NetIQ® Identity Manager
Driver for SharePoint Implementation Guide

October 2014

Contents

About this Book and the Library

The *Identity Manager Driver for SharePoint Implementation Guide* explains how to install, configure, and manage the Identity Manager Driver for SharePoint.

Intended Audience

This book provides information for SharePoint administrators, NetIQ eDirectory administrators, and others who implement the Identity Manager driver for SharePoint.

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 SharePoint Driver

This section contains high-level information about how the SharePoint driver functions.

1.1 Key Terms

1.1.1 Identity Manager

NetIQ Identity Manager is a service that synchronizes data among servers in a set of connected systems by using a robust set of configurable policies. Identity Manager uses the Identity Vault to store shared information, and uses the Metadirectory engine for policy-based management of the information as it changes in the vault or connected system. Identity Manager runs on the server where the Identity Vault and the Metadirectory engine are located.

1.1.2 Connected System

A connected system is any system that can share data with Identity Manager through a driver. SharePoint is a connected system.

1.1.3 Identity Vault

The Identity Vault is a persistent database powered by eDirectory and used by Identity Manager to hold data for synchronization with a connected system. The vault can be viewed narrowly as a private data store for Identity Manager or more broadly as a metadirectory that holds enterprise-wide data. Data in the vault is available to any protocol supported by eDirectory, including NCP (the traditional protocol used by iManager), LDAP, and DSML.

Because the vault is powered by eDirectory, Identity Manager can be easily integrated into your corporate directory infrastructure by using your existing directory tree as the vault.

1.1.4   Metadirectory Engine

The Metadirectory engine is the core server that implements the event management and policies of Identity Manager. The engine runs on the Java Virtual Machine in eDirectory.

1.1.5   SharePoint Driver

The SharePoint driver for NetIQ Identity Manager enables user and group membership events to be synchronized between the Identity Vault and a SharePoint 2010 or SharePoint 2013 site collection. A single driver can process these events for a single site collection, which maintains user and group membership information for one or more SharePoint sites.

The SharePoint driver includes both Subscriber and Publisher channels. A Subscriber channel synchronizes events from Identity Vault to SharePoint, and a Publisher channel synchronizes events from SharePoint to the Identity Vault. By using the driver filter, you can configure the SharePoint driver to either use the subscriber channel or the Publisher channel, or both. SharePoint account creation, removal, and group assignments can be entitlement-based, and can be triggered from role assignments that grant or revoke entitlements. They can also be granted and revoked in other ways, depending on the driver policy.

1.1.6   .NET Driver Shim

A driver shim is the component of a driver that converts the XML-based Identity Manager command and event language (XDS) to the protocols and API calls needed to interact with a connected system. The shim is called to execute commands on the connected system after the Output Transformation runs. Commands are usually generated on the Subscriber channel but can be generated by command write-back on the Publisher channel.

The shim also generates events from the connected system for the Input Transformation policy. The SharePoint driver shim is implemented in C# and uses the .NET framework API for SharePoint access. The SharePoint driver shim is implemented as a Windows .NET DLL file named `DXMLSharepointDriver.dll`.

The SharePoint driver must be loaded and run by the .NET Remote Loader. Unlike most other Identity Manager drivers, the SharePoint driver cannot be loaded and run directly by the Metadirectory engine.

1.1.7   .NET Remote Loader

A Remote Loader enables a driver shim to execute from a remote machine where the Metadirectory engine is not installed. A Remote Loader is typically used when the driver shim requirement are not met by the Identity Manager server. Because the SharePoint driver shim relies on the SharePoint .NET APIs that are only available on the SharePoint server, the SharePoint driver shim must be loaded and run from the .NET Remote Loader on the SharePoint server.

The .NET Remote Loader is a service that executes the driver shim and passes information between the shim and the Metadirectory engine. When you use a .NET Remote Loader, you install the driver shim on the server where the .NET Remote Loader is running, not on the server where the Metadirectory engine is running. You can choose to use SSL to encrypt the connection between the Metadirectory engine and the .NET Remote Loader. For more information, see the instructions in "Installing Remote Loader" in the *NetIQ Identity Manager Setup Guide*.

When you use the Remote Loader with the SharePoint driver shim, a connection exists between the Metadirectory engine and the Remote Loader. The SharePoint driver shim uses local SharePoint .NET APIs to communicate directly with the SharePoint service.

1.2   SharePoint Differs from Other Drivers

Unlike most other drivers, the SharePoint driver cannot be loaded directly by the Identity Manager engine. It can only be run from the .NET Remote Loader that has been created specifically for use with the SharePoint driver. The .NET Remote Loader and the SharePoint driver shim must be installed directly on the SharePoint server.

The SharePoint server that you install the .NET Remote Loader and driver shim on must have access to the SharePoint site collection for the SharePoint driver to work.

Any Identity Manager installation that can make a network connection (TCP/IP) to the SharePoint server can then load the SharePoint driver through the .NET Remote Loader.

1.3   Data Transfers between Systems

Data flows between SharePoint and the Identity Vault by using the Publisher and Subscriber channels.

The Publisher channel does the following:

- ◆ Watches for changes to SharePoint users and groups.
- ◆ Synchronizes SharePoint user and group changes with the Identity Vault.

The Subscriber channel does the following:

- ◆ Watches for changes to the Identity Vault users and groups.
- ◆ Synchronizes Identity Vault user and groups changes with SharePoint.

TIP: Run the `get-spuser` powershell command to verify if the user is added to SharePoint. For example, the `get-spuser -Web <http://sharepoint server>` command returns all users and the `get-spuser "SHAREPOINT\johndoe" -Web http://sharepoint server | Format-List` command returns all attributes.

You can configure the driver so that Identity Vault is allowed to update a specific attribute. In this configuration, the most recent change determines the attribute value, except in the case of merge operations that are controlled by the filters and merge authority.

1.4   Key Driver Features

The sections below contain a list of the key driver features.

1.4.1   Local Platforms

The SharePoint driver does not run locally.

1.4.2   Remote Platforms

The SharePoint driver uses the .NET Remote Loader service to run on a Windows SharePoint server other than the Metadirectory server. The Remote Loader service for the SharePoint driver can be installed on Windows Server 2003 SP2 (32-bit), Windows Server 2008 (32-bit and 64-bit), and Windows Server 2008 R2 (64-bit).

For additional information about system requirements, refer to the *NetIQ Identity Manager Setup Guide*.

1.4.3   Entitlements

The SharePoint driver implements entitlements.

Entitlements make it easier to integrate Identity Manager with the Identity Manager User Application and Role-Based Services in eDirectory. In the User Application, an action such as provisioning an account in SharePoint is delayed until the proper approvals have been made. In Role-Based Services, rights assignments are made 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 has been 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 something in SharePoint. You can use entitlements to grant the right to an account in SharePoint 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 upon its own rules.

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*.

The driver can be configured without using entitlements. In these scenarios, Active Directory could be the authoritative source for both users and group membership. After the Active Directory driver synchronizes identities and group membership from Active Directory into the Identity Vault, the SharePoint driver synchronizes them from the Identity Vault into SharePoint.

1.5   Driver Packages

The SharePoint driver is created in Designer using packages. The packages create a driver with a set of policies and rules suitable for synchronizing with SharePoint. If your requirements for the driver are different from the default policies, you need to modify the default policies to do what you want. Pay close attention to the default matching policies. The data that you trust to match users usually is different from the default. The policies themselves are commented and you can gain a greater understanding of what they do by importing a test driver and reviewing the policies with Designer or iManager. When you configure the SharePoint driver, you can either select the default or LDAP configuration to synchronize the identities. The default configuration contains the default configuration information for the SharePoint driver. With default configuration, you can synchronize

identities that have an association with the Active Directory. The LDAP configuration contains the default configuration information for the SharePoint driver. With LDAP configuration, you can synchronize identities that have an association with the LDAP directory

- Section 1.5.1, "Data Flow," on page 13

1.5.1 Data Flow

Data flow between SharePoint and the Identity Vault is controlled by the filters, mappings, and policies that are in place for the SharePoint driver.

- "Filters" on page 13
- "Schema Mapping" on page 13

Filters

The driver filter determines which classes and attributes are synchronized between SharePoint and the Identity Vault, and in which direction synchronization takes place.

Schema Mapping

Table 1-1 and Table 1-2 list Identity Vault user and group attributes that are mapped to SharePoint user and group attributes.

The mappings listed in the tables are default mappings. You can remap same-type attributes.

- Table 1-1, "Mapped User Attributes," on page 13
- Table 1-2, "Mapped Group Attributes," on page 14
- Table 1-3, "Mapped User Attribute when configured in LDAP Mode," on page 14

Table 1-1 *Mapped User Attributes*

eDirectory - User	SharePoint - SPuser
Full Name	Name
DirXML-ADAliasName	LoginName
Description	Notes
Internet EMail Address	Email

The DirXML-ADAliasName is provided to the SharePoint driver by the Active Directory driver. This attribute is used as the LoginName for the SharePoint system.

Table 1-2   *Mapped Group Attributes*

eDirectory - Group	SharePoint - SPGroup
Member	Users
CN	Name
Description	Description
Owner	Owner

Table 1-3   *Mapped User Attribute when configured in LDAP Mode*

Active Directory-Group	SharePoint - SPGroup
Full Name	SharePoint - SPuser
CN	Name
Description	LoginName
Internet EMail Address	Email

2 Preparing SharePoint

In this section:

2.1 Prerequisites

❑ Read the NetIQ Identity Manager 4.5 prerequisites, as listed in *System Requirements for the Identity Manager Engine* in the *NetIQ Identity Manager Setup Guide*.

❑ Microsoft .NET Framework version 3.5 or 3.5.1.

❑ Windows Server 2008 SP2 (64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit), or Windows Server 2012 R2 (64-bit).

❑ SharePoint Server 2010 or SharePoint Server 2013 on the same machine where the SharePoint driver needs to be installed.

❑ Active Directory driver.

The machine where you are installing the SharePoint driver is a member of the Active Directory domain that is connected to the Identity Manager through Active Directory driver. The SharePoint driver must be connected to the same Identity Vault as the Active Directory driver. The drivers can be in different driver sets, but they must be in the same Identity Vault.

❑ LDAP Directory driver.

2.2 Installing the .NET Remote Loader and the SharePoint Driver

The .NET Remote Loader can be installed through the Identity Manager integrated installer or the framework installer.

2.2.1 Using the Identity Manager Integrated Installer

To install the.NET Remote Loader and the SharePoint driver:

1 Run `install.exe` from the Identity Manager integrated installer installation folder.

See *Preparing to Install the Engine, Drivers, and Plug-ins* in the *NetIQ Identity Manager Setup Guide*.

2 Accept the license agreement and click **Next**.

3 Select **Metadirectory Server**. When you select meta directory server .NET RL and sharepoint driver will get installed automatically on windows.

4 Review the Summary page, then click **Install** to complete the installation.

2.2.2 Using the Identity Manager Framework Installer

To install .NET Remote Loader and SharePoint driver:

1 Run `install.exe` from the Identity Manager framework installer installation folder.

2 Accept the license agreement and click **Next**.

3 Select **NetIQ Identity Manager Connected System Server (.NET).**

When you select the .NET Remote Loader, the installer automatically installs the SharePoint driver.

4 Select the .NET Remote Loader installation directory on your system and continue the installation.

2.3 Configuring and Running the SharePoint Driver

You can configure the SharePoint Driver in two ways:

2.3.1 Using the Command Line

1 Open a command prompt.

2 Change to the installation directory of the .NET Remote Loader.

3 Edit the `sharepoint-conf.txt` sample configuration file from the .NET Remote Loader directory.

The command line options of .NET Remote Loader are same as the conventional Remote Loader. Detailed options can be seen by running `remoteloader.exe` without passing any parameters, which opens an HTML help page. For detailed command line options, see the *Using the Command Line to Start Driver Instances on UNIX or Linux* in the *NetIQ Identity Manager Setup Guide*.

4 Run the `remoteloader.exe -config <configFile> -sp` command to set the Remote Loader and the driver passwords.

The SharePoint driver can be created as an application or service. For creating it as an application or service, you need to set the Remote Loader and the driver passwords.

Running `remoteloader.exe` initializes the lcache. It might take a while before the password is requested.

lcache is required for auditing purpose.

5 Start this SharePoint instance as an application or service.

- As an application:
    1. Run the following command:

      ```
      remoteloader.exe –config <configFile>
      ```

The trace is started in the same command window. If you close the command window, the driver stops.

2. To stop the SharePoint application instance, enter Ctrl + C.

◆ As a service:

1. Run the following command:

```
remoteloader.exe -config <configFile> -service
```

This starts the .NET Remote Loader service and opens a trace window.

2. To stop the SharePoint driver service, go to **Services**, then stop the service.

For more information about Remote Loader, see *Configuring the Remote Loader and Drivers* in the *NetIQ Identity Manager Setup Guide*.

NOTE: If you run the .Net Remote Loader service with the default user privilege, it does not allow the Sharepoint driver to start and access the Sharepoint site collection. The Remote Loader service must run as User that has Administrator privilege for site collection. This applies for both configuring the SharePoint driver by using the command line as well as the .NET Remote Loader GUI.

2.3.2 Using the .NET Remote Loader Graphical Interface

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 parameters in the page that displays.

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

The SharePoint driver can be configured as an application or as a service.

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

When the driver is started, a trace window opens.

2.3.3 Modifying the .NET Version Preference for SharePoint 2013

The .NET version preference in the `RemoteLoader.exe.config` and `RemoteLoaderSvc.exe.config` files must be modified for SharePoint 2013.

The following is the default configuration:

```
<?xml version="1.0"?>
<configuration>
  <runtime>
    <NetFx40_LegacySecurityPolicy enabled="true"/>
  </runtime>
<startup>
  <supportedRuntime version="v2.0.50727"/>
  <supportedRuntime version="v4.0.30319"/>
</startup>
</configuration>
```

The above default configuration must be modified as follows:

```
<?xml version="1.0"?>
<configuration>
  <runtime>
    <NetFx40_LegacySecurityPolicy enabled="true"/>
  </runtime>
<startup>
  <supportedRuntime version="v4.0.30319"/>
  <supportedRuntime version="v2.0.50727"/>
</startup>
</configuration>
```

3 Creating a New Driver Object

After the SharePoint driver files are installed on the server where you want to run the driver, you can create the driver in the Identity Vault. You do so by installing the driver packages or importing the basic driver configuration file and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- Section 3.1, "Creating the Driver Object in Designer," on page 19
- Section 3.2, "Activating the Driver," on page 24
- Section 3.3, "Adding Packages to an Existing Driver," on page 25

3.1 Creating the Driver Object in Designer

You create the SharePoint driver object by installing the driver packages and then modifying the configuration to suit your environment. After you create and configure the driver, you need to deploy it to the Identity Vault and start it.

- Section 3.1.1, "Importing the Current Driver Packages," on page 19
- Section 3.1.2, "Installing the Driver Packages," on page 20
- Section 3.1.3, "Configuring the Driver Object," on page 22
- Section 3.1.4, "Deploying the Driver," on page 23
- Section 3.1.5, "Starting the Driver," on page 24

NOTE: You should not create driver objects by using the new Identity Manager 4.0 and later configuration files through iManager. This method of creating driver objects is no longer supported. To create drivers, you now need to use the new package management features provided in Designer.

3.1.1 Importing the Current Driver Packages

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

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

1 Open Designer.

2 In the toolbar, click **Help** > **Check for Package Updates**.

3 Click **OK** to update the packages

   or

   Click **OK** if the packages are up-to-date.

4 In the Outline view, right-click the Package Catalog.

5 Click **Import Package**.
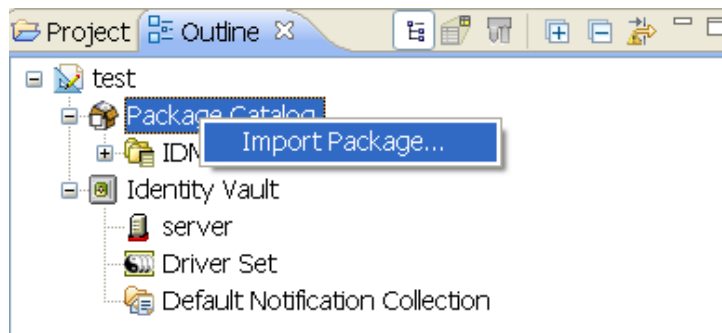
6 Select any SharePoint driver packages

or

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

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

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

8 After the current packages are imported, continue with Section 3.1.2, "Installing the Driver Packages," on page 20.

3.1.2 Installing the Driver Packages

1 In Designer, open your project.

2 From the Palette, drag-and-drop the SharePoint driver to the desired driver set in the Modeler.

The SharePoint driver is under the Enterprise category in the Palette.

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

4 Select the optional features to install for the SharePoint driver. The options are:

Default Configuration: This package contains the default configuration information for the SharePoint driver. With default configuration, you can synchronize identities that have an association with the Active Directory.

LDAP Configuration: This package contains the default configuration information for the SharePoint driver. With LDAP configuration, you can synchronize identities that have an association with the LDAP directory.

NOTE: When you configure the SharePoint driver, you can either select the default or LDAP configuration to synchronize the identities. You can also configure the Identity Vault to act as the LDAP identity provider. If you choose to configure the Identity Vault as the LDAP identity provider, no association to any other LDAP directory is required.

The LDAP directory as identity provider is not supported with SharePoint server 2013 in Identity Manager 4.5.

The **Default** and **LDAP configuration** options are mutually exclusive.

Entitlements: Verify that this option is selected to use the predefined entitlements for account management. For more information, see *NetIQ Identity Manager Entitlements Guide*.

5 Click **Next**.

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

7 (Conditional) If more than one type of package dependency must be installed, you are presented with these packages separately. Continue to click **OK** to install any additional package dependencies.

8 (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:

User Container: Select the Identity Vault container where SharePoint 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.

.If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

Group Container: Select the Identity Vault container where SharePoint 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.

.If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

9 Click **Next**.

10 On the Install SharePoint Base page, specify a name for the driver that is unique within the driver set, then click **Next**.

11 On the new Install SharePoint Base page, fill in the following fields, then click **Next**:

Site Collection Information: Fill in the following fields to define the SharePoint site collection:

   ◆ **User Name:** Specify the name of the SharePoint user. The driver shim requires this name to access the SharePoint site (For example, AD-DOMAIN\username).

   ◆ **User Password:** Specify the password of the SharePoint user. The driver shim requires this password to access the SharePoint site.

   ◆ **Site Collection URL:** Specify the URL of the top-level SharePoint site collection with which the shim will interact.

   ◆ **AD Domain Name:** Specify the Active Directory domain name of the domain used by the SharePoint site collection. This value is used with the value of the Identity Vault DirXML-ADAliasName attribute to construct the SharePoint User LoginName attribute (For example, AD-DOMAIN and JDoe become AD-DOMAIN\JDoe).

   ◆ **AD Driver:** Specify the Active Directory driver that synchronizes user to the Active Directory domain that SharePoint uses for authentication. If a driver is specified here, a valid association from that driver on the user is a prerequisite to synchronizing the user to SharePoint. The users synchronizes to Active Directory before synchronizing to SharePoint.

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

   ◆ **Domain Name:** Specify the Active Directory domain name that the SharePoint site collection is a part of. On most systems, the NETBIOS name is the domain name. The Publisher channel synchronizes objects only from this domain. To synchronize all the objects found in the SharePoint site collection that match the Publisher channel filter, leave this field blank.

   ◆ **Polling Interval:** Specify the number of seconds the Publisher channel waits after polling the SharePoint system for new changes before polling again.

12 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.

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

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

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

14 After you have installed the driver, you can change the configuration for your environment. Proceed to Section 3.1.3, "Configuring the Driver Object," on page 22.

or

If you do not need to configure the driver, continue with Section 3.1.4, "Deploying the Driver," on page 23.

3.1.3 Configuring the Driver Object

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 Parameters located on the Driver Configuration page and the Global Configuration Values. These settings must be configured properly for the driver to start and function correctly.

If you do not have the Driver Properties page displayed in Designer:

1 Open your project.

2 In the Modeler, right-click the driver icon ⬚ or the driver line, then select **Properties**.

3 Make any desired changes, then click **OK** to save the changes.

To configure the settings in iManager:

1 Ensure that the Modify Object page for the SharePoint driver is displayed in iManager. If it is not:

   1a In iManager, click ⬚ to display the Identity Manager Administration page.

   1b Click **Identity Manager Overview**.

   1c Browse to and select the driver set object that contains the new driver.

   1d Click the driver set name to access the Driver Set Overview page.

   1e Click the upper right corner of the driver, then click **Edit properties**.

2 Review the settings on the various pages and modify them as needed for your environment. The configuration settings are explained in Appendix A, "Driver Properties," on page 33.

3 After modifying the settings, click **OK** to save the settings and close the Modify Object page.

4 (Conditional) If the SharePoint driver's Summary page for the Import Configuration Wizard is still displayed, click **Finish**.

WARNING: Do not click **Cancel** on the Summary page. This removes the driver from the Identity Vault and results in the loss of your work.

In addition to the driver settings, you should review the set of default policies and rules contained in the driver packages. Although these policies and rules are suitable for synchronizing with SharePoint, your synchronization requirements for the driver might differ from the default policies. If this is the case, you need to change them to carry out the policies you want. The default policies and rules are discussed in Section 1.5, "Driver Packages," on page 12.

3.1.4 Deploying the Driver

After the driver object 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 line, then select **Live > Deploy**.

3 If you are authenticated to the Identity Vault, skip to Step 5; otherwise, specify the following information:

   ◆ **Host:** Specify the IP address or DNS name of the server hosting the Identity Vault.

   ◆ **Username:** Specify the DN of the user object used to authenticate to the Identity Vault.

   ◆ **Password:** Specify the user's password.

4 Click **OK**.

5 Read through the deployment summary, then click **Deploy**.

6 Read the successful message, then click **OK**.

7 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. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.

   7a Click **Add**, then browse to and select the object with the correct rights.

   7b Click **OK** twice.

      For more information about defining a Security Equivalent User in objects for drivers in the Identity Vault, see "Establishing a Security Equivalent User" in the *NetIQ Identity Manager Security Guide*.

8 Click **Exclude Administrative Roles** to exclude users that should not be synchronized.

   You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

   8a Click **Add**, then browse to and select the user object you want to exclude.

   8b Click **OK**.

   8c Repeat Step 8a and Step 8b for each object you want to exclude.

   8d Click **OK**.

9 Click **OK**.

3.1.5   Starting the Driver

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

To start the driver by using Designer:

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon [image] or the driver line, then select **Live > Start Driver**.

The driver cannot initialize completely unless it successfully connects to the .NET Remote Loader and loads the SharePoint driver shim.

To start the driver by using iManager:

1 In iManager, click [image] 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**.

The driver cannot initialize completely unless it successfully connects to the .NET Remote Loader and loads the SharePoint driver shim.

For information about management tasks with the driver, see Chapter 5, "Managing the Driver," on page 29.

3.2   Activating the Driver

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

If driver activation has expired, the following error message is displayed in the ndstrace window:

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

To use the driver, you must reactivate it.

For information on activation, refer to "Activating Identity Manager" in the *NetIQ Identity Manager Setup Guide*.

3.3   Adding Packages to an Existing Driver

You can add new functionality to an existing driver by adding new packages to an existing driver.

1 Right-click the driver, then click **Properties**.

2 Click **Packages**, then click the **Add Packages** icon ✚.

3 Select the packages to install. If the list is empty, there are no available packages to install.

4 (Optional) Deselect the **Show only applicable package versions** option, if you want to see all available packages for the driver, then click **OK**.

   This option is only displayed on drivers. By default, only the packages that can be installed on the selected driver are displayed.

5 Click **Apply** to install all of the packages listed with the Install operation.
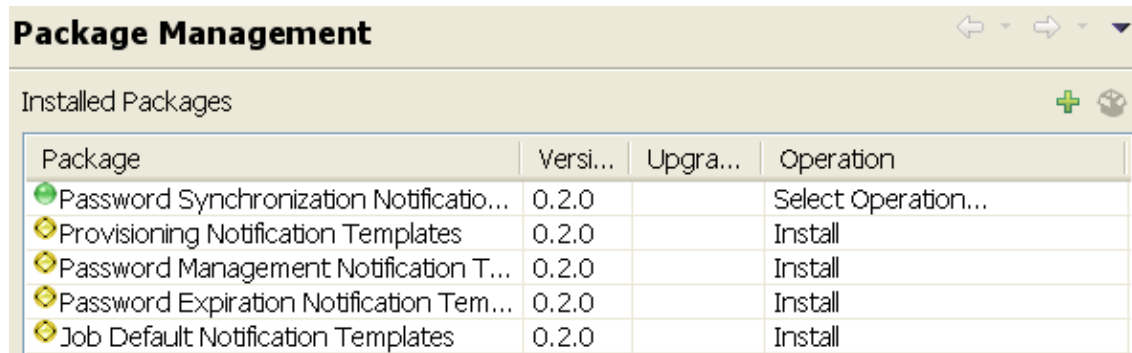
6 (Conditional) Fill in the fields with appropriate information to install the package you selected for the driver, then click **Next**.

7 Read the summary of the installation, then click **Finish**.

8 Click **OK** to close the Package Management page after you have reviewed the installed packages.
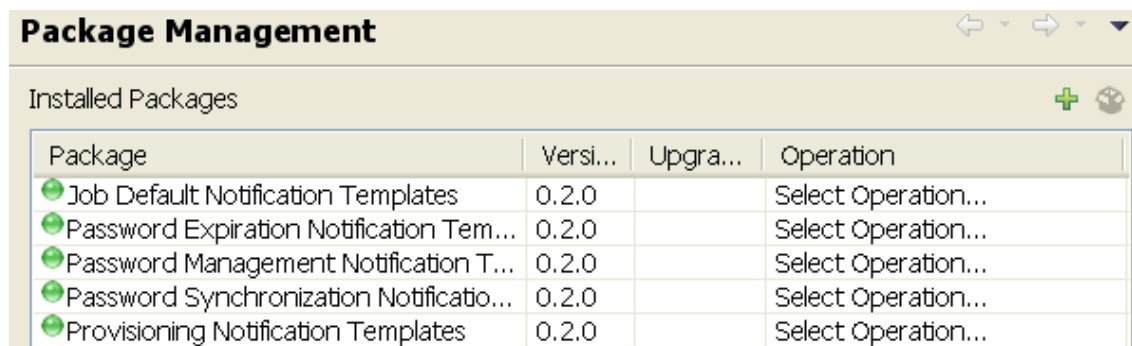
9 Repeat Step 1 through Step 8 for each driver where you want to add the new packages.

4 Upgrading an Existing Driver

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

- Section 4.1, "Supported Upgrade Paths," on page 27
- Section 4.2, "What's New in Version 4.5," on page 27
- Section 4.3, "Upgrade Procedure," on page 27

4.1 Supported Upgrade Paths

You can upgrade from 4.0 version of the SharePoint driver to 4.5 version.

4.2 What's New in Version 4.5

Version 4.5 of the driver does not include any new features.

4.3 Upgrade Procedure

The process for upgrading the SharePoint driver is the same as for other Identity Manager drivers. For detailed instructions, see "Upgrading the Identity Manager Drivers" in the *NetIQ Identity Manager Setup Guide*.

NOTE: If you are applying Engine 4.0.2 Patch 5 or above, check if you have the correct .NET runtime order, as mentioned in Section 2.3.3, "Modifying the .NET Version Preference for SharePoint 2013," on page 17.

5 Managing the Driver

As you work with the SharePoint driver, there are a variety of 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
- Synchronizing objects
- Migrating and resynchronizing data
- Activating the driver
- Upgrading an existing driver

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*.

6 Troubleshooting

Refer to the following sections if you are experiencing a problem with the SharePoint driver.

6.1 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use ndstrace. You should only use it during testing and troubleshooting the driver. Running ndstrace 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*.

6.2 .NET Remote Loader Issues

6.2.1 Adding a group without the managedBy attribute in Active Directory does not synchronize with SharePoint

When you add a group in Active Directory, it does not reflect in SharePoint unless the managedBy attribute for that group is added and the managedBy user of that group is already present in SharePoint.

6.2.2 In the .NET Remote Loader GUI, stopping an application instance with a wrong password shows as stopped

If you stop an application instance, for example SharePoint driver, with the correct password, it stops the instance and also shows the Stopped status in the .NET Remote Loader GUI.

If you stop an application instance with the wrong password, it displays the following error in the trace window:

```
Invalid response to challenge during command authentication
```

In the .NET Remote Loader GUI, it shows that the application instance is stopped, and the **Stop** button is replaced with the **Start** button. The Task Manager shows that the Remote Loader process is still running.

To work around this issue: In order to know the correct status of the application instance and to display the **Stop** button in the .NET Remote Loader console, click the **Start** button. Because the application instance is already running, it changes the status to Started and shows the **Stop** button in the GUI.

6.2.3 In the .NET Remote Loader GUI, if the trace window of an application or a service instance is closed, it stops the application or service

A trace window opens when the application or service instance is started in the .NET Remote Loader GUI and is automatically closed when the instance is stopped through the GUI. If the instance is still running as an application or as a service, closing the trace window stops the application or the service instance.

To work around the issue, do not close the trace window.

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the SharePoint driver. These are the only unique properties for drivers. 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 an icon.

- Section A.1, "Driver Configuration," on page 33
- Section A.2, "Global Configuration Values," on page 35

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 33
- Section A.1.2, "Driver Object Password (iManager Only)," on page 34
- Section A.1.3, "Authentication," on page 34
- Section A.1.4, "Startup Option," on page 34
- Section A.1.5, "Driver Parameters," on page 35

A.1.1 Driver Module

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

Java/Native: This option is not used with the SharePoint driver.

Connect to Remote Loader: This option should be used for SharePoint driver when the driver is connecting remotely to the connected system. Designer includes two suboptions:

- ◆ **Driver Object Password:** Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.

- ◆ **Remote Loader Client Configuration for Documentation:** : Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

A.1.2 Driver Object Password (iManager Only)

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.

Authentication ID: Specify a user application ID. This ID is used to pass Identity Vault subscription information to the application.

Example: `Administrator`

Authentication Context: Specify the IP address or name of the server the application shim should communicate with.

Remote Loader Connection Parameters: Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, when 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` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine.

Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`

Cache limit (KB): Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited. 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** field.

Remote Loader Password: Used only if the driver 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 allows 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.

Do not automatically synchronize the driver: This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

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 different categories:

Driver Options

User name: The name of the SharePoint user that the shim can use to access the SharePoint site. (For example, `AD-DOMAIN\username`)

User password: The password of the SharePoint user that the shim can use to access the SharePoint site. If you want to use Password Synchronization, select **Negotiate**.

Site Collection URL: The URL of the top-level SharePoint site collection with which the shim can interact.

Publisher Options

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 driver process must have write access to the directory.

Domain name: Specify the Active Directory domain name that the SharePoint site collection is a part of. On most systems, NETBIOS name is the domain name. The Publisher channel synchronizes objects only from this domain. To synchronize all the objects found in the SharePoint site collection that match the Publisher filter, leave the **Domain Name** blank.

Polling Interval: Specify the number of seconds the Publisher channel should wait after polling SharePoint for new changes before polling again.

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 SharePoint driver includes many GCVs. You can also add your own if 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 SharePoint 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 Active Directory driver icon 🖼 or line, then select **Properties > Global Configuration Values.**

or

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

The global configuration values are organized as follows:

A.2.1 Driver Configuration

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

Site collection URL: The URL of the top-level SharePoint site collection with which the shim will interact.

AD Domain Name: The Active Directory domain name of the domain used by the SharePoint site collection. This value is used with the value of the Identity Vault DirXML-ADAliasName attribute to construct the SharePoint User LoginName attribute (for example, AD-DOMAIN and JDoe become AD-DOMAIN\JDoe).

AD Driver: The Active Directory driver that synchronizes user to the Active Directory domain that SharePoint uses for authentication. If a driver is specified here, a valid association from that driver on the user is a prerequisite to synchronizing the user to SharePoint. The users synchronizes to Active Directory before synchronizing to SharePoint.

A.2.2 Entitlements

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

Entitlements Configuration

Use the following GCVs to control how the entitlements for the driver work. For more information about entitlements, see the *NetIQ Identity Manager Entitlements Guide*.

Use User Account Entitlement: Entitlements act like an On/Off switch to control account access. Enable the driver for entitlements to create accounts, and remove/disable when the account entitlement is granted to or revoked from users. If you select **True**, user accounts in SharePoint can be controlled by using Entitlements.

- ◆ **When account entitlement revoked:** Select the desired action in the SharePoint system when a User Account entitlement is revoked from an Identity Vault user. The options are **Remove user from the SharePoint site collection** or **do nothing**.

- ◆ **Parameter Format:** Select the parameter format the entitlement agent must use. The options are **Identity Manager 4** or **Legacy**.

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

- ◆ **Parameter Format:** Select the parameter format the entitlement agent must use. The options are **Identity Manager 4** or **Legacy**.

Role Mapping

The Identity Manager Catalog Administrator allows you to map business roles with IT roles. For more information, see the *NetIQ Identity Manager Catalog Administrator User Guide* .

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

Allow mapping of user accounts: Select **Yes** if you want to allow mapping of user accounts in Catalog 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.

Resource Mapping

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

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

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

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

Entitlement Extensions

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

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

B Trace Levels

The driver supports the following trace levels:

Table B-1 *Supported Trace Levels*

Level	Description
0	No trace messages are displayed or logged
1	Basic trace messages are displayed and logged
2	Level 1 messages and the contents of XML documents that are used during event processing are displayed and logged
3	Trace Level 2 messages and extensive rule processing messages are displayed and logged the above plus template instantiations
4	Trace Level 3 messages, extensive rule processing message, and connections are displayed
5	Trace Level 5 is a user-defined trace level