

## Driver for Salesforce.com Implementation Guide

# Novell® Identity Manager

**4.0**

October 15, 2010

[www.novell.com](http://www.novell.com)



## Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2010 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

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

## **Novell Trademarks**

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

## **Third-Party Materials**

All third-party trademarks are the property of their respective owners.



# Contents

<b>About This Guide</b>	<b>7</b>
<b>1 Understanding the Salesforce.com Driver</b>	<b>9</b>
1.1 Driver Concepts	9
1.1.1 Data Management	9
1.1.2 How the Driver Works	10
1.1.3 Understanding Operation Data	10
1.2 Support for Standard Driver Features	11
1.2.1 Local Platforms	11
1.2.2 Remote Platforms	11
1.2.3 Supported Operations	11
<b>2 Installing the Driver Files</b>	<b>13</b>
<b>3 Creating a New Driver</b>	<b>15</b>
3.1 Creating the Driver in Designer	15
3.1.1 Importing the Current Driver Packages	15
3.1.2 Installing the Driver Packages	16
3.1.3 Configuring the Driver	18
3.1.4 Deploying the Driver	18
3.1.5 Starting the Driver	19
3.2 Creating the Driver in iManager	19
3.2.1 Importing the Driver Configuration File	19
3.2.2 Configuring the Driver	21
3.2.3 Starting the Driver	22
3.3 Activating the Driver	22
<b>4 Customizing the Driver</b>	<b>23</b>
4.1 Creating XSLT Style Sheets	23
4.2 Managing Operation Data	23
4.2.1 Using Operation Data to Specify XML to Be Returned on the Result	23
4.3 Managing the Driver	24
4.4 Schema Mapping	24
<b>5 Securing Communication</b>	<b>25</b>
5.1 Configuring the Subscriber Channel	25
<b>6 Managing the Driver</b>	<b>27</b>
<b>7 Troubleshooting the Driver</b>	<b>29</b>
7.1 Driver Shim Errors	29
7.2 Troubleshooting Driver Processes	32

<b>A</b>	<b>Driver Properties</b>	<b>33</b>
A.1	Driver Configuration . . . . .	33
A.1.1	Driver Module . . . . .	33
A.1.2	Driver Object Password . . . . .	34
A.1.3	Authentication . . . . .	34
A.1.4	Startup Option . . . . .	34
A.1.5	Driver Parameters . . . . .	35
A.2	Global Configuration Values . . . . .	35
A.2.1	Driver Configuration . . . . .	36
A.2.2	Password Synchronization . . . . .	37

# About This Guide

This guide explains how to install and configure the Identity Manager 4.0 Driver for Salesforce.com. The guide includes the following information:

- ♦ Chapter 1, “Understanding the Salesforce.com Driver,” on page 9
- ♦ Chapter 2, “Installing the Driver Files,” on page 13
- ♦ Chapter 3, “Creating a New Driver,” on page 15
- ♦ Chapter 4, “Customizing the Driver,” on page 23
- ♦ Chapter 5, “Securing Communication,” on page 25
- ♦ Chapter 6, “Managing the Driver,” on page 27
- ♦ Chapter 7, “Troubleshooting the Driver,” on page 29
- ♦ Appendix A, “Driver Properties,” on page 33

## Audience

This guide is for Identity Manager and Salesforce.com administrators who are using the Identity Manager Driver for Salesforce.com. You should also have an understanding of SOAP, HTML, and HTTP protocols.

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to [www.novell.com/documentation/feedback.html](http://www.novell.com/documentation/feedback.html) and enter your comments there.

## Documentation Updates

For the most recent version of this document, see the [Identity Manager 4.0 Drivers Documentation Web site \(http://www.novell.com/documentation/idm40drivers/index.html\)](http://www.novell.com/documentation/idm40drivers/index.html).

## Additional Documentation

For information on Identity Manager, see the [Identity Manager Documentation Web site \(http://www.novell.com/documentation/idm40\)](http://www.novell.com/documentation/idm40).





# Understanding the Salesforce.com Driver

# 1

Identity Manager 4.0 offers automatic provisioning and synchronization of users to cloud applications. The new Salesforce.com driver for Novell Identity Manager can seamlessly provision and de-provision users to 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 is a Subscriber channel only driver and 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 an Identity Vault with Salesforce.com.

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

- ♦ [Section 1.1, “Driver Concepts,” on page 9](#)
- ♦ [Section 1.2, “Support for Standard Driver Features,” on page 11](#)

## 1.1 Driver Concepts

This section contains the following information:

- ♦ [“Data Management” on page 9](#)
- ♦ [“How the Driver Works” on page 10](#)

### 1.1.1 Data Management

The Salesforce.com driver communicates with the 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” on page 9](#)
- ♦ [“XML” on page 10](#)
- ♦ [“HTTP” on page 10](#)

#### 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.

---

### 1.1.2 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's output transformation stylesheet translates the XDS to the Salesforce.com API represented as XML.

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

Salesforce.com processes the request, and returns a response to the driver shim. The input transformation style sheet processes the response, converting it into appropriate XDS that is reported back to the Identity Manager engine.

### 1.1.3 Understanding Operation Data

The driver shim applies special handling to Subscriber commands based on an XML element embedded in the command, which appears in the driver shim as `<operation-data>`. The `<operation-data>` element is used to match commands with the responses they generate, which can be useful for creating associations.

The `<operation-data>` element is added to the command from one of the Subscriber channel policies or in the output transformation stylesheet. The driver shim removes the `<operation-data>` element from the command before it is sent to the application, and restores the `<operation-data>` element to the resulting response.

By default, when the `<operation-data>` element is restored on the response, it is appended as a child element of the root node. This can be overridden by providing one or more `parent-node-n` attributes to the `<operation-data>` element, where *n* is a number beginning with 1 that is incremented for each parent specifier you want to provide. The driver shim examines the operation data node, looking for `parent-node-n` attributes. If attributes are found, each is tried in turn and if the named node exists, the node is used as the parent for the operation data on the response.

To see how the `<operation-data>` element works with the style sheets, see [Section 4.2, “Managing Operation Data,” on page 23](#).

## 1.2 Support for Standard Driver Features

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

- ♦ [Section 1.2.1, “Local Platforms,” on page 11](#)
- ♦ [Section 1.2.2, “Remote Platforms,” on page 11](#)
- ♦ [Section 1.2.3, “Supported Operations,” on page 11](#)

### 1.2.1 Local Platforms

A local installation is an installation of the driver on the Metadirectory server. The Salesforce.com driver can be installed on the operating systems supported for the Metadirectory server.

For information about the operating systems supported for the Metadirectory server, see “[Metadirectory Server](#)” in “[System Requirements](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

### 1.2.2 Remote Platforms

The Salesforce.com driver can use the Remote Loader service to run on a server other than the Metadirectory server. The Salesforce.com driver can be installed on the operating systems supported for the Remote Loader.

For information about the supported operating systems, see “[Remote Loader](#)” in “[System Requirements](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

### 1.2.3 Supported Operations

The basic configuration files for the Salesforce.com driver are capable of performing the following operations.

- ♦ 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 the Salesforce.com. If the password is not provided, a random password is generated for the user. 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.
-

# Installing the Driver Files

# 2

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 “[System Requirements](#)” in the *Identity Manager 4.0 Integrated Installation Guide*.

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



# Creating a New Driver

# 3

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:

- ♦ [Section 3.1, “Creating the Driver in Designer,” on page 15](#)
- ♦ [Section 3.2, “Creating the Driver in iManager,” on page 19](#)
- ♦ [Section 3.3, “Activating the Driver,” on page 22](#)

## 3.1 Creating the Driver in Designer

You create the Salesforce.com driver 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.

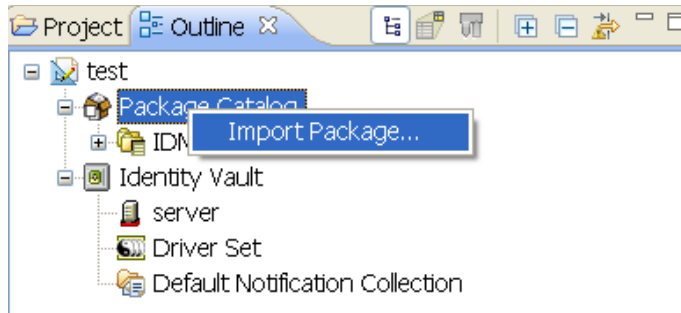
- ♦ [Section 3.1.1, “Importing the Current Driver Packages,” on page 15](#)
- ♦ [Section 3.1.2, “Installing the Driver Packages,” on page 16](#)
- ♦ [Section 3.1.3, “Configuring the Driver,” on page 18](#)
- ♦ [Section 3.1.4, “Deploying the Driver,” on page 18](#)
- ♦ [Section 3.1.5, “Starting the Driver,” on page 19](#)

### 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 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 [Section 3.1.2, “Installing the Driver Packages,”](#) on page 16.

### 3.1.2 Installing the Driver Packages

**1** In Designer, open your project.

**2** 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*.

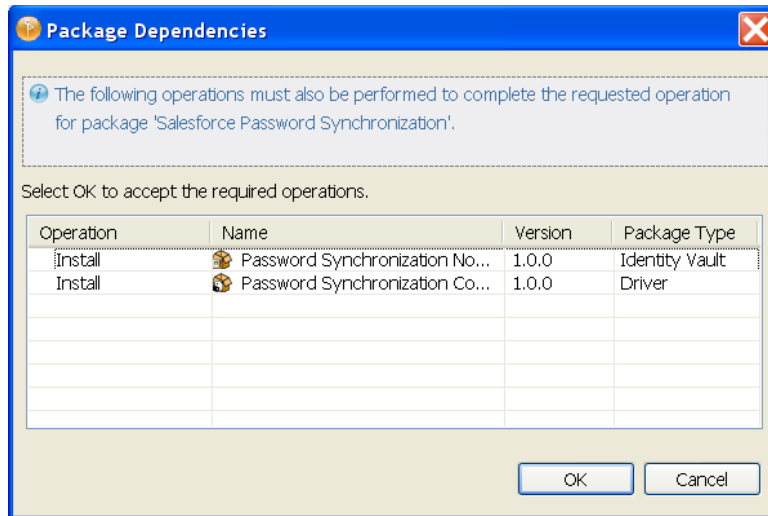
**4** Select the optional features to install for the Salesforce.com driver. The options are:

**Salesforce Password Synchronization:** This package contains the policies that allow the Salesforce.com driver to synchronize password to the Identity Vault. By default, it is not selected. For more information, see the [Identity Manager 4.0 Password Management 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 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:
 

**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.

**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 Click *Next*.
- 10 Fill in the following fields for Remote Loader information:
 

**Connect To Remote Loader:** Select *Yes* or *No* to determine if the driver will use the Remote Loader. For more information, see the [Identity Manager 4.0 Remote Loader Guide](#).

If you select *No*, skip to [Step 11](#). If you select *Yes*, use the following information to complete the configuration of the Remote Loader:

**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 Metadirectory server. It must be the same password that is specified as the Driver Object Password on the Remote Loader.
- 11 Click *Next*.
- 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 [Section 3.1.3, “Configuring the Driver,” on page 18.](#)
- or
- If you do not need to configure the driver, continue with [Section 3.1.4, “Deploying the Driver,” on page 18.](#)

### 3.1.3 Configuring the Driver


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.
- 4 After the driver is created in Designer, it must be deployed to the Identity Vault. Proceed to [Section 3.1.4, “Deploying the Driver,” on page 18](#) to deploy the driver.

### 3.1.4 Deploying the Driver

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

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver 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.
- 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:

**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 6, “Managing the Driver,” on page 27](#).

## 3.2 Creating the Driver in iManager

You create Salesforce.com driver by importing the driver's configuration file and then modifying the configuration to suit your environment. After you've created and configured the driver, you need to start it.

- ♦ [Section 3.2.1, “Importing the Driver Configuration File,” on page 19](#)
- ♦ [Section 3.2.2, “Configuring the Driver,” on page 21](#)
- ♦ [Section 3.2.3, “Starting the Driver,” on page 22](#)

### 3.2.1 Importing the Driver Configuration File

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

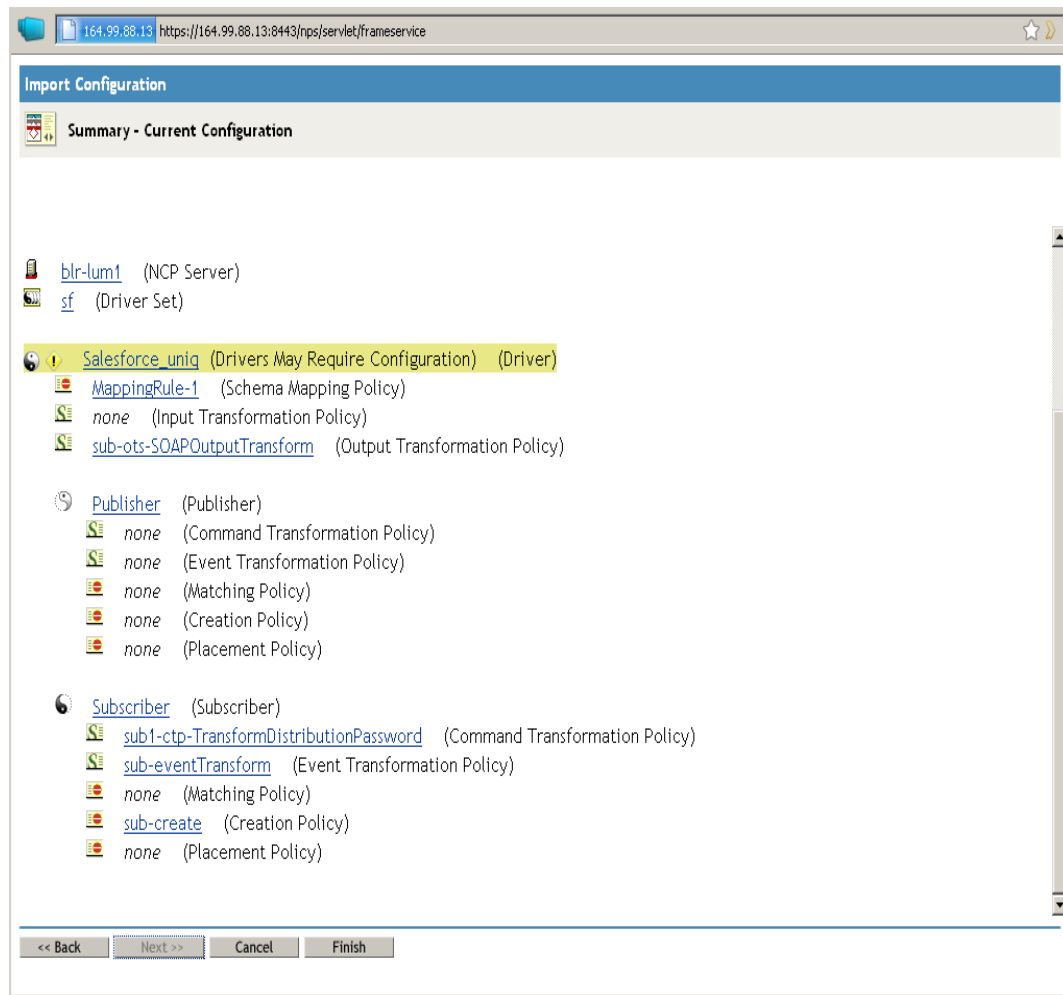
**2** In the Administration list, click *Import Configuration* to launch the Import Configuration Wizard.

**3** Follow the wizard prompts, filling in the requested information (described below) until you reach the Summary page.

Prompt	Description
Where do you want to place the new driver?	You can add the driver to an existing driver set, or you can create a new driver set and add the driver to the new set. If you choose to create a new driver set, you are prompted to specify the name, context, and server for the driver set.

Prompt	Description
Import a configuration into this driver set	<p>Use the default option, <i>Import a configuration from the server (.XML file)</i>.</p> <p>In the <i>Show</i> field, select <i>Identity Manager 3.6.1 configurations</i>.</p> <p>In the <i>Configurations</i> field, select the select the <code>SALESFORCE-IDM3_6_0-V1.xml</code> file.</p>
Driver Name	Type a name for the driver. The name must be unique within the driver set.
Driver is Local/Remote	Select <i>Local</i> if this driver will run on the Metadirectory server without using the Remote Loader service. Select <i>Remote</i> if you want the driver to use the Remote Loader service, either locally on the Metadirectory server or remotely on another server.
Remote Host Name and Port	<p>This applies only if the driver is running remotely.</p> <p>Specify the host name or IP address of the server where the driver's Remote Loader service is running.</p>
Driver Password	<p>This applies only if the driver is running remotely.</p> <p>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.</p>
Remote Password	<p>This applies only if the driver is running remotely.</p> <p>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</p>
Driver Settings	Specify the fields such as, <nds>, <input>, <output> element handling, Salesforce login URL, Salesforce Login ID, Salesforce Login Password, Salesforce Security Token, Proxy Host and Port, and Truststore file.
Define Security Equivalences	The driver requires rights to objects within the Identity Vault and to the input and output directories on the server. 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.
Exclude Administrative Roles	You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

When you finish providing the information required by the wizard, a Summary page, similar to the following is displayed.



At this point, the driver is created from the basic configuration file. To ensure that the driver works the way you want it to for your environment, you must review and modify the driver's default configuration settings.

- 4 To modify the default configuration settings, click the linked driver name, then continue with the next section, [Configuring the Driver](#).

or

To skip the configuration settings at this time, click *Finish*. When you are ready to configure the settings, continue with [Configuring the Driver](#).

### 3.2.2 Configuring the Driver

After importing the driver configuration file, you need to configure the driver before it can run. 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, “Customizing the Driver,” on page 23](#).
- ♦ **Set Up a Secure HTTPS Connection:** The connection between the driver and the SPML or DSML server can be configured to use a secure HTTPS connection rather than an HTTP connection. For instructions, see [Chapter 5, “Securing Communication,” on page 25](#)

After completing the configuration tasks, continue with the next section, [Starting the Driver](#).

### 3.2.3 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 iManager, click  to display the Identity Manager Administration page.
- 2 Click *Identity Manager Overview*.
- 3 Browse to and select the driver set object that contains the driver you want to start.
- 4 Click the driver set name to access the Driver Set Overview page.
- 5 Click the upper right corner of the driver, then click *Start driver*.

## 3.3 Activating the Driver

To activate the Salesforce.com driver, activate the Metadirectory engine, then activate the driver by using the separate Salesforce.com 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.

For information on activation, refer to “[Activating Novell Identity Manager Products](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

# Customizing the Driver

# 4

The following sections provide information to help you understand what the driver does and what customization you might need to make to the driver:

- ♦ [Section 4.1, “Creating XSLT Style Sheets,” on page 23](#)
- ♦ [Section 4.2, “Managing Operation Data,” on page 23](#)
- ♦ [Section 4.3, “Managing the Driver,” on page 24](#)
- ♦ [Section 4.4, “Schema Mapping,” on page 24](#)

## 4.1 Creating XSLT Style Sheets

The application-specific protocol handling is done in Input Transformation and Output Transformation style sheets. The driver preconfig contains default policies for Salesforce.com. For detailed information on writing style sheets, refer to the sample style sheets that come with this driver. For more information on style sheets see [“Defining Policies by Using XSLT Style Sheets”](#) in the *Understanding Policies for Identity Manager 4.0*.

## 4.2 Managing Operation Data

The driver shim applies special handling to Subscriber commands based on the `<operation-data>` element. On the Subscriber channel, the `<operation-data>` element can be added to a command to specify XML data that you want included with the command result. In this way you can match commands with the responses they generate, which is useful for creating associations.

As discussed in [Chapter 1, “Understanding the Salesforce.com Driver,” on page 9](#), the `<operation-data>` element is added to the command from one of the Subscriber channel policies. The driver shim removes the operation data from the command before it is sent to the application, and restores the `<operation-data>` element (and all child elements) to the resulting response. If needed, rules and style sheets can then access the operation-data element on the result.

- ♦ [Section 4.2.1, “Using Operation Data to Specify XML to Be Returned on the Result,” on page 23](#)

### 4.2.1 Using Operation Data to Specify XML to Be Returned on the Result

The sample configurations for the Salesforce.com driver use the `<operation-data>` element to keep track of identifying information for a command, so the result can be recognized and associations can be properly assigned. Check these samples for details of how the `<operation-data>` element is used.

When the `<operation-data>` element is restored on the response, it appended as a child element of the root node. You can override this by providing one or more `parent-node-n` attributes to the `<operation-data>` element, where *n* is a number beginning with 1 that is incremented for each parent specifier provided. The driver shim looks for `parent-node-n` attributes. When they are found, the attribute is checked to see if the named node exists. If the node is found, it uses as the parent for the `<operation-data>` element on the response.

## 4.3 Managing the Driver

As you work with the Salesforce.com 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

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the [\*Identity Manager 4.0 Common Driver Administration Guide\*](#).

## 4.4 Schema Mapping



# Securing Communication

# 5

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 following sections provide instructions for creating a secure connection:

- [Section 5.1, “Configuring the Subscriber Channel,” on page 25](#)

## 5.1 Configuring the Subscriber Channel

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 \(http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html\)](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*.



# Managing the Driver

# 6

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 [\*Identity Manager 4.0 Common Driver Administration Guide\*](#).



# Troubleshooting the Driver

# 7

You can log Identity Manager events by using Novell 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:

- ♦ [Section 7.1, “Driver Shim Errors,” on page 29](#)
- ♦ [Section 7.2, “Troubleshooting Driver Processes,” on page 32](#)

## 7.1 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 \(http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html\)](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 [Section A.1.5, "Driver Parameters," on page 35](#).

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 Metadirectory 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, "Customizing the Driver," 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

## 7.2 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 *Identity Manager 4.0 Common Driver Administration Guide*.



# Driver Properties

# A


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 *Identity Manager 4.0 Common Driver Administration Guide* for information about the common properties.

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

- ♦ [Section A.1, “Driver Configuration,” on page 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:

### A.1.1 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.com.SalesforceDriver
```

**Navtive:** 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.

## A.1.2 Driver Object Password

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

## A.1.3 Authentication

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

**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 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:** 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.

## 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.

**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.

**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.


---

## 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 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 global configuration values are organized as follows:

## A.2.1 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.

**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.

## A.2.2 Password Synchronization

Use the following GCVs to configure the driver to synchronize passwords to the Identity Vault. For more information, see [Identity Manager 4.0 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.

