.0" ndsversion="8.x">
  <source>
    <product edition="Advanced" version="4.0.2.0">DirXML</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <query class-name="MSolUser" event-id="0" scope="subtree">
        <search-class class-name="Powershell"/>
        <search-attr attr-name="psexecute">
                <value>get-mailbox -Identity MyUserName</value>
        </search-attr>
        <read-attr attr-name="LegacyExchangeDN"/>
        <read-attr attr-name="ArchiveStatus"/>
        <read-attr attr-name="LitigationHoldEnabled"/>
        <read-attr attr-name="UMEnabled"/>
    </query>
  </input>
</nds>
```

Below is a sample query to retrieve all the attributes required for exchange hybrid mode synchronization:

```
<nds dtdversion="4.0" ndsversion="8.x">
  <source>
    <product edition="Advanced" version="4.0.2.0">DirXML</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <query class-name="MSolUser" event-id="0" scope="entry">
        <association>6ddfed09-441c-4a7a-ba04-62dffca8a5a3</association>
        <search-class class-name="MSolUser"/>
        <read-attr attr-name="LegacyExchangeDN"/>
        <read-attr attr-name="ArchiveStatus"/>
        <read-attr attr-name="LitigationHoldEnabled"/>
        <read-attr attr-name="UMEnabled"/>
    </query>
  </input>
</nds>
```

1.3.7   Creating PowerShell Cmdlets Parameters from Filter

The Office 365 driver generates cmdlets parameters based on the filter configuration. Although an attribute is not present in the driver schema, you can add it as part of XDS operation for the driver to execute it.

1.3.8 Supporting 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 *NetIQ Identity Manager 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.

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 prerequisites mentioned in Section 2.1, "Prerequisites," on page 17.
- Install the driver shim. For more information, see Chapter 2, "Installing the Driver Files," on page 17.
- Review the default Publisher channel configuration with the driver. For more information, see Chapter 5, "What's New?," on page 33.
- Create and configure the driver object. For more information, see Chapter 4, "Creating a New Driver Object," on page 25.

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 "Planning Overview" in the *NetIQ Identity Manager Setup 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

- NetIQ Identity Manager 4.5.1 or later

  For more information, see the *Identity Manager 4.5 Setup Guide*. For information about Identity Manager 4.6, see the *NetIQ Identity Manager 4.6 Setup Guide*.

  NOTE: Identity Manager 4.5.1 includes .NET Remote Loader required for the Office 365 driver to run.

- Microsoft Windows Server 2016 (64-bit), Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, or Microsoft Windows Server 2008 R2 (64-bit)

  The Office 365 driver supports .NET Remote Loader running on these Windows platforms.

- Microsoft Windows Management Framework 4.0 or later. Perform the following steps to verify the version of Windows Management Framework:

  1. Log in to the PowerShell module.
  2. Execute the following command:

     ```
     $PSVersionTable
     ```
  3. Check the **PSVersion value**.

  NOTE: This is required to be installed on Microsoft Windows Server 2008 R2 (64-bit). The Microsoft Windows Management Framework 4.0 installs Microsoft Windows PowerShell Version 4.0.

- Microsoft .NET Framework Version 4.5 or later. To verify the version of .NET Framework that is installed on your server, see the Microsoft documentation page.

  NOTE: This is required to be additionally installed on Microsoft Windows Server 2008 R2 (64-bit). This is automatically installed on Microsoft Windows Server 2012 and Microsoft Windows Server 2012 R2.

- Microsoft Visual C++ 2012 Redistributable packages

  For installing instructions, visit the Microsoft download page.

- Microsoft Online Services Sign-In Assistant version 7.250.4556.0 and above and Windows Azure Active Directory Module for Windows PowerShell on the same computer where you want to install Office 365 driver.

Perform the following steps to verify the versions of **Microsoft Online Services Sign-In Assistant** and **Microsoft Azure Active Directory Module for Windows Powershell**:

1. Open Control Panel.
2. Click **Programs**.
3. Click **Programs and Features**.
4. From the program list, check the versions of **Microsoft Online Services Sign-In Assistant** and **Microsoft Azure Active Directory Module for Windows Powershell**.

- If you are running the Office 365 driver in service mode, ensure that you disable the **Interactive Services Detection** service:

    1. Open Control Panel.
    2. Click **System Security** > **Administrative Tools**.
    3. Double-click **Services**.
    4. From the services list, search for **Interactive Services Detection**.
    5. Right-click **Interactive Services Detection** and then click **Properties**.
    6. Stop the service.
    7. Select **Disabled** in the **Startup Type** field and then click **OK**.

The following are the minimum system requirements for a computer running Office 365 or a Web Application server:

- CPU: Dual core 1.6 GHz or higher
- Memory: 2 GB or higher

Table 2-1 *Hardware requirements*

Hardware Requirements
For objects lesser than 10,000

♦ CPU - 1.6 GHz
    ♦ Memory - 4 GB
    ♦ Hard drive - 70 GB

For objects between 10,000 - 50,000

♦ CPU - 1.6 GHz
    ♦ Memory - 8 GB
    ♦ Hard drive - 70 GB

For objects between 50,000 - 100,000

♦ CPU - 1.6 GHz
    ♦ Memory - 16 GB
    ♦ Hard drive - 100 GB

For objects between 100,000 - 300,000

♦ CPU - 1.6 GHz
    ♦ Memory - 32 GB
    ♦ Hard drive - 300 GB

Hardware Requirements

For objects between 300,000 - 600,000

- ◆ CPU - 1.6 GHz
- ◆ Memory - 32 GB
- ◆ Hard drive - 450 GB

For objects more than 600,000

- ◆ CPU - 1.6 GHz
- ◆ Memory - 32 GB
- ◆ Hard drive - 500 GB

2.2 Installing the Office 365 Driver

- ◆ Section 2.2.1, "Installing the Driver Shim," on page 19
- ◆ Section 2.2.2, "Configuring the Office 365 Driver," on page 20

2.2.1 Installing the Driver Shim

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 requirements as in the prerequisites.

  The Microsoft Online module is installed in the default Windows PowerShell path of your Windows computer.

  By default, Microsoft Online Services Sign-In Assistant is installed in the path `C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSOnline`.

  and Microsoft Online Services Module in `C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSOnlineExtended`.

  For the driver to start successfully, ensure that you copy all the `dll` files from these two default Windows PowerShell paths to the driver installation folder.

To create and configure the driver, install the driver files from the installation directory of the `msonlinedriverfp.zip` file.

To install the driver, perform the following steps:

1 Before starting the installation, stop the .NET Remote Loader service.

2 Unzip the `msonlinedriverfp.zip` file to the driver installation folder.

3 From the unzipped file, copy the `DXMLMSOnlineDriver.dll`, `SQLite.Interop.dll`, and `System.Data.SQLite.dll` files to the .NET Remote Loader installation folder.

4 Download the driver packages from the Package Update channel.

5 For creating a driver, see Chapter 4, "Creating a New Driver Object," on page 25.

2.2.2 Configuring the Office 365 Driver

Use the .NET Remote Loader graphical interface to configure the Office 365 driver:

1 Browse to the installation directory of the .NET Remote Loader and run `rlconsole.exe` to open the GUI console. The .NET Remote Loader GUI is similar to the traditional Remote Loader GUI.

2 Click **Add**, then specify the **Description**, **Driver** (`DXMLMSOnlineDriver.dll`) and other parameters in the page that displays.

3 To configure the Office 365 driver as an application, deselect the **Establish a Remote Loader service for this driver instance**.

   You can configure the Office 365 driver as an application or as a service.

4 Click **OK**. A prompt displays asking you if you want to start the Remote Loader. You can start the driver now or later.

   When the driver is started as an application, a trace window opens. It doesn't open if the driver is started as a service.

3 Upgrading an Existing Driver

The following sections provide information to help you upgrade an existing driver:

3.1 Supported Upgrade Paths

If you are running a 4.0.2 Office 365 driver, do the following:

1. Upgrade the Identity Manager engine to 4.5 or later version to include the updates for .NET Remote Loader.

2. Upgrade Identity Manager 4.5 engine to 4.5.1 or latest. This version includes software updates for .NET Remote Loader necessary for the Office 365 4.1 driver.

If you are running a 4.0.2 Office 365 driver, you need to first upgrade the Remote Loader engine to Identity Manager 4.5 or later version and then to Remote Loader engine version 4.5.1 or latest service pack.

3.2 Upgrading a 4.1.0.x Driver to 4.1.x Version

1 Stop the driver instance from the .NET Remote Loader console.

2 Stop the driver by using iManager or Designer.

3 Download the Windows Azure Active Directory Module for Windows PowerShell version 1.1.166 from this page.

   3a Download the `AdministrationConfig-V1.1.166.0-GA.msi` file.

   3b Install the `AdministrationConfig-V1.1.166.0-GA.msi` file.

4 Delete the following `.dlls` that you would have previously copied from `MsOnline` and `MSOnlineExtended` folders:

- `Microsoft.Azure.ActiveDirectory.Client.Framework.dll`
- `Microsoft.Online.Administration.Automation.PSModule.dll`
- `Microsoft.Online.Administration.Automation.PSModule.Resources.dll`
- `Microsoft.Online.Administration.Automation.PSModule.Resources.resources.dll`
- `Microsoft.Online.Identity.Federation.PowerShell.dll`
- `Microsoft.Online.Identity.Federation.PowerShell.Strings.dll`

5 Copy the following `.dlls` from the `C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSonline` folder to the `.NET Remote Loader` folder:

- `Microsoft.Azure.ActiveDirectory.Client.Framework.dll`
- `Microsoft.Online.Administration.Automation.PSModule.dll`

- ◆ `Microsoft.Online.Administration.Automation.PSModule.Resources.dll`
   - ◆ `System.IdentityModel.Tokens.Jwt.dll`

6 To check if the MSonline modules are correctly installed, perform the following steps:

   6a Open Windows PowerShell module.

   6b Execute the `Import-Module msonline` command.

   The above command should execute without any error.

7 Unzip the `IDM451_O365_41x.zip` file to the driver installation folder.

8 From the unzipped file, copy the `DXMLMSOnlineDriver.dll`, `SQLite.Interop.dll`, and `System.Data.SQLite.dll` files to the .NET Remote Loader installation folder.

9 Start the .NET Remote Loader instance.

10 Start the driver.

3.3 Upgrading a 4.0.x Driver to 4.1.x Version

1 Stop the driver instance from the .NET Remote Loader console.

2 Stop the driver by using iManager or Designer.

3 (Conditional) Download and install the latest .NET Framework 4.5.2.

This is only required for Microsoft Windows Server 2008 R2 (64-bit).

4 (Conditional) Install the Windows Management Framework 4.0.

Microsoft Windows Management Framework 4.0 installs Microsoft Windows PowerShell Version 4.0.

This is only required for Microsoft Windows Server 2008 R2 (64-bit).

5 Download and install the latest Visual C++ Redistributables Visual Studio 2012.

6 Remove the existing Microsoft Online Services Module for Windows PowerShell.

7 Remove the existing Microsoft Online Service Sign-in Assistant.

8 On the user prompt, restart the server for the changes to take effect.

9 Download the Windows Azure Active Directory Module for Windows PowerShell version 1.1.166 from this page.

   9a Download the `AdministrationConfig-V1.1.166.0-GA.msi` file.

   9b Install the `AdministrationConfig-V1.1.166.0-GA.msi` file.

10 Apply Identity Manager 4.5 Service Pack 1 or later. For more information about what each service pack provides, see the Release Notes accompanying the release from the Identity Manager documentation page. For installation instructions, see Installing the Engine, Drivers, and iManager Plug-ins in the NetIQ Identity Manager Setup Guide.

11 Delete the following `.dlls` that you would have previously copied from `MsOnline` and `MSOnlineExtended` folders:

   - ◆ `Microsoft.Azure.ActiveDirectory.Client.Framework.dll`
   - ◆ `Microsoft.Online.Administration.Automation.PSModule.dll`
   - ◆ `Microsoft.Online.Administration.Automation.PSModule.Resources.dll`
   - ◆ `Microsoft.Online.Administration.Automation.PSModule.Resources.resources.dll`
   - ◆ `Microsoft.Online.Identity.Federation.PowerShell.dll`
   - ◆ `Microsoft.Online.Identity.Federation.PowerShell.Strings.dll`

12 Copy the following `.dlls` from the
`C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSonline` folder to the `.NET Remote Loader` folder:

- `Microsoft.Azure.ActiveDirectory.Client.Framework.dll`
- `Microsoft.Online.Administration.Automation.PSModule.dll`
- `Microsoft.Online.Administration.Automation.PSModule.Resources.dll`
- `System.IdentityModel.Tokens.Jwt.dll`

13 To check if the MSonline modules are correctly installed, perform the following steps:

13a Open Windows PowerShell module.

13b Execute the `Import-Module msonline` command.

The above command should execute without any error.

14 (Conditional) Remove the Publisher cache from your computer. By default, the change cache is located in the `C:\Temp` folder on the Remote Loader server.

15 Delete the **DirXML-ApplicationSchema** attribute for the Office 365 driver by using iManager.

16 Unzip the `IDM451_O365_41x.zip` file to the driver installation folder.

17 From the unzipped file, copy the `DXMLMSOnlineDriver.dll`, `SQLite.Interop.dll`, and `System.Data.SQLite.dll` files to the .NET Remote Loader installation folder.

18 Start the .NET Remote Loader instance.

19 Start the driver.

4 Creating a New Driver Object

You install the Office 365 driver files on the server where you want to run the driver, and then proceed to create the driver in the Identity Vault. You create the Office 365 driver 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:

4.1 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.

4.1.1 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 should use 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**.
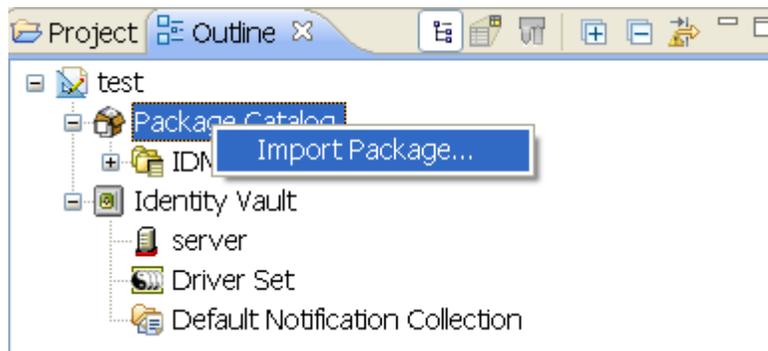
6 Select any Office 365 driver packages.

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 .

4.1.2   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 *NetIQ Identity Manager 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 *Administrator Guide to NetIQ Identity Reporting*.

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 *Administrator Guide to NetIQ Identity Reporting*.

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 *Administrator Guide to NetIQ Identity Reporting*.

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 *NetIQ Identity Manager 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** 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 Office 365 ProPlus and Lync Online services from your enterprise plan, use this string: OFFICESUBSCRIPTION,MCOSTANDARD.

    NOTE: For adding licenses, run the `Get-MSolAccountSku` run PowerShell command. To set up exclusions, go to **Driver Configuration > Subscriber Options** and add a custom license. The name of the license will be similar to `NoSharepointNoOffice` with a value of `SHAREPOINTWAC_EDU,SHAREPOINTSTANDARD_EDU`. When the driver connects to the Remote Loader and the PowerShell session starts, the driver shim reads all licenses from Office 365 and creates a custom license for each of the Subscriber option licenses. For example, if you have four different licenses installed in Office 365

and one custom license configured in the driver, the driver returns eight licenses when you query for the License entitlement in the User Application, which includes four Office 365 licenses and additional four custom licenses.

Publisher Options: Select **Show** to display the Publisher options. 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 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.

4.1.3 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.

After completing the configuration tasks, continue with Section 4.1.4, "Deploying the Driver Object," on page 30.

4.1.4 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**.

4.1.5 Starting the Driver

After you create the driver, you should start the driver in order to start the processing of the events. 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 7, "Managing the Driver," on page 37.

> **IMPORTANT:** When you start the driver for the first time, all users existing in Office 365 portal are assumed to be the initial state of the portal. The driver reports the new user additions only after the first poll completes.

4.2 Activating the Driver

The Identity Manager driver for Office 365 is part of the Identity Manager Integration Module for Microsoft Enterprise. This integration module includes the following drivers:

- NetIQ Identity Manager Driver for Multi-Domain Active Directory
- NetIQ Identity Manager Driver for SharePoint
- NetIQ Identity Manager Driver for Office 365

This integration module requires a separate activation. After purchasing the integration module, you will receive activation details in your NetIQ Customer Center.

If you create a new Office 365 driver in a driver set that already includes an activated driver from this integration module, the new driver inherits the activation from the driver set.

If you create the driver in a driver set that has not been previously activated with this integration module, the driver will run in the evaluation mode for 90 days. You must activate the driver with this integration module during the evaluation period; otherwise, the driver will be disabled.

If driver activation has expired, `ndstrace` displays an error message indicating that you need to reactivate the driver to use it. For information on activation, refer to Activating Identity Manager in the *NetIQ Identity Manager Setup Guide*.

5 What's New?

5.1 What's New in Version 4.1.2.0?

This version of the driver does not provide any new features.

5.2 What's New in Version 4.1.1.0?

This version of the driver provides support for Windows Server 2016 (64-bit).

5.3 What's New in Version 4.1.0.2?

This version of the driver provides the following key feature:

- The Publisher setting is configurable.

  You can turn the Publisher channel on or off as required.

5.4 What has Changed in the Previous Versions?

The Publisher settings underwent some changes with the recent driver releases. The following table lists the changes corresponding to each driver release and the driver package version that contains these changes.

Driver Version	Publisher Channel Behavior	Driver Base Package Version
4.1.2.0	No new features added	NOVLOFFIBASE_2.9.0.20170622162314
4.1.0.1	Publisher channel is always enabled. The Subscriber channel is not required to wait for the cache to build up.	NOVLOFFIBASE_2.6.0.20150410181838
4.1.0.0	Publisher channel is always enabled. The Subscriber channel must wait for the Publisher channel cache to build up.	NOVLOFFIBASE_2.6.0.20150410181838
Versions prior to 4.1.0.0	Publisher channel is configurable. You can turn it on or off as required.	NOVLOFFIBASE_2.5.0.20140930161237

Certain features of the driver requires you to configure the Publisher channel as described in the following table. To use these features, configure the Publisher channel appropriately.

Features	Publisher Requirement
Only Subscriber synchronization	OFF
On Active Directory Federation Services (ADFS) deployments	ON
Exchange hybrid deployment	ON
Publisher synchronization for Exchange and Office 365	ON

6 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.

You can encrypt the change cache. The driver stores the Publisher cache in the SQL database supported by the .NET framework. To encrypt the change cache, set the database password on the Driver Parameters. For more information, see Section A.1.5, "Driver Parameters," on page 51.

7 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 Driver Administration Guide*.

8 Configuring PowerShell Support

Identity Manager provides support for managing Active Directory and Microsoft Exchange Online by using Windows PowerShell cmdlets.

 ◆ Section 8.1, "Overview of PowerShell Functionality," on page 39
 ◆ Section 8.2, "Implementing PowerShell Cmdlets in the Office 365 Driver," on page 39

8.1 Overview of PowerShell Functionality

PowerShell is a shell-based automation framework created by Microsoft that allows users to manage the internal functions of other Microsoft products, including Microsoft Online Services and Exchange Online. PowerShell uses special .NET classes called cmdlets to perform various processing actions on objects in your Active Directory or Exchange Online environments. Identity Manager can use PowerShell cmdlets to perform additional event processing by sending cmdlets to the Office 356 driver using one or more policies.

NOTE: Only policies from the Subscriber channel can run PowerShell cmdlets.

For more information about PowerShell, see the following resources:

 ◆ "Getting Started with Windows PowerShell" (http://technet.microsoft.com/en-us/library/aa973757%28VS.85%29.aspx)
 ◆ "Windows PowerShell Owner's Manual" (http://technet.microsoft.com/library/ee221100.aspx)
 ◆ "A Task-Based Guide to Windows PowerShell Cmdlets" (http://technet.microsoft.com/en-us/scriptcenter/dd772285.aspx)

8.2 Implementing PowerShell Cmdlets in the Office 365 Driver

To call cmdlets, create a rule which adds the `PSExecute` containing the PowerShell command string.

The Office 365 driver looks for the `PSExecute` attribute in the input XDS code, reads any cmdlets embedded in a `<value/>` tag, and sends those commands to the Exchange Online service running on the Active Directory server. The Active Directory server executes the commands sequentially using a programmatic PowerShell interface.

NOTE: When including the `PSExecute` attribute in an Add or Modify event policy, you must adhere to the XDS format, or the driver ignores the embedded cmdlets.

8.2.1 Sample Office 365 Policy Rule for Executing Cmdlets

You can create a rule in the Office 365 driver policy to allow an administrator to send PowerShell cmdlets to the driver for execution.

Example 8-1 *The following example rule includes a PowerShell cmdlet in an Add event:*

```
<policy>
<rule>
    <description>PowerShell cmdlet with add</description>
       <conditions>
          <and>
            <if-operation op="equal">add</if-operation>
          </and>
       </conditions>
       <actions>
          <do-add-dest-attr-value name="PSExecute">
              <arg-value type="string">
                    <token-text xml:space="preserve">Get-MSolUser -
UserPrincipalName acmeUser@example.onmicrosoft.com | fl * | Out-File c:\msu1.txt</
token-text>
                    </arg-value>
          </do-add-dest-attr-value>
              <do-add-dest-attr-value name="PSExecute">
              <arg-value type="string">
                          <token-text xml:space="preserve">Get-Mailbox</token-
text>
              </arg-value>
                    </do-add-dest-attr-value>
       </actions>
</rule>
</policy>
```

You can also create rules to include PowerShell cmdlets in Modify events. However, if you include a cmdlet in a Modify event, ensure that you use the XDS format for constructing that type of event and including the `PSExecute` attribute

```
<policy>
<rule>
    <description>Powershell cmdlet in modify</description>
      <conditions>
         <and>
             <if-operation op="equal">modify</if-operation>
             <if-op-attr name="Title" op="equal">manager</if-op-attr>
         </and>
      </conditions>
      <actions>
       <do-add-dest-attr-value name="PSExecute">
          <arg-value type="string">
              <token-text xml:space="preserve">Get-Mailbox</token-text>
          </arg-value>
       </do-add-dest-attr-value>
</rule>
</policy>
```

Similarly, you also can create a rule to use the PoweShell cmdlets. The following is the sample output for `pwd` powershell cmdlet.

```
<status level="success" event-id="0" type="powershell" />
    <instance class-name="PowerShell" event-id="0">
      <attr attr-name="Drive">
        <value>C</value>
      </attr>
      <attr attr-name="Provider">
        <value>Microsoft.PowerShell.Core\FileSystem</value>
      </attr>
      <attr attr-name="ProviderPath">
        <value>C:\Novell\remoteloader.NET</value>
      </attr>
      <attr attr-name="Path">
        <value>C:\Novell\remoteloader.NET</value>
      </attr>
    </instance>
```

However, the execution of wrong powershell cmdlet `pwdi` displays output similar to this:

```
<status level="error" event-id="0" type="Powershell">The term 'pwdi' is not
recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
</status>
```

The following is a sample query XDS in PowerShell that allows an administrator to search for Microsoft Online users.

```
<query class-name="MSolUser" event-id="0"
  scope="subordinates">
   <search-class class-name="PowerShell"/>
     <search-attr attr-name="psexecute">
      <value>get-msoluser</value>
     </search-attr>
</query>
```

8.2.2 Creating Office 365 Policies for Executing Cmdlets

To use cmdlets in Identity Manager, first use Designer to create a new policy in the Office 365 driver. For more information about creating policies in Designer, see *Policies in Designer* (http://www.netiq.com/documentation/identity-manager-46/policy_designer/data/bookinfo.html) and *Understanding Policies for Identity Manager* (http://www.netiq.com/documentation/identity-manager-46/policy/data/bookinfo.html).

After you create a new policy, add a rule to the policy that includes an `add destination attribute value` action to create the `PSExecute` attribute, which calls one or more PowerShell cmdlets. You can include several cmdlet strings in multiple `value` tags for a single `PSExecute` attribute, as necessary.

To configure the rule using the Policy Builder, complete the following steps:

1 In Designer, right-click the policy in the Outline view and select **Edit**.

2 In the Policy Builder, select the location where you want to create the `PSExecute` attribute.

3 In the toolbar, click **Rule** and select **Action** > **Insert Action After**.

4 In the Do field under **Define new action below**, select **add destination attribute value**.

5 Specify `PSExecute` as the attribute name.

6 In the **Select mode** field, select **add to current operation**.

7 In the **Select object** field, select **Current object**.

8 In the **Specify value type** field, select **string**.

9 In the **Enter string** field, specify the PowerShell command string you want to use, enclosed in quotation marks.

10 Click **OK**.

11 Save the policy.

When specifying the PowerShell command string, you can include other variables configured in separate actions within the rule, as necessary.

For example, for the sample policy provided in Section 8.2.1, "Sample Office 365 Policy Rule for Executing Cmdlets," on page 39, you first add a rule to define the variable `identityname` as the name of the user account you want to disable using a PowerShell cmdlet, and then you specify the following string for the `PSExecute` variable, which uses the new `identityname` variable in the PowerShell command string:

```
"Disable-ADAccount -Identity"+Local Variable("identityname")
```

NOTE: You can also configure a policy to execute a specified cmdlet by modifying the XML directly, in the XML Source tab of the Policy Builder.

8.2.3 Verifying Office 365 Cmdlet Execution

When a PowerShell cmdlet runs successfully, the Active Directory returns a specific `success` event in the output XML, with the type `powershell`. After you run a cmdlet, check the output XML file for the following event:

```
<status level="success" event-id="linux-djs#20120510164317#1#2:facdcbbb-d440-4340-
1b85-bbcbcdfa40d4" type="powershell"/>
```

If the PowerShell cmdlet does not run successfully, the driver instead logs an `error` event in the output XML. The error message includes the reason for the failure and looks similar tot he following:

```
<status level="error" event-id="0" type="Powershell">The term 'pwdi' is not
recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
</status>
```

NOTE: If you execute multiple cmdlets in a single rule and one of the cmdlets does not run successfully, the driver does not execute any subsequent cmdlets in the rule and only logs the error event for the failed cmdlet. The driver does not log error events for the subsequent cmdlets, even though they did not run successfully, because the driver does not run those cmdlets after the failure occurs.

9 Troubleshooting the Driver

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

9.1 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 Driver Administration Guide*.

9.2 Troubleshooting Office 365 Driver Issues

9.2.1 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.

9.2.2 Adding a user with a long 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.

9.2.3 Adding a user with a long 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.

9.2.4 Initials Synchronization not Supported on the Subscriber channel

The Office 365 driver does not support the synchronization of user initials on the Subscriber channel. To workaround this issue, send the powershell cmdlet `Set-User -Initials <initals> - username` as part of the subscriber event.

9.2.5 Synchronization of an attribute depends on the selected MsolUser or MsolGroup type

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

For some operations, traces might appear with this message:

`Disallowed attribute Sync : <attr>.`

For more information on MsolUser and MsolGroup type attribute synchronization, see Table B-2 on page 63 and Table B-5 on page 65.

9.2.6 Synchronization Issues with EmailAddresses Attribute

The Office 365 driver displays invalid EmailAddresses attribute synchronization message when you add a user to the Office 365 portal. To workaround this issue, perform any one of the following actions:

- Configure a new single-valued eDirectory attribute of the type syntax string and map it with the MsolUserType in the schema mapping. You must set the MsolUserType attribute to UserMailbox/MailUser to synchronize the exchange attributes during the Add operation.
- Customize the Subscriber command transformation policy to include a rule that adds the MSolUserType attribute to the Add XDS event if MsolUsertype is not defined.

9.2.7 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.
```

9.2.8 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.

9.2.9 TypeInitializationException Errors during the Driver Startup

The `TypeInitializationException` exception can occur in the following cases:

1. PowerShell help is not up-to-date.
2. The Office 365 driver is not compatible with the Microsoft Online Services module.
3. The Microsoft Online Services are not present in the driver installation folder.

To start the driver successfully, perform one of the following actions:

- Run the `get-help new-msoluser` PowerShell command or run the `Update-Help` command to download and install the most recent help files for the Windows PowerShell modules. You can run the `PSVersion` command to verify the powershell version.

  A prompt displays asking you to confirm the update. Click **Yes** to proceed with the update.

- Upgrade the Office 365 driver to the latest patch and the Microsoft Online Services to the latest version. For more information, see Section 2.1, "Prerequisites," on page 17.
- Ensure that all the `dll` files from the default Windows PowerShell path are copied to the driver installation folder. For more information, see Chapter 2, "Installing the Driver Files," on page 17.
- Unblock the downloaded `dlls`. To unblock them, right-click the following binary files and select **Properties > Unblock**.
  - `DXMLMSOnlineDriver.dll`

- ◆ `SQLite.Interop.dll`
- ◆ `System.Data.SQLite.dll`

9.2.10   Re-granting Entitlements Generates an Error

The driver generates error messages if you try to re-grant an RBPM role that includes multiple entitlements to a user.

It is safe to ignore the error because it does not affect the re-granting role operation.

9.2.11   Synchronization Issues for Description Attribute

The description attribute does not synchronize for the Exchange groups on both Subscriber and Publisher channels.

There is no workaround at this time.

9.2.12   Publisher Event Removes Exchange Security/DL Group Exchange Attributes

The driver does not support exchange group attributes poll on the Publisher channel. NetIQ recommends that you set exchange attributes to **Ignore** on the driver filter.

9.2.13   Driver Deletes Description Attribute while Updating the eMailAddress attribute

When the Publisher channel updates the eMailAddress attribute for an exchange group, the driver sends a delete event and removes the group Description attribute from the Identity Vault.

9.2.14   Deleting All Groups from the Office 365 Portal is not Synchronized with the Identity Manager

The Office 365 driver does not synchronize the delete event with the Identity Manager if all the groups are deleted from the Office 365 portal.

9.2.15   Duplicate Primary Email Address in the Identity Vault

Identity Manager creates duplicate primary email addresses (SMTP) for the Office 365 users when the users are renamed.

To workaround this issue, set the **Optimize modifications to Identity Vault** option to **No** for the Internet EMail Address attribute in the driver filter.

9.2.16 Random Issue Observed While Connecting to the Exchange Portal

The `O365 throttling issue encountered` error randomly occurs when a user or group operation fails on the Exchange portal.

This is a Microsoft issue. Contact Microsoft support to troubleshoot the issue.

9.2.17 Exception Errors During Driver Restart

The Office 365 driver displays exception errors when you restart the driver after an abnormal exit. This is due to unavailability of runspaces required for establishing new remote PowerShell connections with the Office 365 portal. Before attempting a driver restart, wait for the Office 365 portal to automatically close the active runspaces because Microsoft allows only limited remote runspaces for each exchange online users.

9.2.18 Deleting a User From Associated Office365 Group Displays Error Message in Driver Logs

When a user is deleted from the Identity Vault which is a member of an associated group, it displays the following error message in the driver logs:

`The member you are trying to delete is not in this group.`

It is safe to ignore this error message.

9.2.19 Account Tracking Attributes Are Not Created When a User's MSolUserType Attribute Contains UserMailbox

When you add a user with MSolUserType attribute set to UserMailbox, the account tracing attributes are not created for the user.

There is no workaround at this time.

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 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 a Designer icon.

- Section A.1, "Driver Configuration," on page 49
- Section A.2, "Global Configuration Values," on page 54

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 50
- Section A.1.2, "Driver Object Password," on page 50
- Section A.1.3, "Authentication," on page 50
- Section A.1.4, "Startup Option," on page 50
- Section A.1.5, "Driver Parameters," on page 51
- Section A.1.6, "ECMAScript," on page 53
- Section A.1.7, "Global Configurations," on page 54

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.

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

- **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 custom license. This will appear as `[domainname]:[license name (service to be disabled)]` in the License Entitlements.

      NOTE: Ensure that there are no whitespace characters in the custom license name. An example for the custom license name is NOOFFICE_NOLYNC.

    - **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 Office 365 ProPlus and Lync Online services in your enterprise plan, use this string: OFFICESUBSCRIPTION,MCOSTANDARD.

      NOTE

      - To add licenses, run the `Get-MSolAccountSkurun` PowerShell command. To set up exclusions, go to **Driver Configuration > Subscriber Options** and add a custom license. For example, you can add the license name as `NoSharepointNoOffice` with a value of `SHAREPOINTWAC_EDU,SHAREPOINTSTANDARD_EDU`. When the driver connects to the Remote Loader and the PowerShell session starts, the driver shim reads all the licenses from Office 365 and creates a custom license for each of the Subscriber option licenses. For example, if you have four different licenses installed in Office 365

and one custom license configured in the driver, the driver returns eight licenses when you query for the License entitlement in the User Application, which includes four Office 365 licenses and additional four custom licenses.

 ◆ To discover service names for your respective subscription, run the `Get-MsolAccountSku` command. The command returns the list of available service names. You can select a desired service name and run the `Get-MsolAccountSku Where-Object <servicename>` command to return the service plan and provisioning status. Table A-1 lists an example of Service Plans and Provisioning Status.

Table A-1 *Service Plans and Status*

ServicePlan	ProvisioningStatus
INTUNE_0365	PendingActivation
OFFICESUBSCRIPTION	Success
MCOSTANDARD	Success
EXCHNAGE_S_ENTERPRISE	Success
SHAREPOINTWAC_DEVELOPER	Success
SHAREPOINT_S_DEVELOPER	Success

 ◆ **Exchange Online Configuration:** Select **Yes** to enable the Exchange Online 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.

   NOTE: By default, the driver adds itself as the owner of the distribution and security exchange groups. This is mandatory for the driver to manage these groups.

   ◆ **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

Show/Hide Publisher Connection: Select **Show** 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. The following filenames are created with the driver object GUID value in the default location:

    - MSOnline_MSolGroup<driver object GUID value>.s3db
    - MSOnline_MSolUser<driver object GUID value>.s3db

  The driver cleans up the database files. However, the cache needs to be deleted manually while uninstalling the driver.

- **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. If the value is set to **True**, the Office 365 driver will not generate any events on the Publisher channel on the driver startup. If the value is set to **False**, the Publisher events are cached when the driver is not running. By default, the value is set to **False**.

- **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 4, "Creating a New Driver Object," on page 25.

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, navigate to **Driver Properties > Global Configuration Values** and edit the password synchronization settings in your password synchronization policy tab.

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 55
   ◆ Section A.2.2, "Driver Configuration," on page 55

A.2.1 Password Synchronization

The following GCVs control password synchronization for the Office 365 driver. For more information, see the *NetIQ Identity Manager 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, to edit the Password management options go to **Driver Properties > Global Configuration Values**, and then edit it in your Password synchronization policy tab.

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**: 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

For more information about entitlements, see Section 1.3.8, "Supporting Entitlements," on page 15.

Use User Account Entitlement: Select **True** to enable the driver to manage user accounts based on the driver's defined entitlements. Select **False** 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. To assign multiple Office 365 licenses, you must create multiple resources on user application. This is required because an Office 365 license entitlement can have only single value.

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 *Administrator Guide to NetIQ Identity Reporting*.

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 Identity Manager Catalog Administrator allows you to map business roles with IT roles.

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

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

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

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

Resource Mapping

The Roles Based Provisioning Module allows you to map resources to users. For more information, see the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

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 *Administrator Guide to NetIQ Identity Reporting*.

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

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 affect the default configuration and policies processing behavior.You can add new attributes depending on your requirement. Table B-1 lists Identity Vault user and group attributes mapped to Office 365 user and group attributes.

Table B-1 Mapped User Attributes

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

Identity Vault	Office 365	Attributes
workforceID	Office	String
Group	**MSolGroup**	String
businessCategory	Group Type	String
CN	DisplayName	String
Description	Description	String
EMail Address	EMailAddress	Structured
	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	String
Owner	ManagedBy	String

NOTE: The driver ships with a default mapping of the attributes listed in Table B-1 on page 61. In case of Structured attributes, the conversion between the attribute mapping is automatically handled by the driver. To change the default mappings, Identity Manager requires you to make appropriate changes to the policies.

In default mapping, Office 365 postal address is mapped to the eDirectory postal address. The street address is a structured attribute and with the default mapping, the driver works as expected. However, if the street address needs to be interpreted differently (For example: string type), then it should be mapped to string type in eDirectory as well and the policy must be changed to flatten the structured syntax.

Example:

```
<rule>
<description>Transform StreetAddress</description>
    <conditions>
<and>
        <if-op-attr name="StreetAddress" op="available"/>
</and>
    </conditions>
<actions>
      <do-set-local-variable name="lv_streetaddress" scope="policy">
<arg-string>
          <token-op-attr name="StreetAddress"/>
</arg-string>
      </do-set-local-variable>
<do-strip-op-attr name="StreetAddress"/>
```

```
        <do-set-dest-attr-value name="StreetAddress">
<arg-value type="structured">
          <arg-component name="string">
<token-text xml:space="preserve">$lv_streetaddress$</token-text>
          </arg-component>
<arg-component name="string"/>
          <arg-component name="string"/>
<arg-component name="string"/>
          <arg-component name="string"/>
<arg-component name="string"/>
        </arg-value>
</do-set-dest-attr-value>
    </actions>
</rule>
```

This policy changes the incoming and outgoing structured type to string type.

Table B-2 lists the new MsolUser attributes.

Table B-2 *New Attributes supported for a Msoluser*

AlternateMobilePhones
CloudExchangeRecipientDisplayType
IsBlackberryUser
IsLicensed
Licenses
LiveId
ProxyAddresses

Table B-3 lists the new UserMailbox and MailUser attributes.

Table B-3 *New MsolOnline UserMailbox/MailUser Attributes*

MSExchRecipientTypeDetails	ProxyAddresses	ExternalEmailAddress
HomePhone	WebPage	Notes
Name	Alias **NOTE:** By default, the Alias attribute of Office 356 is mapped to DisplayName attribute of the Identity Vault. Ensure that you do not have any spaces in the value for this attribute. The driver converts spaces in Alias value to underscore.	SamAccountName
MicrosoftOnlineServicesID	DirectReports	Manager
OtherFax	OtherHomePhone	OtherTelephone
Pager	CountryOrRegion	StateOrProvince
CreateDTMFMap	TelephoneAssistant	WindowsEmailAddress

Identity	IsValid	Phone
FederatedIdentity	CustomAttribute1	CustomAttribute2
CustomAttribute3	CustomAttribute4	CustomAttribute5
CustomAttribute6	CustomAttribute7	CustomAttribute8
CustomAttribute9	CustomAttribute10	CustomAttribute11
CustomAttribute12	CustomAttribute13	CustomAttribute14
CustomAttribute15	ExtensionCustomAttribute1	ExtensionCustomAttribute2
ExtensionCustomAttribute3	ExtensionCustomAttribute4	ExtensionCustomAttribute5
LitigationHoldEnabled	RetentionHoldEnabled	UnifiedMailbox
IsMailboxEnabled	ForwardingAddress	ForwardingSmtpAddress
IsShared	IsLinked	UMEnabled
ArchiveStatus	IsInactiveMailbox	EmailAddresses

NOTE: In Table B-3, ProxyAddresses, ArchiveStatus, UMEnabled, and LitigationHoldEnabled are the synced attributes used in an Exchange hybrid deployment scenario.

Table B-4 lists the attributes that are written back to the on-premises Active Directory from the Active Directory driver in an Exchange hybrid deployment scenario.

Table B-4   Synced Attributes in an Exchange Hybrid Deployment Scenario

Write-Back attribute	MsolUser Attribute
msExchArchiveStatus	ArchiveStatus
msExchUserHoldPolicies	LitigationHoldEnabled
ProxyAddresses(LegacyExchangeDN as X500)	LegacyExchangeDN
msExchUCVoiceMailSettings	UMEnabled

Table B-4 lists the new MsolGroup attributes. These MsolGroup attributes are synchronized only on the Subscriber channel. Set the filter as **Ignore** for the Publisher channel to retain the eDirectory values.

Table B-5   *New MsolGroup Attributes*

Name	PrimarySmtpAddress	SimpleDisplayName
WindowsEmailAddress	Notes	RoomList
SamAccountName	CustomAttribute1	CustomAttribute2
CustomAttribute3	CustomAttribute4	CustomAttribute5
CustomAttribute6	CustomAttribute7	CustomAttribute8
CustomAttribute9	CustomAttribute10	CustomAttribute11
CustomAttribute12	CustomAttribute13	CustomAttribute14
CustomAttribute15	ExtensionCustomAttribute1	ExtensionCustomAttribute2
ExtensionCustomAttribute3	ExtensionCustomAttribute4	ExtensionCustomAttribute5

You can add custom attributes to the filter depending on your requirement. For example, the following filter entries include `CustomAttribute15` and `ExtensionCustomAttribute2` custom attributes.

```
<filter-attr attr-name="customAttribute15" merge-authority="default" priority-
sync="false" publisher="sync" publisher-optimize-modify="true" subscriber="sync"/
```

```
<filter-attr attr-name="ExtensionCustomAttribute2" merge-authority="default"
priority-sync="false" publisher="sync" publisher-optimize-modify="true"
subscriber="sync"/>
```