AUTHORIZED DOCUMENTATION

Driver for SAP Portal Implementation Guide

Novell®
Identity Manager

3.6.1

August 17, 2009

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2009 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., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide provides information about the Identity Manager driver for SAP* Portal.

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Installing the SAP Portal Driver,” on page 13
- Chapter 3, “Creating a New Driver,” on page 17
- Chapter 4, “Implementing the Preconfigured Entitlements,” on page 25
- Chapter 5, “Configuring the SAP System,” on page 29
- Chapter 6, “Security Best Practices,” on page 31
- Chapter 7, “Managing the Driver,” on page 33
- Chapter 8, “Troubleshooting the Driver,” on page 35
- Appendix A, “Driver Properties,” on page 37

Audience

This guide is intended for SAP integrators and Identity Manager administrators.

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 and enter your comments there.

Documentation Updates

For the most recent version of the *Identity Manager Driver for SAP Portal Implementation Guide*, visit the Novell Compliance Management Platform Extension for SAP Environments Documentation Web site (http://www.novell.com/documentation/ncmp_sap10/).

Additional Documentation

For documentation on Identity Manager, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36/index.html).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell® trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Overview

1

The SAP Portal driver provisions users to the SAP NetWeaver* Application Server. This provides another way to provision and manage your user accounts in your SAP environment. You can use this driver by itself or with the SAP User Management driver.

The following sections explain concepts you should understand before implementing the SAP Portal driver.

- Section 1.1, “Terminology,” on page 9
- Section 1.2, “Supported SAP Versions,” on page 9
- Section 1.3, “Driver Concepts,” on page 9
- Section 1.4, “Support for Standard Driver Features,” on page 10

1.1 Terminology

This section gives you essential information about terminology used with SAP and the SAP Portal driver.

ABAP: Advanced Business Application Programming. A programming language designed for creating large-scale business applications.

BAPI: Business APIs for the SAP business object types.

CUA: Central User Administration.

SPML: Service Provisioning Markup Language. An XML-based framework for managing the provisioning and allocation of identity information and system resources within and between organizations.

UME: User Management Engine.

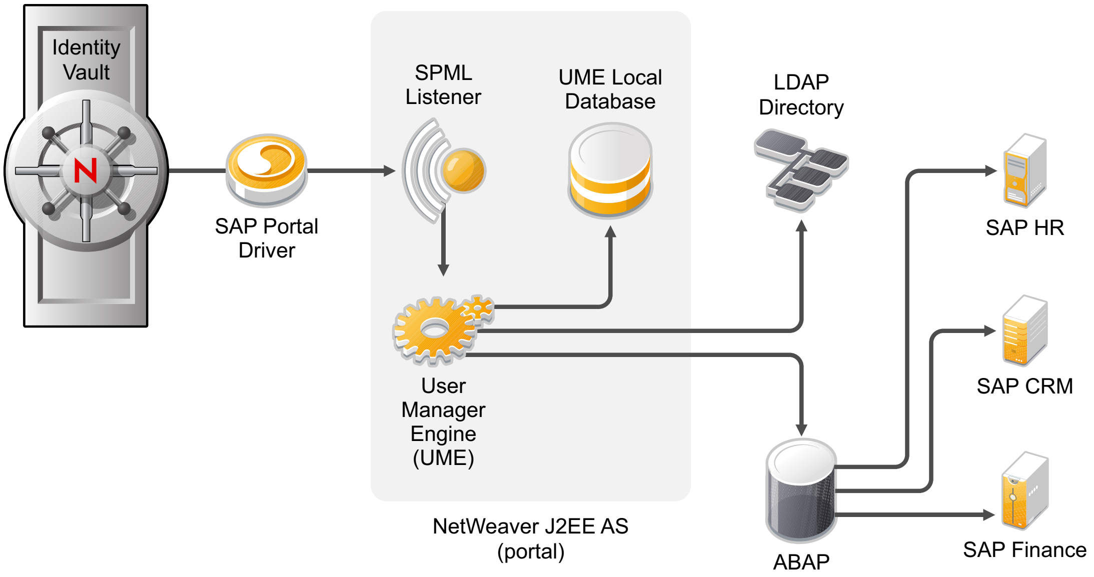
1.2 Supported SAP Versions

The SAP Portal driver supports SAP NetWeaver 7.x.

1.3 Driver Concepts

The following figure shows how the SAP Portal driver works. The driver provisions users from the Identity Vault and pass them to the SPML listener service on the portal. The SPML listener passes the requests to the User Management Engine (UME) and the UME writes the request to the UME local database, to an external LDAP directory, or to an ABAP system, depending on the configuration of the identity store for the portal. If the request is written to the ABAP system, the request can be passed to any CUA SAP systems that are part of the ABAP back end.

Figure 1-1 *SAP Portal Driver*



The SAP Portal driver synchronizes SAP users as well as the user's SAP group assignments and SAP role assignments. If the Portal is configured with an ABAP user store, the user account is synchronized and added to the ABAP system; however, the ABAP roles, which display as SAP group objects in the portal, cannot be assigned directly in the SPML service. To synchronize groups, you must use the SAP User Management driver with the SAP Portal driver. For more information, see the *Identity Manager 3.6.1 Driver for SAP User Management Implementation Guide*.

The SAP Portal driver can be configured to use any of the back-end identity stores that are available.

The SAP Portal driver synchronizes information from the Identity Vault into the portal. Synchronizing information from the portal into the Identity Vault is not supported. This is unidirectional driver.

1.4 Support for Standard Driver Features

The following sections provide information about how the SAP Portal driver supports standard driver features:

- Section 1.4.1, "Local Platforms," on page 10
- Section 1.4.2, "Remote Platforms," on page 11
- Section 1.4.3, "Entitlements," on page 11
- Section 1.4.4, "Password Synchronization," on page 11
- Section 1.4.5, "Account Tracking," on page 11
- Section 1.4.6, "Identity Manager Role Mapping Administrator," on page 11

1.4.1 Local Platforms

A local installation is an installation of the driver on the same server as the Metadirectory engine and the Identity Vault.

The SAP Portal driver can be installed on the same operating systems supported by the Metadirectory engine. For information, see “Metadirectory Server” in “System Requirements” in the *Identity Manager 3.6.1 Installation Guide*.

1.4.2 Remote Platforms

You can install the Remote Loader f you don’t want to install the Metadirectory engine and the Identity Vault (eDirectory™) on the same server.

The SAP Portal driver can be installed on the same operating systems supported by the Remote Loader. For information, see “Remote Loader” in “System Requirements” in the *Identity Manager 3.6.1 Installation Guide*.

1.4.3 Entitlements

Entitlements are a way to set up a list of criteria to grant or revoke users, roles, and groups access to resources. The SAP Portal drivers contains three preconfigured entitlements. For more information, see Chapter 4, “Implementing the Preconfigured Entitlements,” on page 25.

1.4.4 Password Synchronization

The SAP Portal driver can synchronize passwords from the Identity Vault into the SAP NetWeaver server. The password synchronization is one way. For more information, see the *Identity Manager 3.6.1 Password Management Guide*.

1.4.5 Account Tracking

Account Tracking allows you to manage all of the identities each user account has in each system connected to the Identity Vault. Account Tracking is a feature included with the Novell® Compliance Management Platform. For more information, see the Novell Compliance Management Platform Web site (http://www.novell.com/products/compliancemanagementplatform/).

1.4.6 Identity Manager Role Mapping Administrator

The SAP Portal driver can be configured to work with the Identity Manager Role Mapping Administrator, which is a tool that allows you to map business roles to IT roles. The Role Mapping Administrator is included with the Novell Compliance Management Platform extension for SAP environments. For more information, see the Novell Compliance Management Platform extension for SAP environments Web site (http://www.novell.com/products/).

Installing the SAP Portal Driver 2

The SAP Portal driver is installed when you install the SAP Integration module. The installation program extends the Identity Vault schema and installs the driver shim. This driver requires latest updated driver configuration file. You must update Designer and iManager to get the updated configuration file.

- Section 2.1, "Downloading the Installation Program," on page 13
- Section 2.2, "Installing the Driver Files on the Metadirectory Engine," on page 13
- Section 2.3, "Installing the Driver Files on the Remote Loader," on page 14
- Section 2.4, "Installing the Designer and iManager Updates," on page 14

2.1 Downloading the Installation Program

The SAP Portal driver installation program is available on the Novell® Identity Manager 3.6.1 Integration Module for Enterprise download site (http://download.novell.com/Download?buildid=XAwwFo5tM8A~).

1. Click *Novell Identity Manager 3.6.1 Integration Module for Enterprise*, then click *Download*.
2. Click *proceed to download*, then download the `NIdM_Drivers_for_SAP.iso` file.

2.2 Installing the Driver Files on the Metadirectory Engine

The installer checks for the installed version of Identity Manager. You must have Identity Manager 3.6.1 installed for the installer to work.

1. Use the correct installation program for your platform on the `NIdM_Driver_for_SAP.iso` file.

Platform	File
Windows*	`sap_drivers_install.exe`
Linux	`./sap_drivers_install_linux.bin`
Solaris*	`./sap_drivers_install_solaris.bin`
AIX*	`./sap_drivers_install_aix.bin`

2. Read and accept the license agreement, then click *Next*.
3. Select *Drivers* and *Schema Extensions*, then click *Next*.
4. Specify the LDAP DN of an administrative user that has rights to extend schema.
5. Specify the password of the administrative user.
6. Review the pre-installation summary, then click *Install*.
7. Review installation complete message, then click *Done*.

2.3 Installing the Driver Files on the Remote Loader

1 Use the correct installation program for your platform on the `NIdM_Driver_for_SAP.iso` file.

Platform	File
Windows	`sap_drivers_install.exe`
Linux	`./sap_drivers_install_linux.bin`
Solaris	`./sap_drivers_install_solaris.bin`
AIX	`./sap_drivers_install_aix.bin`

2 Read and accept the license agreement, then click *Next*.

3 Select *Drivers* and *Utilities*, then click *Next*.

4 Specify the path to install the driver. The default location is:

Platform	Location
Windows	`c:\Novell\RemoteLoader\lib`
Linux/UNIX	`/opt/novell/eDirectory/lib/dirxml`

5 Click *Next*.

6 Specify the path to install the utilities. The default location is:

Platform	Location
Windows	`c:\Novell\NDS\DirXML\Utilities`
Linux/UNIX	/opt/novell/

7 Review the pre-installation summary, then click *Install*.

8 Review the installation complete message, then click *Done*.

2.4 Installing the Designer and iManager Updates

There is a new driver configuration file for the SAP Portal driver that must be installed to use the driver.

- Section 2.4.1, "Installing the 3.0.1 Designer Auto Update," on page 15
- Section 2.4.2, "Installing the Updated iManager Plug-Ins for Identity Manager," on page 15

2.4.1 Installing the 3.0.1 Designer Auto Update

In order to manage drivers with structured GCVs, you must install the 3.0.1 Designer Auto Update.

1. From the Designer 3.0.1 toolbar, select *Help* > *Check for Designer Updates*.
2. Follow the prompts to complete the installation.
3. Click *Yes* to restart Designer.

   Designer must be restarted for the changes to take effect.

2.4.2 Installing the Updated iManager Plug-Ins for Identity Manager

In order to manage drivers with structured GCVs, you must install the updated iManager plug-ins.

1. Launch iManager and log in as an administrative user.
2. From the toolbar, click the *Configure* icon .
3. Click *Plug-in Installation* > *Available Novell Plug-in Modules*.
4. Select the *Identity Manager 3.6.1 FP1 Plug-in for iManager 2.7*, then click *Install*.
5. Select *I Agree* in the license agreement, then click *OK*.
6. After the installation finishes, click *Close* twice.
7. Log out of iManager and restart Tomcat to have the changes take effect.

Creating a New Driver

3

After the SAP Portal driver files are installed on the server where you want to run the driver (see Chapter 2, “Installing the SAP Portal Driver,” on page 13), you can create the driver in the Identity Vault. You do so by importing the basic driver configuration file and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- Section 3.1, “Using Designer to Create and Configure the Driver,” on page 17
- Section 3.2, “Using iManager to Create and Configure the Driver,” on page 20
- Section 3.3, “Activating the Driver,” on page 23

3.1 Using Designer to Create and Configure the Driver

The following sections provide steps for using Designer to create and configure a new SAP Portal driver. For information about using iManager to accomplish these tasks, see Section 3.2, “Using iManager to Create and Configure the Driver,” on page 20.

- Section 3.1.1, “Using Designer to Import the Driver Configuration File,” on page 17
- Section 3.1.2, “Using Designer to Adjust the Driver Settings,” on page 18
- Section 3.1.3, “Using Designer to Deploy the Driver,” on page 19
- Section 3.1.4, “Using Designer to Start the Driver,” on page 19

3.1.1 Using Designer to Import the Driver Configuration File

Importing the SAP Portal driver configuration file creates the driver in the project and adds the policies needed to make the driver function properly.

1. In Designer, open your project.
2. In the Modeler, right-click the driver set where you want to create the driver, then select *New* > *Driver* to display the Driver Configuration Wizard.
3. In the *Driver Configuration* list, select *SAP Portal*, then click *Run*.
4. On the Import Information Requested page, fill in the following fields:
    - **Driver Name:** Specify a name that is unique within the driver set.
    - **URL of the remote SPML Provisioning Service Point:** Specify the URL of the remote SAP Portal SPML Provisioning Service Point.

      For example: `http://my.sap.com:50000/spml/spmlservice`
    - **Authentication ID:** Specify the authentication ID for the remote SAP Portal SPML Provisioning Service Point. For more information, see Section 5.1, “Creating an Administrative User Account for the Driver,” on page 29.
    - **Use User Account Entitlement:** Select *True* if you have entitlements enabled in your environment. Select *False* if entitlements are not enabled. The SAP Portal driver contains three preconfigured entitlements. For more information, see Chapter 4, “Implementing the Preconfigured Entitlements,” on page 25.

- **User Container:** Specify the Identity Vault top level container where the users objects are monitored for Subscriber events. This value is used for all drivers and is stored on the driver set. If you want a different location for each driver, create a driver level GCV parameter with the same name.
- **Group Container:** Specify the Identity Vault top level container where the groups are monitored for Subscriber events. This value is used for all drivers and is stored on the driver set. If you want a different location for each driver, create a driver level GCV parameter with the same name.
- **Driver is Local/Remote:** Select whether the driver is running locally or is using the Remote Loader. For more information, see the *Identity Manager 3.6.1 Remote Loader Guide*.
- **Enter the password for the Authentication Password:** Specify the password for the Authentication ID, then reenter the password for verification.
- **Enter the password to Reset Password:** Specify a default password to be set for users when the driver resets a user's password in the SAP Portal. It is set during password changes if the user-supplied password is not accepted by the SAP server. This is only used if the driver resets the password.

  The password must comply with your SAP Portal Security Policy for passwords. The default SAP Portal Security Policy requires alphanumeric passwords between 5 and 14 characters in length.

5. Click *Next* to import the driver configuration.

   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 (if necessary) the driver's default configuration settings.

6. To modify the default configuration settings, click *Configure*, then continue with the next section, Using Designer to Adjust the Driver Settings.

   or

   To skip the configuration settings at this time, click *Close*. When you are ready to configure the settings, continue with the next section, Using Designer to Adjust the Driver Settings.

7. Continue with Section 3.1.3, "Using Designer to Deploy the Driver," on page 19, to deploy the driver into the Identity Vault.

3.1.2 Using Designer to Adjust the Driver Settings

The information specified on the Import Information Requested page is the minimum information required to import the driver. However, the base configuration might not meet your needs, or you might need to change the configuration you created when you imported the driver.

- You might need to change whether the driver is running locally or remotely.
- You might need to change whether the driver is using entitlements.

If you need to do additional configuration for the driver, you must access the properties page of the driver. If you do not have the Driver Properties page displayed:

1. In Designer, open your project.

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

This opens the properties page for the driver. Use the information in Appendix A, “Driver Properties,” on page 37 to adjust the configuration.

3.1.3 Using Designer to Deploy 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 to authenticate:

- **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*.

3.1.4 Using Designer to Start the Driver

When a driver is created, it is stopped by default. You must start the driver before events are processed.

To start the driver after the driver is deployed:

1 In Designer, open your project.

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

For information about management tasks with the driver, see Chapter 7, “Managing the Driver,” on page 33.

3.2 Using iManager to Create and Configure the Driver

The following sections provide steps for using iManager to create and configure a new SAP Portal driver. For information about using Designer to accomplish these tasks, see Section 3.1, “Using Designer to Create and Configure the Driver,” on page 17.

- Section 3.2.1, “Using iManager to Import the Driver Configuration File,” on page 20
- Section 3.2.2, “Using iManager to Configure the Driver Settings,” on page 22
- Section 3.2.3, “Using iManager to Start the Driver,” on page 23

3.2.1 Using iManager to Import the Driver Configuration File

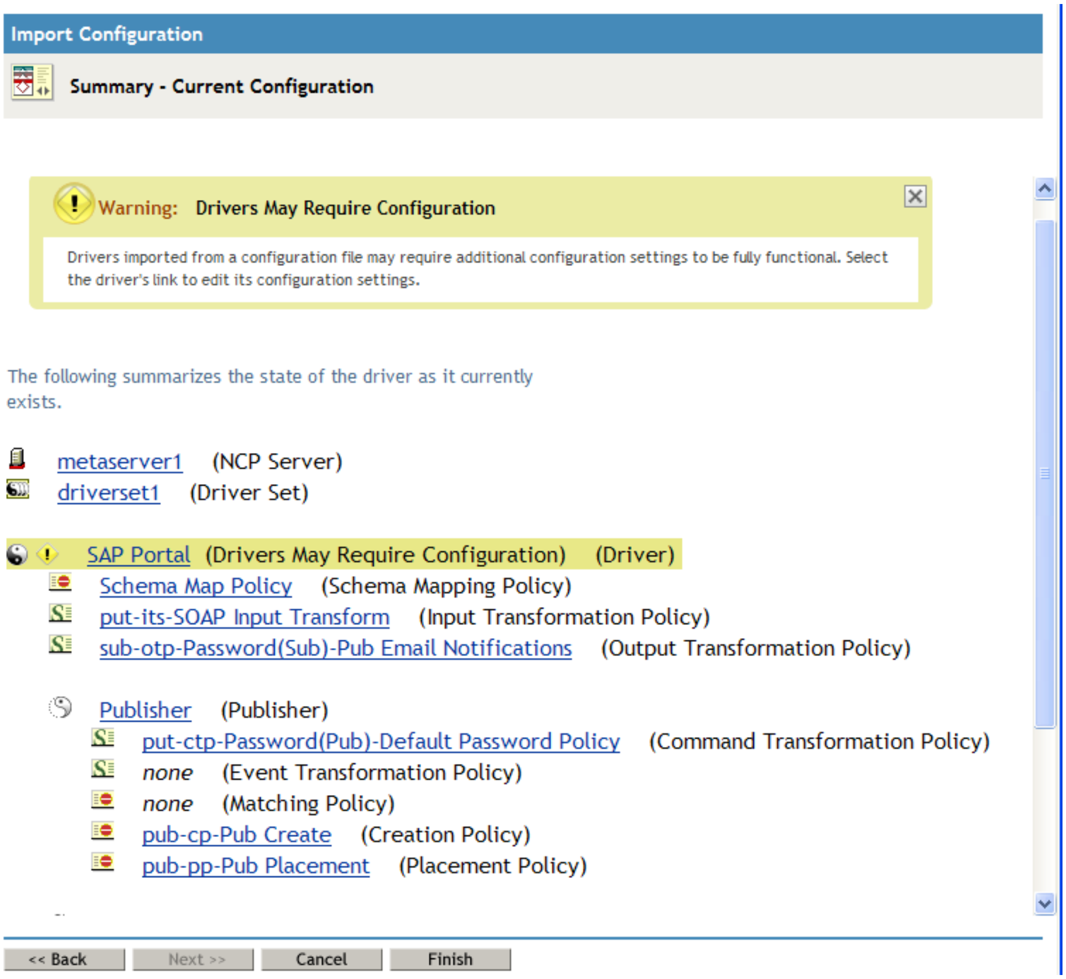
Importing the SAP Portal driver configuration file creates the driver in the Identity Vault and adds the policies needed to make the driver work properly.

1. In iManager, click to display the Identity Manager Administration page.
2. In the Administration list, click *Utilities* > *Import Configuration* to launch the Import Configuration Wizard.
3. Select the name of the SAP Portal configuration file to import.
4. Use the following information to complete the wizard and create the driver.

Prompt	**Description**
Where do you want to place the imported configuration?	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.
Import a configuration into this driver set	Use the default option, *Import a configuration from the server (.XML file)*. In the *Show* field, select *Identity Manager 3.6 configurations*. In the *Configurations* field, select the `SAPPortal-IDM3_6_0-V1.xml` file.
Driver name	Specify a name that is unique within the driver set.
URL of the remote SPML Provisioning Service Point	Specify the URL of the remote SAP Portal SPML Provisioning Service Point. For example: `http://my.sap.com:50000/spml/spmlservice`
Authentication ID	Specify the authentication ID for the remote SAP SPML Provisioning Service Point. For more information, see Section 5.1, “Creating an Administrative User Account for the Driver,” on page 29.

Prompt	Description
Use User Account Entitlement	Select *True* if you have entitlements enabled in your environment. Select *False* if entitlements are not enabled. The SAP Portal driver contains three preconfigured entitlements. For more information, see Chapter 4, "Implementing the Preconfigured Entitlements," on page 25.
User Container	Specify the Identity Vault container where the users objects will be added if they don't already exist in the Identity Vault. This value is used for all drivers and is stored on the driver set. If you want a different location for each driver, create a driver level GCV parameter with the same name.
Group Container	Specify the Identity Vault container where the groups are created if they don't already exist in the Identity Vault. This value is used for all drivers and is stored on the driver set. If you want a different location for each driver, create a driver level GCV parameter with the same name.
Driver is Local/Remote	Select whether the driver is running locally or is using the Remote Loader. For more information, see the *Identity Manager 3.6.1 Remote Loader Guide*.
Enter the password for the Authentication Password	Specify the password for the Authentication ID, then reenter the password for verification.
Enter the password for the Reset Password	Specify a default password to be set for users when the driver resets a user's password in the SAP Portal. It is set during password changes if the user-supplied password is not accepted by the SAP server. This is only used if the driver resets the password. The password must comply with your SAP Portal Security Policy for passwords. The policies require alphanumeric passwords between 5 and 14 characters in length.
Define Security Equivalences	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.
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.



Warning: Drivers May Require Configuration

Drivers imported from a configuration file may require additional configuration settings to be fully functional. Select the driver's link to edit its configuration settings.

The following summarizes the state of the driver as it currently exists.

metaserver1 (NCP Server)
driverset1 (Driver Set)

SAP Portal (Drivers May Require Configuration) (Driver)
Schema Map Policy (Schema Mapping Policy)
put-its-SOAP Input Transform (Input Transformation Policy)
sub-otp-Password(Sub)-Pub Email Notifications (Output Transformation Policy)

Publisher (Publisher)
put-ctp-Password(Pub)-Default Password Policy (Command Transformation Policy)
none (Event Transformation Policy)
none (Matching Policy)
pub-cp-Pub Create (Creation Policy)
pub-pp-Pub Placement (Placement Policy)

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 (if necessary) the driver's default configuration settings.

5. To modify the default configuration settings, click the linked driver name, then continue with the next section, Using iManager to Configure the Driver Settings.

   or

   To skip the configuration settings at this time, click *Finish*. When you are ready to configure the settings, continue with the next section, Using iManager to Configure the Driver Settings.

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

3.2.2 Using iManager to Configure the Driver Settings

The information specified during the creation of the driver is the minimum information required to import the driver. However, the base configuration might not meet your needs.

- You might need to change whether the driver is running locally or remotely.
- You might need to change whether the driver is using entitlements.

To configure the settings:

1. Make sure the Modify Object page for the SAP Portal driver is displayed in iManager. If it is not:
   - **1a** In iManager, click to display the Identity Manager Administration page.
   - **1b** Click *Identity Manager Overview*.
   - **1c** Browse to and select the driver set object that contains the new SAP Portal driver.
   - **1d** Click the driver set name to access the Driver Set Overview page.
   - **1e** Click the upper right corner of the driver, then click *Edit properties*.

     This displays the properties page of the driver.
2. Review the settings for the driver parameters, global configuration values, or engine control values. The configuration settings are explained in Appendix A, “Driver Properties,” on page 37.
3. After modifying the settings, click *OK* to save the settings and close the Modify Object page.

3.2.3 Using iManager to Start the Driver

When a driver is created, you must start the driver. Identity Manager is an event-driven system, so after the driver is started, it processes events as they occur.

To start the driver after the additional configuration is completed:

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

For information about management tasks with the driver, see Chapter 7, “Managing the Driver,” on page 33.

3.3 Activating the Driver

The SAP Portal driver is part of the Identity Manager Integration Module for Enterprise, and this module requires a separate activation from the Metadirectory engine and services driver activation. After you have purchased the Integration Module for Enterprise, the new activation is available in your Novell Customer Center.

If you create the driver in a driver set where you’ve already activated a driver that comes with the Integration Module for Enterprise, the SAP Portal driver inherits the activation. If you created the SAP Portal driver in a driver set that has not been activated, you must activate the driver, with the Integration Module for Enterprise activation, within 90 days. Otherwise, the driver does not start.

The drivers that are included in the Integration Module for Enterprise are:

- Driver for SAP HR
- Driver for SAP Portal

- Driver for SAP User Management
- Driver for PeopleSoft*

For information on activation, refer to "Activating Novell Identity Manager Products" in the *Identity Manager 3.6.1 Installation Guide*.

Implementing the Preconfigured Entitlements 4

Entitlements are a way to set up a list of criteria to grant or revoke users' access to resources in the SAP Portal system. The SAP Portal driver comes with three preconfigured entitlements, that work with an entitlement agent. The entitlements usage is controlled through Global Configuration Values (GCVs) on the driver.

This section explains each preconfigured entitlement, how to enable the entitlement, and what an entitlement agent is.

- Section 4.1, "Entitlement Agents," on page 25
- Section 4.2, "User Account Entitlement," on page 25
- Section 4.3, "Portal Role Entitlement," on page 26
- Section 4.4, "Portal Group Entitlement," on page 27

4.1 Entitlement Agents

An entitlement agent grants an entitlement to a user when criteria are met. You must create and configure one of the following entitlement agents for use with the preconfigured entitlements in the SAP Portal driver.

- **Role-Based Entitlements (RBE):** Manages entitlements based on the events that occur in the Identity Vault. It is used for simple automation. For example, when a user is added to the HR system, the user is automatically granted accounts in other systems. This requires an Entitlements driver created with policies that define the desired action. For instructions, see the "Checklist for Implementing Entitlements" in the *Identity Manager 3.6 Driver for Role-Based Entitlements: Implementation Guide*.
- **Workflow:** Manages entitlements through provisioning workflows. It is used when approvals are required. For example, when a user is added to the HR system, the manager must approve the accounts for the user. This requires a workflow that contains the desired actions. For instructions, see *"Configuring and Managing Provisioning Workflows"* (http://www.novell.com/documentation/idmrbpm361/agpro/index.html?page=/documentation/idmrbpm361/agpro/data/b88n0ju.html).
- **Roles Based Provisioning Module (RBPM):** Manages entitlements based on roles that are assigned to users. For example, when a user is added to the Accounting role, the user automatically receives all accounts associated with the Accounting role. This requires that the Roles Based Provisioning Module be installed and configured for roles. For installation instructions, see the "Installation Checklist" (http://www.novell.com/documentation/idmrbpm361/install/data/bf8up4w.html) for the Roles Based Provisioning Module.

4.2 User Account Entitlement

The user account entitlement is a simple (no parameters) entitlement used to control user account creation on the Subscriber channel. After the user account entitlement is enabled, the user account is provisioned when the entitlement is granted.

This entitlement also has Subscriber policies that define actions to take when the entitlement is revoked. When an entitlement is revoked, there are two actions that can be taken:

- **Disable:** When the entitlement is revoked, the user account is locked in the connected SAP Portal.
- **Delete:** A request is sent to delete the account.

To enable this entitlement:

1. Verify that an entitlement agent that contains your list of criteria to grant or revoke a user's access to resources in SAP exists. For more information, see Section 4.1, "Entitlement Agents," on page 25.
2. If you have an existing driver, skip to Step 3; otherwise, during the creation of a driver, select *True* for the *Use User Account Entitlement* option.

   This sets the entitlement GCVs to True.
3. Access the GCVs page for the driver.
4. Select *show* for the *Show entitlements configuration* option.
5. Enable the user account entitlement by selecting *true*.
6. Select what to do when the user account entitlement is revoked by indicating whether you want the account disabled, deleted, or nothing done to the account.
7. Click *OK* to save the changes.

The entitlement is now enabled. However, a new user account is not provisioned until the entitlement is granted.

4.3 Portal Role Entitlement

The portal role entitlement adds users to the SAP Portal roles, and it is disabled by default if you selected to use entitlements during the creation of the driver. This entitlement contains parameters, which means it can be granted multiple times. The parameters for the entitlement are roles returned by the entitlement query to the SAP Portal. When the entitlement is granted with an SAP Portal Role as the parameter, the SAP User is added to the Portal Role.

For example, assume there is an RBPM role that contains two UMERole entitlements, one with a parameter of User Admins and the second with a parameter of HR Admin. When the RBPM role is granted and the entitlements are granted, the user is added to the User Admins and the HR Admin roles in the SAP Portal.

This entitlement is disable by default. The best practice is to assign Portal users to Portal groups, which in turn contains the appropriate Portal Roles. However, if you want to assign Portal roles directly to the Portal users, this entitlement allows you to do that.

To manually enable this entitlement:

1. Verify that an entitlement agent that contains your list of criteria to grant or revoke Portal role assignments in SAP exists. For more information, see Section 4.1, "Entitlement Agents," on page 25.
2. If you have an existing driver skip to Step 3; otherwise, during the creation of a driver, select *True* for the *Use Portal Role Entitlement* option.

   This sets the entitlement GCVs to True.

3. Access the GCVs page for the driver.
4. Select *True* for the *User Portal Role Entitlement* option.
5. Click *OK* to save the changes.

The entitlement is now enabled. When a user is granted a role through one of the entitlement agents, the associated Portal role assignments are automatically made for the user by the SAP Portal driver.

4.4 Portal Group Entitlement

The portal group entitlement adds users to the SAP Portal Groups, and it is enabled by default. This entitlement contains parameters, which means it can be granted multiple times. The parameters for the entitlement are SAP groups returned by the entitlement query to the SAP Portal.

The SAP ABAP roles might appear as UME Groups when the entitlement query is issued, but the SAP Portal driver cannot assign ABAP roles directly.

To manually enable this entitlement:

1. Verify that an entitlement agent that contains your list of criteria to grant or revoke Portal group assignments in SAP exists. For more information, see Section 4.1, "Entitlement Agents," on page 25.
2. If you have an existing driver, skip to Step 3; otherwise, during the creation of a driver, select *True* for the *Use Portal Group Entitlement* option.

   This sets the entitlement GCVs to True.
3. Access the GCVs page on the driver.
4. Select *True* for the *User Portal Group Entitlement* option.
5. Click *OK* to save the changes.

The entitlement is now enabled. When a user is granted a UME group entitlement through one of the entitlement agents, the SAP Portal driver automatically adds the user to the associated Portal groups.

Configuring the SAP System 5

The following items must be configured on your SAP system for the SAP Portal driver to work:

- Verify that the SPML listener on the SAP Web Application server is available and working.
- You must create an administrative user for the driver to use instead of using the SAP Administrator account. For more information, see Section 5.1, “Creating an Administrative User Account for the Driver,” on page 29.

5.1 Creating an Administrative User Account for the Driver

The driver must authenticate to the SAP Portal as a member of the Administrators group in order to create, delete, and modify accounts in the SAP Portal system. Creating a separate account that has administrative rights prevents the SAP Administrator account from ever being locked by any actions of the SAP Portal driver. For example, the Administrator password is changed, but the old password is still stored in the driver. The driver attempts to log into the portal as part of its normal activity and locks the Administrator account based on the SAP Portal security policy.

To create an administrative user for the driver:

1. Log into the SAP Portal as the Administrator.
2. Search for the Administrator user account in Identity Management.
3. Select the Administrator user account.
4. Click *Copy to New User* to create a user with the same rights as the Administrator.
5. Specify the *Logon ID* for the administrative user.
6. Specify a password for this user in the *Define Initial Password* field.
7. Click *Save* to save the new user.
8. Log out of the portal.
9. Log back into the portal as the new administrative user.

   This prompts the user to set a permanent password.
10. Specify this user in the “Portal Authentication Information > Authentication ID” on page 40, then update the password in the “Portal Authentication Information > Authentication Password” on page 40 on the Subscriber settings of the driver.

After the permanent password is set, the driver has the same rights as the Administrator user. You can check the administrative user’s rights by verifying that it is a member of the Administrators group in the UME configuration.

6 Security Best Practices

This section contains a description of the security parameters unique to the SAP Portal driver.

For additional information about securing your Identity Manager system, see the *Identity Manager 3.6 Security Guide*.

To increase security, you can configure the SAP Portal driver to communicate over HTTPS, then create a secure connection for it to use.

To create a secure connection:

1 Create a server certificate in iManager.

1a In the *Roles and Tasks* view, click *Novell Certificate Server* > *Create Server Certificate*.

1b Browse to and select the server object where the SAP Portal driver is installed.

1c Specify a certificate nickname.

1d Select *Standard* as the creation method, then click *Next*.

1e Click *Finish*, then click *Close*.

2 Export a self-signed certificate from the certificate authority in eDirectory™.

2a In the *Roles and Tasks* view, click *Directory Administration* > *Modify Object*.

2b Select your tree's certificate authority object, then click *OK*.

It is usually found in the Security container and is named something like *TREENAME CA.Security*.

2c Click *Certificate* > *Self Signed Certificate*.

2d Click *Export*.

2e When you are asked if you want to export the private key with the certificate, click *No*, then click *Next*.

2f Depending on the client to be accessing the Web service, select either *File in binary DER format* or *File in Base64 format* for the certificate, then click *Next*.

If the client uses a Java-based keystore or trust store, then you can choose either format.

2g Click *Save the exported certificate to a file*.

2h Click *Save* and browse to a known location on your computer.

2i Click *Save*, then click *Close*.

3 Import the self-signed certificate into the client's trust store:

3a Use the keytool executable that is included with any Java* JDK*.

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).

3b Import the certificate into your trust store or create a new trust store by entering the following command at a 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
```

4 Configure the Subscriber channel to use the trust store you created in Step 3:

4a In iManager, in the *Roles and Tasks* view, click *Identity Manager > Identity Manager Overview*.

4b Locate the driver set containing the SAP Portal driver, then click the driver's icon to display the Identity Manager Driver Overview page.

4c On the Identity Manager Driver Overview page, click the driver's icon again, then scroll to *Subscriber Settings*.

4d In the *Keystore File* setting, specify the path to the trust store you created in Step 3 on page 31.

5 Click *Apply*, then click *OK*.

Managing the Driver

7

As you work with the SAP Portal driver, there are a variety of management tasks you might need to perform, including the following:

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

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 3.6.1 Common Driver Administration Guide*.

Troubleshooting the Driver

8

The following sections contain potential problems and error codes you might encounter while configuring or using the driver.

8.1 Authenticating to the SPML Service

If the driver is not connecting to the UME, authenticate to the SPML service to verify if it is available and communicating.

8.2 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the processes, use DSTrace. You should only use DSTrace during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see "Viewing Identity Manager Processes" in the *Identity Manager 3.6.1 Common Driver Administration Guide*.

8.3 Error LOGONID_TOO_LONG

If you use the maximum length for a user name in the Identity Vault, the SAP Portal driver does not process the event and this is the error is in the DSTrace. To fix this issue, increase the *Maximum Length of Logon ID* value in the SAP Portal under *Identity Management* > *Configuration* > *Security Policy*.

8.4 Error PASSWORD_TOO_SHORT or ALPHANUM_REQUIRED_FOR_PSWD

If the reset password does not comply with the SAP Portal Security Policy, these errors are visible in the DSTrace. The reset password is used when resetting a user's password in the SAP Portal. The password must comply with your SAP Portal Security Policy for passwords. The default SAP Portal Security Policy requires alphanumeric passwords between 5 and 14 characters in length.

8.5 Error Occurs when Uninstalling the Driver

If you have installed the SAP Portal driver on a server that does not have a Java Virtual Machine (JVM) installed on it, you receive the following error when trying to uninstall the driver.

```
No Java virtual machine could be found from your PATH
environment variable. You must install a VM prior to
running this program.
```

The problem only occurs if you install the SAP Portal driver on a server that does not have Identity Manager or the Remote Loader installed on it.

The work around is to install the driver on a server with Identity Manager or the Remote Loader, or install the JVM and add the installation location to the PATH variable.

Linux/UNIX: To add the JVM to the PATH variable:

1. From a command line, enter `export PATH=<JAVA-HOME-PATH>/bin/:$PATH`.
2. Run the uninstall script for the Sentinel driver, where the JAVA-HOME-PATH is the Java or JRE installation location.

Windows: To add the JVM to the PATH variables, use the following command:

```
"Uninstall Novell Identity Manager Drivers for SAP.exe" LAX_VM "<JAVA-HOME-
PATH>\bin\java.exe"
```

Driver Properties

A

This section provides information about the Driver Configuration and Global Configuration Values properties for the SAP Portal driver. These are the only unique properties for this driver. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *Identity Manager 3.6.1 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 37
- Section A.2, "Global Configuration Values," on page 42

A.1 Driver Configuration

In Designer:

1 Open a project in the Modeler.

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

In iManager:

1 In iManager, 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 SAP Portal 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 properties page opens with the *Driver Configuration* tab displayed.

The Driver Configuration options are divided into the following sections:

- Section A.1.1, "Driver Module," on page 37
- Section A.1.2, "Driver Object Password (iManager Only)," on page 38
- Section A.1.3, "Authentication," on page 38
- Section A.1.4, "Startup Option," on page 39
- Section A.1.5, "Driver Parameters," on page 40

A.1.1 Driver Module

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

Table A-1 *Driver Modules*

Option	Description
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 name of the Java class is: `com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim`
Native	This option is not used with the SAP Portal 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 SAP Portal driver.

A.1.2 Driver Object Password (iManager Only)

Table A-2 *Driver Object Password*

Option	Description
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 options store the information required to authenticate to the connected system.

Table A-3 *Authentication Options*

Option	Description
Authentication ID	This field is not used for the SAP Portal driver. The authentication field is in the Subscriber settings documented in Table A-6 on page 40 in the Portal Authentication Information > URL of the remote SPML Provisioning Service Point.

Option	Description
Authentication Context or *Connection Information*	This field is not used for the SAP Portal driver.
Remote Loader Connection Parameters or *Host name* Port *KMO* *Other 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`
Driver Cache Limit (kilobytes) or *Cache limit (KB)*	Specify the maximum event cache file size (in KB). If this option is set to zero, the file size is unlimited. Click *Unlimited* to set the file size to unlimited in Designer.
Application Password or *Set Password*	Specify the password for the user object listed in the *Authentication ID* field.
Remote Loader Password or *Set 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 options allow you to set the driver state when the Identity Manager server is started.

Table A-4 *Startup Options*

Option	Description
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 option is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

The driver parameters let you tune driver behavior to align with your network environment.

The parameters are presented by category:

- Table A-5, "Driver Settings," on page 40
- Table A-6, "Subscriber Settings," on page 40
- Table A-7, "Publisher Settings," on page 42

Table A-5 *Driver Settings*

Parameter	Description
XML element handling specific for Identity Manager (<nds>, <input>, <output>)	Enables the Identity Manager engine to handle XML elements. ◆ **Remove/add elements:** Enables the driver shim to remove and add the required XML elements of `<nds>`, `<input>`, and `<output>`. These required elements are removed from the XML documents sent to the application and the elements are added to the XML documents received from the application before presenting the document to the Identity Manager engine. ◆ **Pass elements through:** Turns off the XML element handling.
Custom Java Extensions	Enables custom Java extensions to extend the driver shim's functionality. Select *Show* to enable the custom Java extensions. Select *Hide* if you don't have any custom Java extensions.

Table A-6 *Subscriber Settings*

Parameter	Description
Portal Authentication Information > URL of the remote SPML Provisioning Service Point	Specify the URL for the remote SPML Provisioning Service Point (PSP). A PSP is a software component that listens for, processes, and returns the results for well-formed SPML requests. For example: `http://my.sap.com:50000/spml/spmlservice`
Portal Authentication Information > Authentication ID	Specify the authentication ID for the remote SPML Provisioning Service Point.
Portal Authentication Information > Authentication Password	Specify the password for the authentication ID.

Parameter	Description
Default Reset Password > Default Reset Password	Specify a default password to be set for users when the driver resets a user's password in the SAP Portal. It is set during password changes if the user-supplied password is not accepted by the SAP server. This is only used if the driver resets the password. The password must comply with your SAP Portal Security Policy for passwords. The policies require alphanumeric passwords between 5 and 14 characters in length. If the reset password does not comply with the SAP Portal Security Policy, the error is visible in the Identity Manager traces. For more information, see Section 8.2, "Troubleshooting Driver Processes," on page 35. Example errors are PASSWORD_TOO_SHORT or ALPHANUM_REQUIRED_FOR_PSWD.
Show Advanced Options	Select *Show* to display advanced driver configuration options.
Show Advanced Options > Trustore file	When the remote server is configured to provide server authentication, this is the path and the name of the keystore file which contains trusted certificates. For example: `c:\security\trustore` Leave this field blank when server authentication is not used.
Show Advanced Options > Set mutual authentication parameters	Select *Show* if you want to set mutual authentication information.
Show Advanced Options > Proxy host and port	When a proxy host and port are used, specify the host address and the host port. Choose an unused port number on your server. Otherwise, leave this field blank. For example: 192.10.1.3:8180
Show Advanced Options > Handle HTTP session cookies	Some HTTP applications set cookies and expect them to be present on future requests. Select *Handle Cookies* if you want the driver to keep track of session cookies. Cookies are only kept until the driver is stopped.
Show Advanced Options > Process empty subscriber documents	Indicates whether or not the Subscriber channel should send empty documents to the target application. Documents could be empty if policy or stylesheets strip the XML without vetoing the command. Select *Ignore* to block empty documents from being sent to the target application.
Show Advanced Options > HTTP errors to retry	List the HTTP error codes that should return a retry status. Must be a list of integers separated by spaces.

Parameter	Description
Show Advanced Options > Customize HTTP Request-Header Fields	Select *Show* if you want to set mutual authentication information. Use the following fields to define the custom HTTP request-header: ◆ **Authorization:** Select *Use* to add the Authentication ID and the password from the Authentication section into this request-header field. ◆ **Key:** Specify Authorization as the keyword for the HTTP request-header field. ◆ **Value:** Specify the value to associate with the keyword in an HTTP request-header field. ◆ **Context Type:** Select *Use* to add the media type to the HTTP request-header field to comply with RFC 2376. ◆ **Key:** Specify Content-Type to set an HTTP request-header field. ◆ **Value:** Specify text/xml; charset=uf-8 as the value of the keyword in the HTTP request-header field. ◆ **SOAPAction:** Select *Use* to enable the SOAPAction HTTP request header field to indicate the intent of the SOAP HTTP request. ◆ **Key:** Specify SOAPAction to set an HTTP request-header field. ◆ **Value:** Specify #batchRequest as the value of the HTTP request-header.

Table A-7 *Publisher Settings*

Parameter	Description
Heartbeat interval in minutes	Specify the heartbeat interval in minutes. Leave this field blank to turn off the heartbeat.

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 SAP Portal driver includes several predefined GCVs. You can also add your own if you need additional ones as you implement policies in the driver.

To access the driver’s GCVs in iManager:

1 Click to display the Identity Manager Administration page.

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

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

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

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

2d Click the GCVs page.

3. Modify the GCVs as necessary, using the information in Table A-8.

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*.
3. Modify the GCVs as necessary, using the information in Table A-8.

Table A-8 *Global Configuration Values*

Option	**Description**
Driver parameters > Connected System or Driver Name	The name of the connected system, application, or Identity Manager driver. This value is used by the e-mail notification templates.
Entitlement Options > Show entitlements configuration	Select *Show* to display the entitlements configuration for this driver.
Entitlements Options > Use User Account Entitlement	Entitlements act like an on/off switch to control access. When the driver is enabled for entitlements, accounts are only created and removed or disabled when the account entitlement is granted to or revoked from users. Select *True* to enable the user account entitlement. You must have an entitlement agent configured in your environment. For more information about entitlements, see the *Identity Manager 3.6.1 Entitlements Guide*.
Entitlements Options > Action when account entitlement revoked	Select which action is taken in the SAP system when a User Account Entitlement is revoked. The options are to disable the account or to delete the account.
Entitlements Options > Use Portal Role Entitlement	Enables the Portal Role entitlement that is included with the driver. Select *True* to enable this entitlement.
Entitlements Options > User Portal Group Entitlement	Enables the Portal Group entitlement that is included with the driver. Select *True* to enable this entitlement.
Password Management > Show password management policy	Displays password management policies. You should edit the Password Management options on the *Server Variable* tab rather than under the GCVs. The *Server Variable* tab has a better view of the relationship between the different GCVs. For more information about how to use the Password Management GCVs, see "Configuring Password Flow " in the *Identity Manager 3.6.1 Password Management Guide*.

Option	Description
Account Tracking > Show Account Tracking Configuration	Select *show* to display the GCVs for Account Tracking through Novell® Sentinel™. Select *hide* to not have the GCVs displayed. Account Tracking is a feature included with the Novell Compliance Management Platform. For more information, see the "*Novell Compliance Management Platform Web site*" (http://www.novell.com/products/compliancemanagementplatform/).
Role Mapping > Show role mapping configuration	Select show to display the GCVs for enabling the driver to work with the Role Mapping Administrator. The Role Mapping Administrator is an application that is part of the Novell Compliance Management Platform for SAP. For more information, see the *"Novell Compliance Management Platform extension for SAP environments Web site"* (http://www.novell.com/documentation/ncmp_sap10/).