NetIQ® Identity Manager

Driver for Salesforce.com Implementation Guide

October 2019

Legal Notices

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

Contents

About this Book and the Library

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

Intended Audience

This book provides information for individuals responsible for using the Identity Manager Driver for Salesforce.com. You should also have an understanding of SOAP, HTML, and HTTP protocols.

Other Information in the Library

For more information about the library for Identity Manager, see the following resources:

- Identity Manager documentation website (https://www.netiq.com/documentation/identity-manager-47/)
- Identity Manager drivers documentation website (https://www.netiq.com/documentation/identity-manager-47-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 Salesforce.com Driver

Identity Manager 4.0 and later offers automatic provisioning and synchronization of users to cloud applications. The new Salesforce.com driver for NetIQ Identity Manager can seamlessly provision and de-provision users to and from the Salesforce.com cloud application keeping the user identity information consistent across the Identity Vault and the cloud application. The Salesforce.com driver supports secure password synchronization across Identity Vault and Salesforce.com cloud and supports authenticated proxy server and configurable user profile for automatic user provisioning. The Salesforce.com driver for Identity Manager offers out-of-the box random password generation policy for the newly provisioned users.

The Salesforce.com driver uses a combination of language and protocols to enable identity provisioning and data synchronization between Identity Vault and Salesforce.com.

IMPORTANT: The Publisher channel is supported with the driver shim version 4.0.0.0 and above only.

This section provides the following information on the Salesforce.com driver:

Driver Concepts

This section contains the following information:

Data Management

The Salesforce.com driver communicates with Salesforce.com using the Salesforce.com partner API. The partner API is represented as XML and its transport is SOAP 1.1 over HTTPS.

SOAP

SOAP (Simple Object Access Protocol) is an XML-based protocol for exchanging messages. It defines the message exchange but not the message content. The driver supports SOAP 1.1.

SOAP documents are organized into three elements:

- **Envelope:** The root XML node.

- **Header:** Provides context knowledge such as a transaction ID and security information.
- **Body:** The method-specific information.

SOAP follows the HTTP request/response message model, which provides SOAP request parameters in an HTTP request and SOAP response parameters in an HTTP response.

XML

XML (Extensible Markup Language) is a generic subset of Standard Generalized Markup Language (SGML) that allows for exchange of structured data on the Internet.

HTTP

HTTP is a protocol used to request and transmit data over the Internet or other computer network. The protocol works well in an Internet infrastructure and with firewalls.

HTTP is a stateless request/response system because the connection is usually maintained only for the immediate request. The client establishes a TCP connection with the server and sends it a request command. The server then sends back its response.

NOTE: Salesforce.com communication mostly happens over HTTPS.

How the Driver Works

The following diagram illustrates the data flow between Identity Manager and Salesforce.com service:

Figure 1-1 *Salesforce.com Driver Data Flow*

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

The driver shim receives the XML from the driver policy. The driver shim uses HTTPS to communicate with Salesforce.com.

Salesforce.com processes the request, and returns a response to the driver shim. The driver processes the response, converting it into appropriate XDS that is reported back to the Identity Manager engine. The Publisher channel periodically polls for additions and modifications to the objects in Salesforce.com. On a successful retrieval of the changes, it stores the polling time for use in the next polling cycle. To prevent loopback, the driver discards modifications done by users that the Subscriber channel uses to update Salesforce.com.

Support for Standard Driver Features

The following sections provide information about how the Salesforce.com driver supports these standard driver features:

Local Platforms

A local installation is an installation of the driver on the Identity Manager server. You can install the Salesforce.com driver on the operating systems supported for Identity Manager server.

For information about the operating systems supported for Metadirectory server, see the NetIQ Identity Manager Technical Information website (https://www.netiq.com/products/identity-manager/advanced/technical-information/).

Remote Platforms

The Salesforce.com driver can use the Remote Loader service to run on a server other than the Identity Manager server. You can install the Salesforce.com driver on the operating systems supported for the Remote Loader.

For information about the supported operating systems for Remote Loader, see the NetIQ Identity Manager Technical Information website (https://www.netiq.com/products/identity-manager/advanced/technical-information/).

Supported Operations

The Salesforce.com driver supports the following operations on the Subscriber channel:

- Add users

  When a user is added to your database, the user is created in the Salesforce.com.
- Update users

  When a user is updated in your database, the updated user information is synchronized with the Salesforce.com.
- Delete users

  When a user is deleted from your database, the user state is made inactive in the Salesforce.com.
- Password synchronization

  The basic configuration files for the Salesforce.com driver are capable of synchronizing passwords.

  When a user is newly created and provided with a password, the password is synchronized with Salesforce.com. If the password is not provided, a random password is generated for the user. You can use the command transformation policies to change the random password generation feature.

NOTE: Salesforce.com driver does not support the following:

- `dn-type` attributes
- Multivalued attributes. If multivalued attributes are added to the Identity Vault, only one of the values is synchronized with the Salesforce.com driver.

The following operations are supported on the Publisher channel:

- Add users
- Modify users

  If the IsActive attribute is set to **False**, the user is disabled in the Identity Vault.

2 Installing the Driver Files

You must install Salesforce.com driver on a server that has HTTP access to the Salesforce.com Web service with which the driver will communicate. The Salesforce.com driver can be installed on multiple systems and platforms. To verify the system requirement list, see the NetIQ Identity Manager Technical Information website (https://www.netiq.com/products/identity-manager/advanced/technical-information/).

By default, the Salesforce.com driver files are installed on the Identity Manager server at the same time as the Identity Manager engine. The installation program extends the Identity Vault's schema and installs the driver shim.

3 Creating a New Driver Object

After the Salesforce.com driver files are installed on the server where you want to run the driver (see Chapter 2, “Installing the Driver Files,” on page 13), you can create the driver in the Identity Vault. You do so by installing the driver packages or importing the driver configuration file and then modifying the driver configuration to suit your environment.

The following sections provide instructions to create the driver:

Creating the Driver Object in Designer

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

Importing the Current Driver Packages

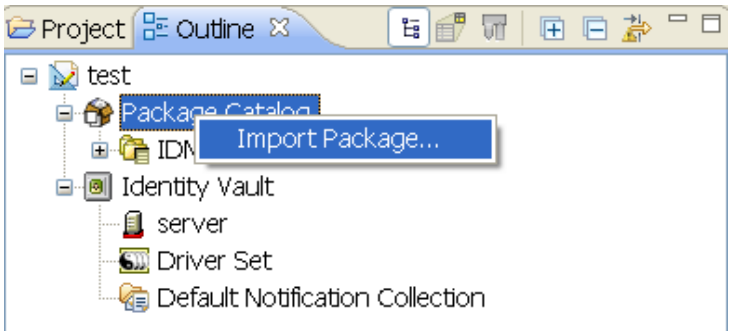
The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package 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 Salesforce 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 "Installing the Driver Packages" on page 16.

Installing the Driver Packages

1 In Designer, open your project.

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

The Salesforce.com driver is under the Enterprise category in the Palette.

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

4 Select the optional features to install for the Salesforce.com driver, then click **Next**.

The options are:

All options are selected by default. The options are:

Default Configuration: These packages contain the default configuration information for the Salesforce.com driver. Always leave this option selected.

Password Generation and Synchronization: This package contains the policies that allow the Salesforce.com driver to synchronize passwords to the Identity Vault. By default, it is not selected. For more information, see the NetIQ Identity Manager Password Management Guide.

Entitlements Support: These packages contain the policies and entitlements required to enable the driver for account creation and management with entitlements. For more information, see the *NetIQ Identity Manager Entitlements Guide*.

Data Collection: These packages contain the policies that enable the driver to collect data for reports. If you are using Identity Reporting, verify that this option is selected. For more information, see the NetIQ Identity Manager Entitlements Guide.

Account Tracking: These packages contain the policies that enables account tracking information for reports. If you are using Identity Reporting, verify that this option is selected. For more information, see the NetIQ Identity Reporting: User's Guide to Running Reports.

5 (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.

6 (Conditional) Fill in the following fields on the Common Settings page, then click **Next**:

The Common Settings page is displayed only if the Common Settings package is not installed already.

User Container: Select the Identity Vault container where the users are added if they don't already existing in the Identity Vault. This value becomes the default value 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.

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

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

Salesforce.com Login URL: Specify the login URL of Salesforce.com.

Salesforce.com Login ID: Specify the e-mail address used to login to Salesforce.com.

Ensure that you create a unique administrator user to be solely used by the Salesforce.com driver for authentication and specify that user in this parameter. If you specify the same user with which you login and administer Salesforce.com, the driver ignores changes on the Publisher channel (loopback detection).

Salesforce.com Login Password: Specify the authentication password to login to Salesforce.com.

Salesforce.com Security Token: Specify the security token for login account at Salesforce.com.

9 Fill in the following fields for the Remote Loader information, then click **Next**:

Connect To Remote Loader: Select **Yes** or **No** to determine if the driver will use the Remote Loader. For more information, see Configuring the Remote Loader and Drivers in the *NetIQ Identity Manager Setup Guide for Linux* or Configuring the Remote Loader and Drivers in the *NetIQ Identity Manager Setup Guide for Windows*.

If you select **No**, skip to Step 12. If you select **Yes**, use the following information to complete the configuration of the Remote Loader, then click **Next**:

Host Name: Specify the IP address or DNS name of the server where the Remote Loader is installed and running.

Port: Specify the port number for this driver. Each driver connects to the Remote Loader on a separate port. The default value is 8090.

Remote Loader Password: Specify a password to control access to the Remote Loader. It must be the same password that is specified as the Remote Loader password on the Remote Loader.

Driver Password: Specify a password for the driver to authenticate to the Identity Manager server. It must be the same password that is specified as the Driver Object Password on the Remote Loader.

10 (Conditional) On the Install Salesforce Account Tracking page, fill in the following fields for Account Tracking, 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 Salesforce.com Domain Name.

11 (Conditional) On the Install Salesforce Managed System Information page, fill in the following fields to define the ownership of Salesforce.com, 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.
- **Vendor:** Specify Salesforce.com as the vendor 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 Salesforce.com. 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 Salesforce.com. 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 Salesforce.com. 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 Salesforce.com.
- Environment: Select the type of environment the Salesforce.com provides. The options are as follows:
  - Development
  - Test
  - Staging
  - Production
  - Other

    If you select **Other**, you must specify a custom environment for the Salesforce.com.

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

13 After you have installed the driver, you can change the configuration for your environment. Proceed to “Configuring the Driver Object” on page 18.

or

If you do not need to configure the driver, continue with “Deploying the Driver Object” on page 19.

Configuring the Driver Object

There are many settings that can help you customize and optimize the driver. You should complete the following tasks to configure the driver:

- **Configure 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 Parameters

located on the Driver Configuration page. The Driver Parameters let you configure the Salesforce login information and security credentials, and other parameters associated with the Publisher channel.

- **Customize 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. For instructions, see Chapter 4, “Schema Mapping,” on page 23.

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.
4. After the driver is create in Designer, it must be deployed to the Identity Vault. Proceed to “Deploying the Driver Object” on page 19 to deploy the driver.

Deploying the Driver Object

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.

   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**.

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:

1. In Designer, open your project.
2. In the Modeler, right-click the driver icon 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 Salesforce.com driver shim.

For information about management tasks for the driver, see Chapter 7, "Managing the Driver," on page 31.

Activating the Driver

The Identity Manager driver for Salesforce.com driver is part of the Identity Manager Integration Module for Salesforce.

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 Salesforce.com 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.

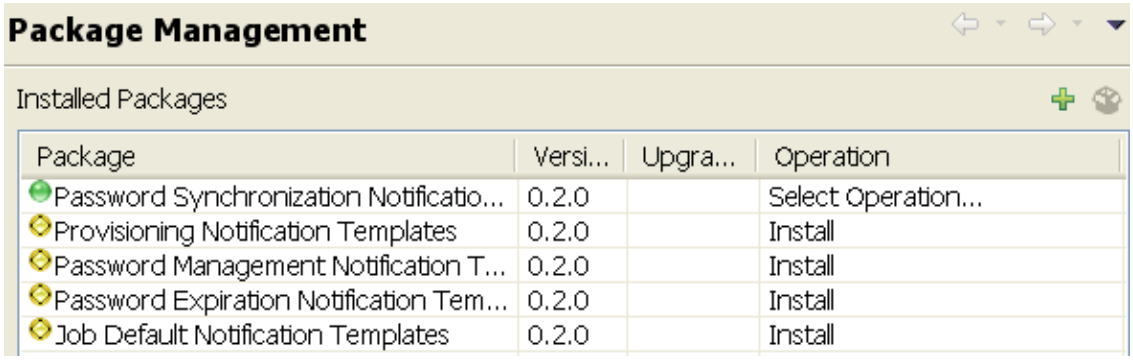
If driver activation has expired, the trace displays an error message indicating that you need to reactivate the driver to use it. For information on activation, refer to Activating Identity Manager in the NetIQ Identity Manager Overview and Planning Guide.

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**.

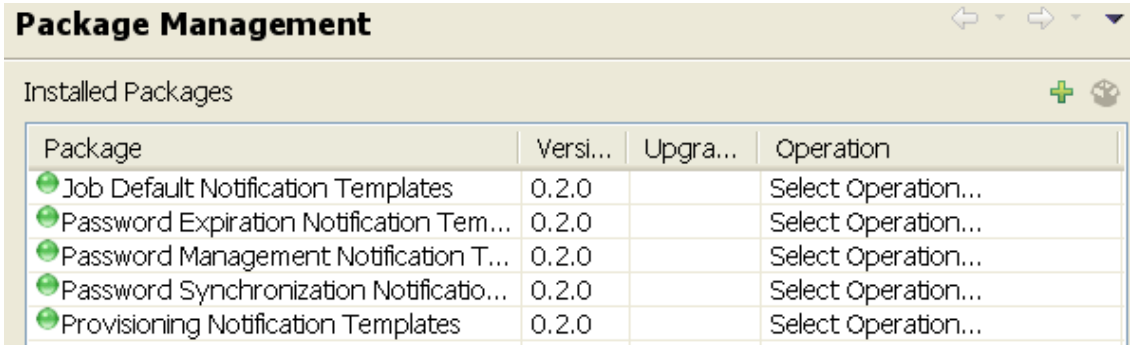
   This option is only displayed on drivers. By default, only the packages that can be installed on the selected driver are displayed.
5. Click **Apply** to install all of the packages listed with the Install operation.



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 Schema Mapping

Table 4-1 lists Identity Vault user attributes that are mapped to the Salesforce.com user attributes. The mappings listed in the table are default mappings. You can remap same-type attributes.

Table 4-1 *Mapped User Attributes when configured in the Salesforce.com*

Identity Vault - User	Salesforce.com - User
company	CompanyName
co	Country
Facsimile Telephone Number	Fax
GivenName	FirstName
Internet EMail Address	Email
	NOTE: In addition, the default policies map the Internet Email Address to the Salesforce.com username.
mobile	MobilePhone
OU	Department
Physical Delivery Office Name	City
Postal Code	PostalCode
S	State
SA	Street
Surname	LastName
Telephone Number	Phone
Title	Title
workforceID	EmployeeNumber

5 Upgrading an Existing Driver

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

Supported Upgrade Paths

You can upgrade 4.0 version of the Salesforce.com driver to 4.1.0 version. For detailed instructions, see *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

What's New in Version in 4.1.0

Identity Manager 4.8 provides support for MapDB 3.0.5. To ensure that your driver works correctly with Identity Manager 4.8 engine, see "Working with MapDB 3.0.5" on page 25.

Working with MapDB 3.0.5

NetIQ recommends that you review the following sections before upgrading your driver to work with Identity Manager 4.8 engine:

Understanding Identity Manager 4.8 Engine Support for Driver Versions

- Drivers shipped with Identity Manager 4.8 are compatible with Identity Manager 4.8 Engine or Remote Loader. You must perform the following actions to complete the driver upgrade:
  1. Upgrade the Identity Manager Engine.
  2. (Conditional) Upgrade the Remote Loader.
  3. Upgrade the driver.
  4. Manually remove the MapDB state cache files from the Identity Vault's DIB directory. For more information, see "Manually Removing the MapDB Cache Files" on page 26.
- Drivers shipped before Identity Manager 4.8 are not compatible with Identity Manager 4.8 Engine or Remote Loader.

- Drivers shipped with Identity Manager 4.8 are not backward compatible with Identity Manager 4.7.x Engine or Remote Loader.
- Drivers shipped with Identity Manager 4.8 are not backward compatible with Identity Manager 4.6.x Engine or Remote Loader.

Manually Removing the MapDB Cache Files

The Identity Manager engine upgrade process removes the existing MapDB driver work cache files (`dx*`) from the Identity Vault's DIB directory (`/var/opt/novell/eDirectory/data/dib` or `C:\Novell\NDS\DIBFiles`). You must manually remove the existing MapDB state cache files for the driver after upgrading the driver. The MapDB state cache files for the JDBC driver are represented in the following formats:

- `<Salesforce Driver Name>.*`
- `<Salesforce Driver Name>`

For example, `<Salesforce Driver>.p`, `<Salesforce Driver>.t`, or `Salesforce Driver1`

This action ensures that your driver works correctly with Identity Manager 4.8 engine.

Upgrading the Driver

The driver upgrade process involves upgrading the installed driver packages and updating the existing driver files. These are independent tasks and can be separately planned for a driver. For example, you can update the driver packages and choose not to update the driver files at the same time. However, you are recommended to complete all the update steps within a short amount of time to ensure that the driver has the latest updates.

- "Upgrading the Installed Packages" on page 26
- "Applying the Driver Patch" on page 27

Before starting the upgrade process, ensure that you have taken a back-up of the current driver configuration.

Upgrading the Installed Packages

1. Download the latest available packages.

   To configure Designer to automatically read the package updates when a new version of a package is available, click **Windows > Preferences > NetIQ > Package Manager > Online Updates** in Designer. However, if you need to add a custom package to the Package Catalog, you can import the package `.jar` file. For detailed information, see the Upgrading Installed Packages in *NetIQ Designer for Identity Manager Administration Guide*.

2. Upgrade the installed packages.

   2a Open the project containing the driver.

   2b Right-click the driver for which you want to upgrade an installed package, then click **Driver > Properties**.

   2c Click **Packages**.

   If there is a newer version of a package, there is check mark displayed in the Upgrades column.

   2d Click **Select Operation** for the package that indicates there is an upgrade available.

2e From the drop-down list, click **Upgrade**.

2f Select the version that you want to upgrade to, then click **OK**.

NOTE: Designer lists all versions available for upgrade.

2g Click **Apply**.

2h (Conditional) Fill in the fields with appropriate information to upgrade the package, then click **Next**.

Depending on which package you selected to upgrade, you must fill in the required information to upgrade the package.

2i Read the summary of the packages that will be installed, then click **Finish**.

2j Review the upgraded package, then click **OK** to close the Package Management page.

For detailed information, see the Upgrading Installed Packages in *NetIQ Designer for Identity Manager Administration Guide*.

Applying the Driver Patch

The driver patch updates the driver files. You can install the patch as a `root` or `non-root` user.

Prerequisites

Before installing the patch, complete the following steps:

1. Take a back-up of the current driver configuration.
2. (Conditional) If the driver is running with the Identity Manager engine, stop the Identity Vault and the driver instance.
3. (Conditional) If the driver is running with a Remote Loader instance, stop the Remote Loader instance and the driver instance.
4. In a browser, navigate to the NetIQ Patch Finder Download Page.
5. Under **Patches**, click **Search Patches**.
6. Specify **Identity Manager *nn* Salesforce Driver nn** in the search box.
7. Download and unzip the contents of the patch file to a temporary location on your server.

Applying the Patch as a Non-Root User

In a root installation, the driver patch installs the driver files RPMs in the default locations on Linux. On Windows, you need to manually copy the files to the default locations.

1. Update the driver files:
   - **Linux:** Log in to your server as `root` and run the following command in a command prompt:

     `rpm -Uvh <Driver Patch File Temporary Location>/linux/novell-DXMLSForce.rpm`

     For example, `rpm -Uvh <IDM45_SF_410.zip>/linux/novell-DXMLSForce.rpm`
   - **Windows:** Navigate to the `<Extracted Driver Patch File Temporary Location>\windows` folder and copy the `SalesforceShim.jar` file to `<IdentityManager installation>\NDS\lib` or `<IdentityManager installation>\RemoteLoader\<architecture>\lib` folder.

2 (Conditional) If the driver is running locally, start the Identity Vault and the driver instance.

   For example, open a command prompt on Linux and run `ndsmanage startall`

3 (Conditional) If the driver is running with Remote Loader, start the Remote Loader and driver instances.

Applying the Patch as a Non-Root User

1 Verify that <*non-root eDirectory location*>/rpm directory exists and contains the file, _db.000.

   The _db.000 file is created during a non-root installation of the Identity Manager engine. Absence of this file might indicate that Identity Manager is not properly installed. Reinstall Identity Manager to correctly place the file in the directory.

2 To set the root directory to non-root eDirectory location, enter the following command in the command prompt:

   ROOTDIR=<*non-root eDirectory location*>

   This will set the environmental variables to the directory where eDirectory is installed as a non-root user.

3 Download the patch and untar or unzip the downloaded file.

4 To install the driver files, enter the following command:

```
rpm --dbpath $ROOTDIR/rpm -Uvh --relocate=/usr=$ROOTDIR/opt/novell/eDirectory
--relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/eDirectory=$ROOTDIR/opt/
novell/eDirectory --relocate=/opt/novell/dirxml=$ROOTDIR/opt/novell/dirxml --
relocate=/var=$ROOTDIR/var --badreloc --nodeps --replacefiles <rpm-location>
```

   For example, to install the Salesforce driver RPM, use this command:

```
rpm --dbpath $ROOTDIR/rpm -Uvh --relocate=/usr=$ROOTDIR/opt/novell/eDirectory
--relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/eDirectory=$ROOTDIR/opt/
novell/eDirectory --relocate=/opt/novell/dirxml=$ROOTDIR/opt/novell/dirxml --
relocate=/var=$ROOTDIR/var --badreloc --nodeps --replacefiles /home/user/
novell-DXMLSForce.rpm
```

6 Securing Communication

If the remote Web service you are accessing allows HTTPS connections, you can configure the driver to take advantage of this increased security.

IMPORTANT: Only certificates from Java keystore are accepted. So, make sure that the keystore of the certificates is a Java keystore.

The Subscriber channel sends information from the Identity Vault to Salesforce.com. To establish a secure connection for the Subscriber channel, you need a trust store containing a certificate issued by the certificate authority that signed the server's certificate.

Import this certificate into a trust store using Java's keytool. For more information on keytool, see Keytool - Key and Certificate Management Tool (http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html).

1. Import the certificate into your trust store or create a new trust store by entering the following command at the command prompt:

   ```
   keytool -import -file name_of_cert_file -trustcacerts -noprompt -keystore
   filename -storepass password
   ```

   For example:

   ```
   keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore
   dirxml.keystore -storepass novell
   ```

2. Configure the Subscriber channel to use the trust store you created in Step 1:
   - **2a** In iManager, in the **Roles and Tasks** view, click **Identity Manager > Identity Manager Overview**.
   - **2b** Locate the driver set containing the Salesforce.com driver, then click the driver's icon to display the Identity Manager Driver Overview page.
   - **2c** On the Identity Manager Driver Overview page, click the driver's icon again, then scroll to **Subscriber Settings**.
   - **2d** In the **Keystore File** setting, specify the path to the trust store you created in Step 1.
3. Click **Apply**, then click **OK**.

7 Managing the Driver

As you work with the Salesforce.com 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 Troubleshooting the Driver

You can log Identity Manager events by using NetIQ Event Auditing Service. Using this service in combination with the driver log level setting provides you with tracking control at a very granular level.

This section contains the following information on error messages:

Driver Shim Errors

The following identifies errors that might occur in the core driver shim. Error messages that contain a numerical code can have various messages, depending on the application or Web service.

307 Temporary Redirect

Source:	The status log or DSTrace screen.
Explanation:	The Subscriber channel attempted to send data to the application or Web service but received a 307 Temporary Redirect response.
Possible Cause:	The Web service is not available.
Action:	The Subscriber waits for a period of time (usually 30 seconds) and tries again.
Level:	Retry

408 Request Timeout

Source:	The status log or DSTrace screen.
Explanation:	The Subscriber channel attempted to send data to the application or Web service but received a 408 Request Timeout response.
Possible Cause:	The Web service or application is busy.
Action:	The Subscriber waits for a period of time (usually 30 seconds) and tries again.
Level:	Retry

503 Service Unavailable

Source:	The status log or DSTrace screen.
Explanation:	The Subscriber channel attempted to send data to the application or Web service but received a 503 Service Unavailable response.
Possible Cause:	The Web service or application is down.
Action:	The Subscriber waits for a period of time (usually 30 seconds) and tries again.

Level: Retry

504 Gateway Timeout

Source: The status log or DSTrace screen.

Explanation: The Subscriber channel attempted to send data to the application or Web service but received a 504 Gateway Timeout response.

Possible Cause: The gateway is down.

Action: The Subscriber waits for a period of time (usually 30 seconds) and tries again.

Level: Retry

200-299 Messages

Source: The HTTP server.

Explanation: The messages in the 200-299 range indicate success.

Action: No action required.

Level: Success

Other HTTP Errors Messages

Source: The status log or DSTrace screen.

Explanation: Other numerical error codes result in an error message containing that code and the message provided by the HTTP server. In most cases, the driver continues to run, and the command that caused the error isn't retried.

Possible Cause: There are multiple causes for the different errors.

Action: See RFC 2616 (http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html) for a list of all HTTP error codes and explanations.

Level: Error

Problem communicating with HTTP server. Make sure the server is running and accepting requests.

Source: The status log or DSTrace screen.

Explanation: The Subscriber channel received an IOException while communicating or attempting to communicate with the HTTP server.

Possible Cause: The HTTP server is not running.

Possible Cause: The HTTP server is overloaded.

Possible Cause: There are firewall restrictions blocking access to the HTTP server.

Possible Cause: The URL provided in the Subscriber configuration is not correct. See "Driver Parameters" on page 39.

Action: Start the HTTP server.

Action: Remove services, if the HTTP server is overloaded.

Action: Change the firewall restrictions to allow access to the HTTP server.

Level: Retry

The HTTP/Salesforce.com driver doesn’t return any application schema by default.

Source: The status log or DSTrace screen.

Explanation: The driver is not returning any application schema, but the driver continues to run.

Possible Cause: The Identity Manager engine calls the DriverShim.getSchema() method of the driver, and the driver is not using the SchemaReporter customization.

Action: A Java class needs to be written that implements the SchemaReporter interface, and the driver needs to be configured to load the class as a Java extension.

Level: Warning

Subscriber.execute() was called but the Subscriber was not configured correctly. The command was ignored.

Source: The status log or DSTrace screen.

Explanation: The Subscriber channel of the driver isn’t initialized properly. The driver continues to run but displays this message each time an event is received by the Subscriber channel.

Possible Cause: An improperly formatted driver configuration.

Action: Configure the driver correctly. See Chapter 4, “Schema Mapping,” on page 23 for more information.

Action: Clear the Subscriber’s filter so it doesn’t receive commands.

Level: Warning

pubHostPort must be in the form host:port

Source: The status log or DSTrace screen.

Explanation: The driver cannot communicate.

Possible Cause: An error occurred with the Publisher channel configuration.

Action: Review the Publisher channel parameters to verify that both a valid host and a valid port number are provided.

Level: Fatal

MalformedURLException

Source: The status log or the DSTrace screen.

Explanation: There is a problem with the format of the URL.

Possible Cause: The URL supplied in the Subscriber channel parameters isn’t in a valid URL format.

Action: Change the URL to a valid format. .

Level: Fatal

Multiple Exceptions

Source: The status log or the DSTrace screen.

Explanation: The HTTP listener fails to properly initialize.

Possible Cause: There are a variety of reasons for this error.

Action: Check your Publisher settings to make sure you have specified a port that is not already in use and that the other Publisher settings are correct.

Level: Fatal

HTTPS Hostname Wrong: Should Be ...

Source: The status log or the DSTrace screen.

Explanation: An SSL handshake failed on the Subscriber channel.

Possible Cause: The subject presented with the server certificate doesn’t match the IP address or hostname given in the HTTPS URL.

Action: Use a DNS hostname rather than an IP address in the URL.

Level: Retry

The DirXML-DriverStorage Attribute Does Not Change With the Latest Polling Interval

The Salesforce.com doesn’t frequently change the timestamp. It keeps sending the same timestamp for some time, so the new values are not updated in the DirXML-DriverStorage attribute of the Identity Manager engine. This causes the previous updates to keep replaying for some time. However, it doesn't cause any loss of events.

Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it 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*.

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the Salesforce.com 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 a Designer icon.

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:

Driver Module

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

Java: Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally.

The Java class name is:

```
com.novell.nds.dirxml.driver.salesforce.SFDriverShim
```

Native: This option is not used with the Salesforce.com driver.

Connect to Remote Loader: Used 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.

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.

Authentication

The authentication section stores the information required to authenticate to the connected system.

Authentication ID: This option is not used with the Salesforce.com driver.

Authentication Context: This option is not used with the Salesforce.com driver.

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 host name 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 Identity Manager 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: This option is not used with the Salesforce.com driver.

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.

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.

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

Salesforce.com Login URL: Specify the URL of the Salesforce.com Login Server based on your choice of Salesforce.com WSDL.

The default URL is https://www.salesforce.com/services/Soap/u/18.0.

Salesforce.com Login ID: Specify the Login ID of the Salesforce.com administrator.

Ensure that you create a unique administrator user to be solely used by the Salesforce.com driver for authentication and specify that user in this parameter. If you specify the same user with which you login and administer Salesforce.com, the driver ignores changes on the Publisher channel (loopback detection).

Salesforce.com Login Password: Specify the password for the Salesforce.com administrator.

If you need to clear the password, select **Remove existing password**, then click **Apply**.

Salesforce.com Security Token: Specify the security token for your login account at Salesforce.com.

Proxy host and port: When an HTTP proxy is used, specify the host address and the host port. For example: 192.10.1.3:18180.

Set Proxy Authentication parameters: Select **Show** to display the proxy authentication parameters.

- **Proxy User ID:** Specify the username of the proxy user for authentication. Leave the field blank for anonymous authentication.
- **Proxy User Password:** Specify the password of the proxy user, if proxy user authentication is used.

Truststore File: Specify the name and path of the keystore file containing the trusted certificates used when the remote server is configured to provide server authentication. For example: `c:\security\truststore`. Leave this field empty when server authentication is not used.

NOTE: A Salesforce.com client calling the Web service in the Publisher channel must specify a URL ending with a slash. For example, *http://1.1.1.1:9095/*. Without a context path (the slash), the driver does not process the request received.

Publisher Settings

Publisher Channel Enabled: Select **Enable** to enable the Publisher connection. The following options are displayed to configure the Publisher channel.

- **Poll Interval (seconds):** Specify how often the Publisher channel polls for the unprocessed IDs. The default value is 60 seconds.
- **Publisher Heartbeat Interval:** Specifies how often, in minutes, the driver shim contacts the Identity Manager engine when there has not been any traffic during the interval time. The default value is 1 minute. Specify 0 to disable the heartbeat.

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 Salesforce.com driver includes several predefined GCVs. You can also add your own 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-click the driver set icon , then click **Properties > GCVs**.

The GCVs are divided into the following categories:

Driver Configuration

The following GCVs control the configuration of the Salesforce.com driver.

Salesforce.com Default Profile ID: This option is used for creating new users when no actual value has been provided in the current transaction.

The **ProfileID** is a 15 character code that uniquely identifies a user profile tied to your Salesforce account.

To find **ProfileID** for any given profile in Salesforce, go to **Setup > Manage Users > Profiles**, click the appropriate profile and select the URL. A standard Salesforce 15 character code displays in the URL. Copy the 15 character code and use it as your **Salesforce.com Default Profile ID**.

Default Time Zone: Specifies the default time zone for users created in the salesforce.com if time zone is not specified during the initial add event.

In order to add additional locations, edit this GCV option and add additional enumeration values. The value part of the field that this GCV represents is named by using region and key city, according to ISO standards.

Default E-Mail Encoding: This option specifies the e-mail encoding information of the users created in the salesforce.com if e-mail encoding is not provided during the initial add event. In order to add additional e-mail encodings, check with salesforce.com to know the correct value for this field, then edit the option to add additional enumeration values.

Default Locale: This option specifies the default locale information of the users created in the salesforce.com if it is not provided during the initial add event.

In order to add additional locales, edit this option and add additional enumeration values. The value part of the field that this GCV represents is built according to the language, and country if necessary, using two-letter ISO codes.

For example, en_US. It is built from the 2 letter language code described in the ISO 639-1, followed by an underscore sign, followed by the 2 letter country code described in the ISO 3166-1.

Default Language: Specify the default language of the users created in the salesforce.com if it is not provided during the initial add event.

In order to add additional languages, edit the option and add additional enumeration values. The value part of the field that this GCV represents is built according to the language, and country if necessary, using two-letter ISO codes.

For example, en_US, built from the 2 letter language code described in the ISO 639-1, followed by an underscore sign, followed by the 2 letter country code described in the ISO 3166-1.

Password Synchronization

Use the following GCVs to configure the driver to synchronize passwords to the Identity Vault. For more information, see NetIQ Identity Manager Password Management Guide.

Connected system name: Specify the name of the connected system. This name is used for password sync failure notifications.

Notify the user of password synchronization failure via e-mail: Select this option if you want to notify the salesforce.com user through e-mail.

Application accepts passwords from Identity Manager: Select whether the application accepts passwords from Identity Manager. Selecting this option to True allows the passwords to flow from the Identity Manager data store to connected system.

Publisher channel password options (not supported by this driver): Leave the setting unchanged. The Salesforce.com driver doesn't support password synchronization on the Publisher channel, this option should remain set to false.

Entitlements

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

Entitlements Configuration

Use Entitlements to Control Salesforce Accounts?: Select **True** to enable the driver to manage user accounts based on the driver's defined entitlements. Select **Fals**e to disable management of user accounts based on the entitlements.

- **On Revoke?:** Select the action to take when a user account entitlement is revoked. There is only one option, **Disable User,** which is selected by default.

Use Group Entitlement: Enables the Group entitlement that is included with the driver. Select **True** to enable this entitlement.

Use Role Entitlement: Enables the Role entitlement that is included with the driver. Select **True** to enable this entitlement.

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.

Parameter Format

Format for Account entitlement: Specifies the parameter format that the entitlement agent uses when granting this entitlement. The options are **Identity Manager 4** or **Legacy**.

Format for Role entitlement: Specifies the parameter format that the entitlement agent uses when granting this entitlement. The options are **Identity Manager 4** or **Legacy**.

Format for Responsibility entitlement: Specifies the parameter format that the entitlement agent uses when granting this entitlement. The options are **Identity Manager 4** or **Legacy**.

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: If **Yes**, it enables the data collection for the driver through 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: If **Yes**, it allows data collection by Data Collection Service for the user accounts.

Allow data collection from groups: If **Yes**, it allows data collection by Data Collection Service for the groups.

Allow data collection from roles: If **Yes**, it allows data collection by Data Collection Service for roles.

Role Mapping

Identity Applications allow you to map business roles with IT roles. For more information, see the NetIQ Identity Manager - Administrator's Guide to the Identity Applications

Enable role mapping: If **Yes**, the driver is visible to Identity Applications.

Allow mapping of user accounts: If **Yes**, it allows mapping of user accounts in Identity Applications. An account is required before a role or responsibility can be granted to it through Identity Applications.

Allow mapping of groups: If **Yes**, it allows mapping of groups in Identity Applications.

Allow mapping of roles: If **Yes**, it allows mapping of groups in Identity Applications.

Resource Mapping

Identity Applications allow you to map resources to users. For more information, see the NetIQ Identity Manager - User's Guide to the Identity Applications.

Enables resource mapping: If **Yes**, the driver is visible to Identity Applications.

Allow mapping of user accounts: If **Yes**, it allows mapping of user accounts in Identity Applications. An account is required before a role or responsibility can be granted to it.

Allow mapping of groups: If **Yes**, it allows mapping of groups in Identity Applications.

Allow mapping of roles: If **Yes**, it allows mapping of roles in Identity Applications.

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.

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

Password Generation

Synchronize Identity Vault Password: Set this option to **Yes** to establish common password synchronization. Change it to **No** to ignore the Identity Vault password.

Enable Password Generation Triggers: Set this option to **Yes** to generate password for new accounts.

New Account: If **On**, the driver generates password for new accounts.

Account Enable: If **On**, the driver generates a new password every time the account is enabled.

Account Disable: If **On**, the driver generates a new password every time the account is disabled.

Password Generation Method: If the universal password synchronization or distribution password is not set for a user account, you need to set an initial password for the user. Specify whether to use an attribute of a user account for setting up an initial password or to use a randomly generated password. If the user account is going to use SAML for authentication, select **Random** for this option. Otherwise, select **Attribute Value**.

Account Tracking

Account tracking is part of Identity Reporting. For more information, see the NetIQ Identity Reporting: User's Guide to Running Reports.

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 Salesforce.com Domain Name.

Object Class: Adds the object class to track. Class names must be in the application namespace.

Identifiers: Adds the account identifier attributes. Attribute names must be in the application namespace.

Status attribute: Is the name of the attribute in the application namespace to represent the account status.

Status active value: Is the value of the status attribute that represents an active state.

Status inactive value: Is the value of the status attribute that represents an inactive state.

Subscription default status: Specifies the default status that the policies assume when an object is subscribed to the application and the status attribute is not set in the Identity Vault.

Publication default status: Specifies the default status that the policies assume when an object is published to the Identity Vault and the status attribute is not set in the application.

Managed System Information

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

- "General Information" on page 44
- "System Ownership" on page 45
- "System Classification" on page 45
- "Connection and Miscellaneous Information" on page 45

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 Salesforce.com 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 Trace Levels

The driver supports the following trace levels:

Table B-1 *Supported Trace Levels*

Level	Description
0	No debugging
1-2	Identity Manager messages. Higher trace levels provide more detail.
3	Previous level plus driver parameters, Remote Loader, driver shim, and driver connection messages
5	Previous level plus driver status log, driver security, driver schema, driver communication details, request and response XML, Salesforce API calls

For information about setting driver trace levels, see “Viewing Identity Manager Processes” in the *NetIQ Identity Manager Driver Administration Guide*.