Fan-Out Driver for SAP User Management Implementation Guide

Identity Manager 4.0.2

October 2012

Novell

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 © 2009-2012 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.
1800 South Novell Place
Provo, UT 84606
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 7

1 Overview 9

1.1 Terminology . . . 9
1.2 Supported Versions . . . 10
1.3 How It Works . . . 10
1.4 Driver Components . . . 11
1.5 Support for Standard Driver Features . . . 12
1.5.1 Local Platforms . . . 12
1.5.2 Remote Platforms . . . 12
1.5.3 Entitlements . . . 12
1.5.4 Password Synchronization . . . 12
1.5.5 Account Tracking . . . 12
1.5.6 Identity Manager Role Mapping Administrator . . . 13

2 Fan-Out Configuration 15

2.1 Association Format . . . 15
2.2 DN Format . . . 16
2.3 User Account Entitlement . . . 17
2.4 Fan-out Life Cycle Process . . . 18

3 Installing the SAP User Management Fan-Out Driver Files 19

4 Configuring the SAP System 21

4.1 Clients and Logical Systems . . . 21
4.2 Defining Sending and Receiving Systems . . . 21
4.2.1 Creating a Logical System . . . 22
4.2.2 Assigning a Client to the Logical System . . . 22
4.3 Creating a Distribution Model . . . 22
4.4 Creating a Port Definition . . . 23
4.4.1 Creating a TRFC Port Definition . . . 23
4.4.2 Creating a File Port Definition . . . 24
4.5 Generating Partner Profiles . . . 25
4.5.1 Generating a Profile . . . 25
4.5.2 Modifying the Port Definition . . . 25
4.6 Activating Central User Administration . . . 26
4.7 Creating a Communication (CPIC) User . . . 26
4.8 Configuring SAP Gateway Ports . . . 27

5 Testing the SAP JCo Client Connection 29

5.1 About the Utility . . . 29
5.1.1 Utility Prerequisites . . . 30
5.1.2 Components . . . 30
5.1.3 Running and Evaluating the Test . . . 30
5.1.4 Understanding Test Error Messages . . . 32

6 Creating a New Driver Object **35**

6.1 Creating the Driver Object in Designer . . . 35
6.1.1 Importing the Current Driver Packages . . . 35
6.1.2 Installing the Driver Packages . . . 36
6.1.3 Using Designer to Adjust the Driver Settings . . . 40
6.1.4 Using Designer to Deploy the Driver Object . . . 40
6.1.5 Using Designer to Start the Driver . . . 41
6.2 Activating the Driver . . . 41
6.3 Adding Packages to an Existing Driver . . . 41

7 Upgrading an Existing Driver **45**

7.1 What's New in Version 4.0.2 . . . 45
7.2 Upgrade Procedure . . . 45

8 Implementing the Preconfigured Entitlements **47**

8.1 Entitlement Agents . . . 47
8.2 Preconfigured Entitlements . . . 48
8.2.1 User Account Entitlement . . . 48
8.2.2 Role (Activity Group) Entitlement . . . 48
8.2.3 Profile Entitlement . . . 49

9 Managing the Driver **51**

10 Troubleshooting the Driver **53**

10.1 Troubleshooting the SAP User Management Fan-Out Driver . . . 53
10.1.1 The Account Tracking Feature Does Not Work Properly for the Existing Users . . . 53
10.1.2 Error Occurs When Uninstalling the Driver . . . 53

A Driver Properties **55**

A.1 Driver Configuration . . . 55
A.1.1 Driver Module . . . 56
A.1.2 Authentication . . . 56
A.1.3 Startup Option . . . 57
A.1.4 Driver Parameters . . . 58
A.1.5 ECMAScript . . . 62
A.1.6 Global Configurations . . . 63
A.2 Global Configuration Values . . . 63
A.2.1 Entitlements . . . 64
A.2.2 Password Synchronization . . . 66
A.2.3 Account Tracking . . . 66
A.2.4 Managed System Information . . . 67
A.2.5 SAP User Management Driver . . . 68

B Application Link Enabling (ALE) **69**

B.1 Clients and Logical Systems . . . 69
B.2 Message Type . . . 70
B.3 IDoc Type . . . 70
B.4 Distribution Model . . . 70
B.5 Partner Profiles . . . 70
B.6 Port . . . 70

B.7 Port Definition . . . 70
B.8 File Port . . . 71
B.9 TRFC Port . . . 71
B.10 CUA . . . 71

C Business Application Programming Interfaces (BAPIs) 73

D Configuration and Deployment Notes 75

D.1 SAP Object Types . . . 75
D.2 User Types: LOGONDATA:USTYP . . . 75
D.3 Output Controller Options . . . 76
D.4 Communication Types: ADDCOMREM:COMM TYPE . . . 76
D.5 Date Formats: DEFAULTS:DATAFM . . . 76
D.6 Decimal Formats: DEFAULTS:DCPFM . . . 76
D.7 Computer Aided Test (CATT): DEFAULTS:CATTKENNZ . . . 77
D.8 Communication Comment Type to Table Mappings . . . 77
D.9 Language Codes . . . 77
D.10 Configuration Parameters . . . 78
D.11 Design Comments and Notes . . . 78

E Example XML Document Received from the Driver 83

F Structured Format Examples 85

G Setting and Clearing Granular Locks 87

G.1 Configuring the SAP System for Granular Locking . . . 87
G.2 Configuring the Driver for Locking . . . 89

H Using Wildcard Search Capabilities 91

About This Guide

This guide explains how to install and configure the SAP User Management Fan-Out driver. It also explains how the SAP User Management Fan-out driver works.

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Fan-Out Configuration,” on page 15
- Chapter 3, “Installing the SAP User Management Fan-Out Driver Files,” on page 19
- Chapter 4, “Configuring the SAP System,” on page 21
- Chapter 5, “Testing the SAP JCo Client Connection,” on page 29
- Chapter 6, “Creating a New Driver Object,” on page 35
- Chapter 7, “Upgrading an Existing Driver,” on page 45
- Chapter 8, “Implementing the Preconfigured Entitlements,” on page 47
- Chapter 9, “Managing the Driver,” on page 51
- Chapter 10, “Troubleshooting the Driver,” on page 53
- Appendix A, “Driver Properties,” on page 55
- Appendix B, “Application Link Enabling (ALE),” on page 69
- Appendix C, “Business Application Programming Interfaces (BAPIs),” on page 73
- Appendix D, “Configuration and Deployment Notes,” on page 75
- Appendix E, “Example XML Document Received from the Driver,” on page 83
- Appendix F, “Structured Format Examples,” on page 85
- Appendix G, “Setting and Clearing Granular Locks,” on page 87
- Appendix H, “Using Wildcard Search Capabilities,” on page 91

Audience

This guide is intended for SAP and Identity Manager consultants.

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 and enter your comments there.

Documentation Updates

For the most recent version of the *Identity Manager Fan-Out Driver for SAP User Management Implementation Guide*, visit the Novell Identity Manager Drivers Documentation Web site (http://www.netiq.com/documentation/idm402drivers/index.html).

Additional Documentation

For documentation on Novell Identity Manager, see the Identity Manager Documentation Web site (http://www.netiq.com/documentation/idm402/index.html).

1 Overview

The SAP User Management Fan-Out driver provisions users and password to SAP application servers or child systems. This version of the User Management driver provides fan-out capabilities. A single driver can synchronize users to CUA systems and child systems.

- Section 1.1, "Terminology," on page 9
- Section 1.2, "Supported Versions," on page 10
- Section 1.3, "How It Works," on page 10
- Section 1.4, "Driver Components," on page 11
- Section 1.5, "Support for Standard Driver Features," on page 12

1.1 Terminology

This section gives you essential information about the terminology used with SAP. If you need further help with SAP terminology, see the Glossary for the SAP Library (http://help.sap.com/saphelp_46c/helpdata/En/35/2cd77bd7705394e10000009b387c12/frameset.htm).

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

ALE: Application Link Enabling. Technology that enables communication between SAP and external systems such as the Identity Vault. For more information, see Appendix B, "Application Link Enabling (ALE)," on page 69.

BAPI: Business Application Programming Interface. SAP has business APIs for the SAP business object types. For more information, see Appendix C, "Business Application Programming Interfaces (BAPIs)," on page 73.

CCMS: Computer Center Management System. A set of tools to monitor, control, and configure an SAP system.

client: In an SAP system, a self-contained unit with its own set of users and data.

CUA: Central User Administration. The SAP tool used to centrally maintain user master records.

ERP: Enterprise resource planning. A software system for planning and automating enterprise-wide business processes.

GRC: Governance, risk, and compliance. Software or business processes that facilitate conformity to legal requirements.

IDocs: Intermediate document. A data exchange format used between SAP systems and between SAP systems and external applications. For more information, see Section B.3, "IDoc Type," on page 70.

JCo: SAP Java Connector. A toolkit that allows Java applications to communicate with any SAP system.

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.

SSCR: SAP Software Change Registration. A procedure for registering manual changes to SAP source code and dictionary object.s

UME: User Management Engine. Provides central user administration for Java applications.

XAL: External interface for alert management. Enables external system management software to read and set properties in order to integrate with SAP administration tools.

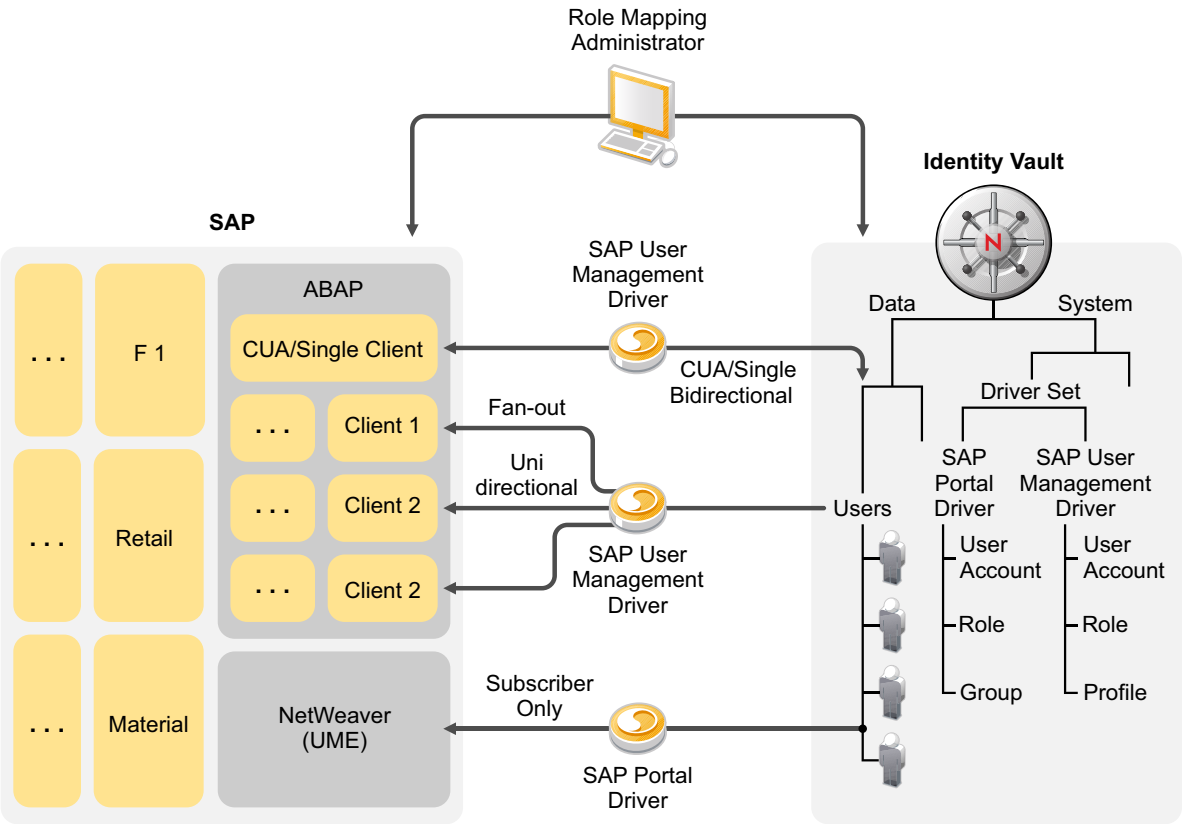
1.2 Supported Versions

This driver supports the same platforms that are supported by JCo 3. Use JCo 3.0.2 or later. Full driver functionality is available only when it is used with a fully patched SAP Basic 7.00 system or later.

1.3 How It Works

The SAP User Management driver can be configured to work with a single client (standalone non-CUA, CUA, central client, or a CUA child client). In this configuration, the synchronization is bidirectional if the client is a CUA central client and it is unidirectional (from the Identity Vault to SAP) in all other configurations. In all cases, the driver can subscribe passwords. It can also be configured to connect to multiple clients in a fan-out configuration. In this configuration, the synchronization is bidirectional to the client on the primary connection, if the client is a CUA central client, and it is unidirectional (from the Identity Vault to SAP) in all other configurations. Each additional connection the fan-out driver makes is a secondary connection, and each secondary connection is also unidirectional. The driver can subscribe passwords in all configurations. For more information about the fan-out configuration, see Chapter 2, “Fan-Out Configuration,” on page 15.

Figure 1-1 *SAP User Management Driver Configurations*



1.4 Driver Components

This section contains information about the following driver components:

- **Driver Packages:** There are multiple packages that contain policies and entitlements that make the driver work. These are what allows the driver to become a fan-out driver or a traditional driver.

  For more information, see Chapter 6, "Creating a New Driver Object," on page 35.

- **Driver Shim:** The driver shim handles communication between the SAP clients and the Metadirectory engine.

  The driver shim filename is `sapumshim.jar`.

  For installation information, see Chapter 3, "Installing the SAP User Management Fan-Out Driver Files," on page 19.

- **SAP User Java Connector Test Utility:** In order to use the driver, you must download and install SAP JCo version 3. The SAP JCo 3 Test utility enables you to check for JCo installation and configuration issues prior to configuring the driver. You can use the JCo 3 test utility to validate the installation of JCo 3, connectivity to the SAP host system, as well as testing for the accessibility of the user management BAPIs used by the driver.

The JCo 3 test utility filename is `UserJCO3Test.class`.

For more information, see Chapter 5, "Testing the SAP JCo Client Connection," on page 29.

1.5 Support for Standard Driver Features

The following sections provide information about how the SAP User Management Fan-Out driver supports standard driver features:

- Section 1.5.1, "Local Platforms," on page 12
- Section 1.5.2, "Remote Platforms," on page 12
- Section 1.5.3, "Entitlements," on page 12
- Section 1.5.4, "Password Synchronization," on page 12
- Section 1.5.5, "Account Tracking," on page 12
- Section 1.5.6, "Identity Manager Role Mapping Administrator," on page 13

1.5.1 Local Platforms

The SAP User Management Fan-Out driver can be installed on the same operating systems supported by the Metadirectory server and JCo 3. For information, see "System Requirements" in the *Identity Manager 4.0.2 Integrated Installation Guide*.

1.5.2 Remote Platforms

If you don't want to install the Metadirectory engine and Identity Vault (eDirectory) on the SAP server, you can use the Remote Loader service to run the driver on the SAP server, and have the Metadirectory engine and Identity Vault on another server.

The SAP User Management Fan-Out driver can be installed on the same operating systems supported by the Remote Loader and JCo 3. For information, see "Configuring the Remote Loader" in the *Identity Manager 4.0.2 Remote Loader Guide*.

1.5.3 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 User Management Fan-Out driver contains preconfigured entitlements. For more information, see Chapter 8, "Implementing the Preconfigured Entitlements," on page 47.

1.5.4 Password Synchronization

The SAP User Management Fan-Out driver supports setting passwords in the SAP system. You can configure the driver to automatically assign passwords to users when they are provisioned to the SAP systems and child systems. For configuration information, see the *Identity Manager 4.0.2 Password Management Guide*.

1.5.5 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 Identity Reporting Module. For more information, see the *Identity Reporting Module Guide*.

1.5.6 Identity Manager Role Mapping Administrator

The SAP User Management Fan-Out 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 Identity Manager Advanced Edition. For more information, see the *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide*.

2 Fan-Out Configuration

The fan-out configuration of the SAP User Management driver provisions one object in the Identity Vault to multiple SAP clients. The SAP User Management Fan-Out driver supports publishing only on the primary connection and not to any additional connections in the fan-out configuration. To support the Publisher channel, the primary connection must be made to a CUA central client.

The SAP User Management Fan-Out driver does fan-out by associations and the destination DN. The policies use entitlements to generate the correct event format for the driver to consume.

- Section 2.1, "Association Format," on page 15
- Section 2.2, "DN Format," on page 16
- Section 2.3, "User Account Entitlement," on page 17
- Section 2.4, "Fan-out Life Cycle Process," on page 18

2.1 Association Format

The association format has changed in the SAP User Management Fan-Out driver. Table 2-1 shows the changes in the association format. The new driver is backward compatible. The older drivers do not support the newer format.

Table 2-1 *Association Format*

Old Association Format	New Association Format
USd<USERNAME> • **US:** The class. • **d:** A delimiter. • **<USERNAME>:** The unique identifier and username in the SAP system. For example: USdBERG	<LSNAME>USd<USERNAME> • **<LSNAME>:** The logical system name where events are sent. • **US:** The class • **d:** A delimiter. • **<USERNAME>:** The unique identifier and username in the SAP system. For example: \S71CLNT800\USdABERG

The two main points to remember the association format are:

- The association is very close to a DN format.
- The first part of the association contains an identifier that tells the shim which logical system receives the event.

The following is an example of the association format in a trace:

```
<nds dtdversion="3.5" ndsversion="8.x">
  <source>
    <product version="3.6.0.4294">DirXML</product>
    <contact>Novell, Inc.</contact>
  </source>
 <input>
   <modify class-name="US" event-id="metaserver1#20090513130202#1#2#0" from-
merge="true" src-dn="\META\data\company\users\aberg" src-entry-id="40801">
      <association>\S7ICLNT800\USdABERG</association>
      <modify-attr attr-name="ADDRESS:FULLNAME">
        <add-value>
          <value timestamp="1234481823#65" type="string">Berg Andrea</value>
        </add-value>
      </modify-attr>
   </modify>
 </input>
</nds>
```

If the driver is running in fan-out mode, there are multiple associations added to the user object. They are required for fan-out to work correctly. The format of the association is:

```
fanout1-xTFRgkLOmElpuMUxUYJCzg==
fanout2-xTFRgkLOmElpuMUxUYJCzg==
```

The `xTFRgkLOmElpuMUxUYJCzg==` value is the GUID of the User object in the Identity Vault.

2.2 DN Format

The legacy SAP User driver did not have a concept of DNs. Placement was not done using the DN, and the username of an account in SAP was not determined through the destination-dn, but from the value of the USERNAME:BAPINAME attribute. This attribute was required and contained a value for every add event going to the SAP system.

The User Management Fan-Out driver introduces the concept of a DN in a format similar to the one already used by the association. The DN format is \<LSNAME>\<USERNAME>, where <LSNAME> is the name of the logical system where events are sent and <USERNAME> is a unique identifier and username in the SAP system.

The DN format does not contain a class identifier. To determine the correct object type when only a destination DN is available, the driver relies on the class-name attribute of the event.

Placement is done through regular placement policies. The placement policies specify the logical system and the username, then the driver places the account in the correct system with the correct name.

For backward compatibility, the driver still supports the legacy way of naming new accounts in SAP. If an add event contains an attribute USERNAME:BAPINAME, the value of the attribute always takes precedence over the leaf portion of the destination DN. The policies in the driver packages use the new destination DN placement method exclusively. The USERNAME:BAPINAME attribute is not populated on outgoing events.

The following is an example of the DN format in a trace:

```
<nds dtdversion="3.5" ndsversion="8.x">
  <source>
    <product version="3.6.0.4294">DirXML</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <add class-name="US" dest-dn="\S7ICLNT800\ABERG" event-
id="metaserver1#20090513131408#1#2#0" src-dn="\META\data\company\users\aberg">
      <add-attr attr-name="UCLASS:LIC_TYPE">
        <value timestamp="1235208846#1" type="string"/>
      </add-attr>
      <add-attr attr-name="ADDRESS:FULLNAME">
        <value timestamp="1234481823#65" type="string">Berg Andrea</value>
      </add-attr>
      <add-attr attr-name="ADDRESS:FIRSTNAME">
        <value timestamp="1241800246#8" type="string">Andrea</value>
      </add-attr>
      <add-attr attr-name="ADDRESS:LASTNAME">
        <value timestamp="1234410222#28" type="string">Berg</value>
      </add-attr>
      <add-attr attr-name="LOGONDATA:USTYP">
        <value type="string">A</value>
      </add-attr>
      <add-attr attr-name="LOCKUSER">
        <value type="state">0</value>
      </add-attr>
      <password><!-- content suppressed --></password>
    </add>
  </input>
</nds>
```

2.3 User Account Entitlement

The SAP User Management Fan-Out packages contain entitlement policies and a set of preconfigured entitlements. The User Account entitlement is used with the fan-out configuration.

Most Identity Manger drivers support the User Account entitlement as an entitlement that can only be granted once and does not take any parameters. It is like an on/off switch for the account in the application. There is a one-to-one relationship between the User Account entitlement and one account in the application. The fan-out configuration requires that a single User object in the Identity Vault be granted multiple User Account entitlements for accounts in different systems. A parameter is added to the User Account entitlement, so each time the entitlement is granted it is a unique event. The parameter indicates the system where the account is granted.

The SAP User Management Fan-Out packages contain a new version of the User Account entitlement and the policies that implement the entitlement. The entitlement can be granted multiple times and uses the parameter that tells the policies where to send the events.

The format of the parameter is:

```
LSNAME=<LSNAME>
```

The LSNAME is the same system identifier (SAP logical system name) that is found in the association and in the destination DN.

The following is an example of the User Account entitlement in a trace:

```
<nds dtdversion="3.5" ndsversion="8.x">
  <source>
    <product version="3.6.0.4294">DirXML</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <add class-name="User" event-id="metaserver1#20090513130202#1#2#0" src-
dn="\META\data\company\users\aberg">
      ...
      <add-attr attr-name="DirXML-EntitlementRef">
        <value timestamp="1242219722#1" type="structured">
          <component name="nameSpace">1</component>
          <component name="volume">\META\system\services\idm\driverset1\SAP-
USER\UserAccount</component>
          <component name="path.xml">
            <ref>
              <src>NRF</src>
              <id>1242219722981</id>
              <param>LSNAME=S7ICLNT800</param>
            </ref>
          </component>
        </value>
      </add-attr>
      ...
    </add>
  </input>
</nds>
```

2.4 Fan-out Life Cycle Process

The fan-out process works as follows:

1. A user in the Identity Vault is granted a User Account entitlement.
2. Based on the entitlement parameter value, the policies create the destination DN that places a new account in the corresponding SAP client.
3. The driver adds an association to the user in the Identity Vault.
4. All changes to the object in the Identity Vault are fanned out based on the specific association.

3 Installing the SAP User Management Fan-Out Driver Files

By default, the SAP User Management Fan-Out driver files are installed when you install the Metadirectory server. The installation program extends the Identity Vault schema and installs the driver shim. The driver packages are included in the latest version of Designer. The installation does not create the driver in the Identity Vault (see Chapter 6, "Creating a New Driver Object," on page 35) or upgrade an existing driver (see Chapter 7, "Upgrading an Existing Driver," on page 45).

If you performed a custom installation and did not install the SAP User Management Fan-Out driver on the Metadirectory server, you have two options:

- Install the files on the Metadirectory server, using the instructions in "Installing the Metadirectory Server" in the *Identity Manager 4.0.2 Framework Installation Guide*.
- Install the Remote Loader (required to run the driver on a non-Metadirectory server) and the driver files on a non-Metadirectory server where you want to run the driver. This the method you should use if you do not want to install the Identity Vault and Identity Manager on the SAP server. For installation instructions, see "Installing the Remote Loader" in the *Identity Manager 4.0.2 Framework Installation Guide*.

You also need to create a driver object, but first you must configure the SAP system to work with the SAP User Management Fan-Out driver. Proceed to Chapter 4, "Configuring the SAP System," on page 21, or if the SAP system is configured, continue with Chapter 6, "Creating a New Driver Object," on page 35.

4 Configuring the SAP System

You must configure the SAP system parameters to enable Application Link Enabling (ALE) and Central User Administration (CUA) processing of USERCLONE IDocs if you want to publish real-time changes of SAP User data to the Identity Vault. Before you continue, make sure you have sufficient rights to configure the distribution model and to distribute user data via ALE.

- Section 4.1, "Clients and Logical Systems," on page 21
- Section 4.2, "Defining Sending and Receiving Systems," on page 21
- Section 4.3, "Creating a Distribution Model," on page 22
- Section 4.4, "Creating a Port Definition," on page 23
- Section 4.5, "Generating Partner Profiles," on page 25
- Section 4.6, "Activating Central User Administration," on page 26
- Section 4.7, "Creating a Communication (CPIC) User," on page 26
- Section 4.8, "Configuring SAP Gateway Ports," on page 27

4.1 Clients and Logical Systems

In the SAP configuration for the driver, a logical system is a representation of either a SAP system or an external system. The logical system is used to distribute data to and from SAP. To use ALE, every SAP system needs to have a base logical system associated with a client. There is a one-to-one relationship between the client and the logical system.

The driver uses an outbound ALE interface. In an outbound ALE interface, the base logical system becomes the *sender* for outbound messages and the *receiver* of inbound messages. A SAP user is probably logged into the base logical system/client when making changes to the database (for example, modifying User profiles or logon preferences). A logical system/client must also be defined for the receiving client. This logical system acts as the receiver of outbound messages.

4.2 Defining Sending and Receiving Systems

In order to distribute data between systems you must first define both the sending and receiving systems as unique logical systems.

For this particular solution, we recommend defining two logical systems. One logical system represents the driver and acts as the *receiver* system. The other logical system represents the SAP system and acts as the *sender* system. Because only one of these clients is used as a data source (that is, the client/logical system where SAP User data is stored and "actions" occur), there is no need to assign a client to the receiving logical system.

NOTE: Depending on your current SAP environment, you might not need to create a logical system. You might only need to modify an existing Distribution Model by adding the USERCLONE message type to a previously configured Model View. For more information, see "Creating a Distribution Model" on page 22.

It is important, however, that you follow SAP's recommendations for logical systems and configuring your ALE network. The following instructions assume that you are creating new logical systems and a new model view.

- Section 4.2.1, "Creating a Logical System," on page 22
- Section 4.2.2, "Assigning a Client to the Logical System," on page 22

4.2.1 Creating a Logical System

1. In SAP, enter transaction code `BD54`.
2. Click *New Entries*.
3. Type an easily identifiable name to represent the SAP *sender* system.

   SAP recommends the following format for logical systems representing R/3 clients: *systemID*CLNT*client number* (such as ADMCLNT100).
4. Type a description for the logical system (such as Central System for SAP User Distribution).
5. Add a second logical system name to represent the Identity Manager external *receiver* system (such as DRVCLNT100).
6. Type a description for the logical system (such as Identity Manager User Management Integration).
7. Save your entries.

4.2.2 Assigning a Client to the Logical System

1. In SAP, enter transaction code `SCC4`.
2. Click *Table View* > *Display* > *Change* to switch from display to change mode.
3. Select the client from which you want User information distributed (such as 100).
4. Click *Goto* > *Details* > *Client Details*.
5. In the *Logical System* field, browse to and select the *sender* logical system you want to assign to this client (such as ADMCLNT100).
6. Save your entry.

4.3 Creating a Distribution Model

The distribution model contains essential information about message flow. The model view defines the systems that will communicate with each other and the messages that will flow between them. The distribution model forms the basis of distribution and controls it directly.

To create a distribution model:

1. Verify that you are logged in to the sending system/client.
2. In SAP, enter transaction code `BD64`. Ensure that you are in Change mode (click *Table View* > *Display* > *Change*.)

3 Click *Edit* > *Model View* > *Create*.

4 Type the short text to describe the distribution model (such as Client 100 Distribution to Identity Manager).

5 Type the technical name for the model (such as SAP2IDM).

6 Accept the default start and end dates or specify valid values. Click the check mark icon to save your entry.

7 Select the view you created, then click *Add BAPI*.

8 In the *Sender/Client* field, type the name of the *sender* logical system (such as ADMCLNT100).

9 In the *Receiver/Client* field, type the name of the *receiver* logical system (such as DRVCLNT100).

10 In the *Obj. Name/Interface* field, add the USER object name.

Ensure that you add the USER object name with all capital letters.

11 In the *Method* field, add Clone.

12 Click the check mark icon to save the BAPI.

13 Select the SAP2IDM model view.

14 Click *Add BAPI*.

15 Define the sender (logical system ADMCLNT100).

16 Define the receiver (logical system DRVCLNT100).

17 In the *Obj. Name/Interface* field, add the UserCompany object name.

18 In the *Method* field, add Clone.

19 Click the check mark icon to save your BAPI entries.

20 Save the Distribution Model entries.

4.4 Creating a Port Definition

The port is the communication channel to which IDocs are sent. The port describes the technical link between the sending and receiving systems.

The driver can be configured to support a connection via a TRFC port or to consume IDocs distributed via a File port. The driver packages assumes that you use the TRFC port configuration.

- Section 4.4.1, "Creating a TRFC Port Definition," on page 23
- Section 4.4.2, "Creating a File Port Definition," on page 24

4.4.1 Creating a TRFC Port Definition

A Transactional Remote Function Call (TRFC) can be used in the integration solution. IDocs are transferred to a specified application process (such as the driver) via the SAP Gateway.

Complete the following two tasks to create a TRFC port definition:

- "Creating the RFC Destination" on page 24
- "Creating the TRFC Port Definition" on page 24

Creating the RFC Destination

If you are distributing data to multiple drivers, each driver must have a unique RFC destination and program ID.

1. In SAP, enter transaction code `SM59`.
2. Click the *Create* icon.
3. Name the RFC destination (use the driver's logical system name, such as, DRVCLNT100.)
4. Select *T* as the connection type (for a TCP/IP connection.)
5. Add a description for the destination (such as JCo Server in IDM User Driver.)
6. Save your entry.
7. Select the option for *Registration* or *Registered Server Program*. Type the program ID to be used for the driver. In the driver packages, this value is set to *IDMUser100*.
8. (Conditional) If the SAP server is configured to use a Unicode database, complete the following steps:
   - **8a** Select the *Special Options* tab.
   - **8b** Select *Unicode*.
9. Save your entry.

Creating the TRFC Port Definition

If you are distributing data to multiple drivers, each driver must have a unique TRFC port.

1. In SAP, enter transaction code *WE21*.
2. Select *Transactional RFC*, then click the *Create* icon.
3. Select *Own Port Option Name*.
   - **3a** Type a port name (such as IDMPORT).
   - **3b** Type a description for the port definition (such as Port to IDM User Driver).
   - **3c** Select a version (such as IDoc record types SAP release 4.X)
   - **3d** Specify the RFC destination. This is the name of the RFC destination representing the driver (such as DRVCLNT100.)
4. Save your entry.

4.4.2 Creating a File Port Definition

A file port can be used in the integration solution. IDocs are transferred to a file in a specified file system location accessible by the SAP host system.

If you are distributing data to multiple drivers, each driver must have a unique file port.

1. In SAP, type transaction code `WE21`.
2. Select *File*, then click the *Create* icon.
   - **2a** Type a port name (such as IDMFILE).
   - **2b** Type a port description (such as File Port to IDM User Driver).
   - **2c** Select a version (such as SAP release 4.X).

3 Define the outbound file:

   3a Select the physical directory. This is the directory where you want IDocs placed. You might need to create this directory.

   Type the directory where the outbound files are written, for example: `\\sapdev\nov\sys\global\sapndsconnector`.

   3b Type the function module name. This names the IDoc file in a specific format. Use the following format: `EDI_PATH_CREATE_CLIENT_DOCNUM`.

4 Save your changes.

   You do not need to configure the other three tabs for the port properties (outbound:trigger, inbound file, and status file).

4.5 Generating Partner Profiles

The system automatically generates a partner profile or you can manually maintain the profile.

NOTE: If you are using an existing distribution model and partner profile, you do not need to generate a partner profile. Instead, you can modify it to include the USERCLONE BAPI.

- Section 4.5.1, "Generating a Profile," on page 25
- Section 4.5.2, "Modifying the Port Definition," on page 25

4.5.1 Generating a Profile

1 In SAP, enter transaction code `BD82`.

2 Select the *Model View*. This should be the Model View previously created in "Creating a Distribution Model" on page 22.

3 Ensure that the *Transfer IDoc Immediately* and *Trigger Immediately* option buttons are selected.

4 Click the *Execute* icon.

   When the status screen appears, ignore any red error or warning messages related to the driver's logical system.

4.5.2 Modifying the Port Definition

The port definition might have been generated incorrectly. For your system to work properly, you might need to modify the port definition.

1 In SAP, enter transaction code `WE20`.

2 Select *Partner Type LS*.

3 Select your *receiver* logical system (such as DRVCLNT100).

4 Click the *Create Outbound Parameter* icon, then select message type *USERCLONE*.

5 Modify the receiver port so it is the *file* or *TRFC port name* you created earlier (such as IDMPORT or IDMFILE).

6 Under *Output Mode*, select *Transfer IDoc Immediately* to send IDocs immediately after they are created.

7 In the IDoc Type section, select the *Basic type* and the appropriate *USERCLONE*:

   - For SAP 4.5, select USERCLONE01

- For SAP 4.6a, select USERCLONE02
- For SAP 4.6c, select USERCLONE03
- For SAP 6.10, select USERCLONE04
- For SAP 6.20 or greater, select USERCLONE05

8 Save your entries.

NOTE: The following procedures are necessary only if you want to distribute company address data.

---

9 Click the *Create Outbound Parameter* icon, then select message type *CCLONE*.

10 Modify the receiver port so it is the *file* or *TRFC port name* you created earlier (such as IDMPORT or IDMFILE.)

11 (Conditional) If you are using a TRFC port, modify the packet size. Select *Packet Size = 1*.

12 Under *Output Mode*, select *Transfer IDoc Immediately* to send IDocs immediately after they are created.

13 In the *IDoc type* section, select *Basic type* and the appropriate *CCLONE*. (For all SAP versions, select *CCLONE01*.)

14 Save your entries.

4.6 Activating Central User Administration

Central User Administration (CUA) is the process that activates the distribution model.

1 In SAP, enter transaction code `SCUA`.

2 In the Maintain System Landscape dialog box, select the distribution *Model View* previously created (such as SAP2IDM).

3 Save your entry.

You might see a message stating `Unable to distribute the system landscape to system IDMDRV.` This is an informative message and is not an error or issue of concern.

On some versions of SAP, all systems in the distribution, including the Identity Manager driver, must be accessible during this step. If a TRFC port is being used for the driver Publisher channel, the driver should be running to ensure connectivity and completion of the CUA configuration.

4.7 Creating a Communication (CPIC) User

Users are client-independent. For each client that uses the driver, a system user with CPIC access must be created.

1 In SAP, enter transaction code `SU01`.

2 From *User Maintenance*, enter a username in the User dialog box (such as IDM_CPIC), then click the *Create* icon.

3 Click the *Address* tab, then type data in the last name fields (Last_IDM).

4 Click the *Logon Data* tab, then define the *initial password* and set the user type to *CPIC* (Communication).

5 Click the *Profiles* tab, then add the *S_A.CPIC profile*. The driver must also have sufficient rights to perform required operations, which might include *SAP_ALL* and *SAP_NEW* depending on your company's system security policy.

We recommend using the most restrictive rights possible.

6 Click the *Systems* tab. Add the *logical name* of the *sender* system (such as ADMCLNT100). This enables the CPIC user to authenticate to the client system.

7 Click *Save*.

NOTE: Initially, you can create a dialog user to test your SAP system configuration. If there are processing problems, you can analyze the dialog user in the debugger. You should also log into the SAP system once to set this user's password. After the system is tested and works properly, you should switch to a CPIC user for security measures.

4.8 Configuring SAP Gateway Ports

The SAP system expects to use ports 3300 through 3399 for SAP gateways. If the Publisher channel of the SAP User driver connects as a JCo server and that server is configured to connect to a gateway on System 01, then SAP tries to connect to the driver on port 3301. If the System is 11, then port 3311 is expected.

The automatic configuration of these ports is prohibited in SUSE Linux Enterprise Server, Windows 2008 64-bit server, and Solaris 64-bit server. For these operating systems, the ports must be manually configured in the following files:

Linux/UNIX: `/etc/services`

For example:

```
sapgw01   3301/tcp  # SAP Gateway for IDM User Driver JCO
```

Windows: `C:\WINDOWS\system32\drivers\etc\services file`

For example:

```
sapgw01   3301/tcp
```

5 Testing the SAP JCo Client Connection

The driver uses the SAP Java Connector Fan-Out and Business Application Programming Interface (BAPI) technologies to connect to and integrate data with the Identity Vault. The SAP JCo is a SAP client that creates service connections to a SAP application server. After the driver is connected to the SAP application server, it calls methods on business objects within the SAP application server via BAPI.

The SAP Java Connector Test utility enables you to check for JCo installation and configuration issues. Use the JCo Test utility to validate installation and connectivity to the SAP JCo client, as well as testing for accessibility to the BAPIs used by the driver.

Ensure that you are using JDK/JRE version 1.6 or later, and JCo version 3.0.2 or later:

- "About the Utility" on page 29
- "Running and Evaluating the Test" on page 30
- "Understanding Test Error Messages" on page 32

5.1 About the Utility

The JCo Test utility completes the following checks:

- Ensures the presence of the file `sapjco3.jar` file, which contains the exported JCo interface.
- Ensures that the JCo native support libraries are properly installed.
- Ensures that connection parameters to the SAP target system are correct.
- Ensures that the authentication parameters to the SAP target system are correct.
- Ensures that the selected language code is valid.
- Ensures that the BAPIs used by the driver are present as expected for the version of the SAP target system.

The following sections help you use the utility.

- Section 5.1.1, "Utility Prerequisites," on page 30
- Section 5.1.2, "Components," on page 30
- Section 5.1.3, "Running and Evaluating the Test," on page 30
- Section 5.1.4, "Understanding Test Error Messages," on page 32

5.1.1 Utility Prerequisites

Before you run the JCo Test utility, you must install the SAP JCo client for the desired platform. The JCo can only be obtained from the SAP Service Marketplace Web site (http://www.sap-ag.de/services). The download is free to any SAP software customer or development partner, but you are required to log in.

In order to configure the driver, you must first download the SAP JCo 3 and install it. For installation instructions, refer to the documentation accompanying the SAP JCo.

Follow the installation instructions for your platform. Each installation requires you to set one or two environment variables, such as CLASSPATH for the `sapjco3.jar` file location. For the UNIX platforms, set either the LD_LIBRARY_PATH or LIBPATH variables for the location of native support libraries. Ensure that these variables are set in the shell environment to run this test and for the subsequent use of the Identity Manager Driver for User Management of SAP Software.

You must also make sure that you have your PATH environment variable set to include the path to your Java executable file. For Win32 platforms, the environment variables are set via the System configuration in the Control Panel. On UNIX systems, edit the appropriate `.profile` or `.bash_profile` to include and export these path variables.

5.1.2 Components

The JCo Test utility consists of the `UserJCO3Test.class` file. The format of an execution batch or script file varies, depending on the platform on which the JCo client has been installed.

The basic content of the file includes a path to the Java executable (or just `java` if your PATH is appropriately configured), and the name of the `UserJCO3Test.class` file. A sample UNIX script file and Win32 batch file are listed below, where `sapjco3.jar` is in the executable directory of the `UserJCOTest3.class` file and the batch file:

```
Win32 jcotest.bat file
java -classpath %CLASSPATH%;. UserJCO3Test

Unix jcotest file
java UserJCO3Test
```

You must use proper slash notation when specifying pathnames, and you must use the proper classpath delimiter for the platform. You must also remember that the name of the `sapjco3.jar` file is case-sensitive on UNIX platforms and that the name of the test class, UserJCO3Test, must be specified with proper case for any platform.

5.1.3 Running and Evaluating the Test

- "Running the Test" on page 31
- "Evaluating the Test" on page 31
- "Post-Test Procedures" on page 32

Running the Test

To run the JCo Test utility on a Win32 platform:

1. From Windows Explorer, double-click `UserJCO3Test.bat`.
   or
   From a command prompt, run the `UserJCO3Test.bat` script.

To run the JCo Test utility on a UNIX platform:

1. From your preferred shell, run the `userjco3test` script file.

NOTE: When you run the test program, an error message might appear before any test output is displayed. This indicates an improper installation of the JCo client components. The error messages are documented for each platform in "Understanding Test Error Messages" on page 32.

Evaluating the Test

If the JCo client is installed properly, the following output is displayed:

```
**The SAP JCO client installation has been verified to be correct.

Version of the JCO-library: version information

Input SAP Server Connection Information
----------------------------------------
```

You then receive a series of prompts for connection and authentication information. All data must be provided unless a default value, identified by [] delimiters, is provided. Failure to fill in a response value to each prompt ends the test. Enter the following when prompted:

- Application server name or IP address
- System number [00]
- Client number
- User
- User password
- Language code [EN]

The values you provide are the same values that could be used to authenticate via the SAPGUI client. Based on the validity of the input, the test either displays error messages with solution suggestions or runs to completion. At the end of the test, a status message displays. If the test indicates full functionality as required by the driver, the following status message appears (it describes valid values that can be used as the configuration parameters for the driver):

```
JCO Test Summary
----------------
The following parameters might be used for SAP User Management Driver Configuration

Authentication ID: Username
Authentication Context: SAP Host Name/IP Address
Application Password: User password
SAP System Number: System Number
SAP User Client Number: Client Number
SAP User Language: Language Code
SAP System ID: System ID
Character Set Encoding: Encoding
All required BAPI and RFC Functionality has been verified.
```

If the test indicates that the functionality required by the driver is not available, the following status message is displayed:

```
JCO Test Summary
----------------
BAPI and RFC support is not complete. Review function list for details.
```

Full driver functionality is not possible if all functions are not available on the target SAP server. Patch the SAP server as needed.

Post-Test Procedures

After the JCo Test utility has successfully passed all tests, you can then begin to configure the driver. Make sure that the `sapjco3.jar` file is copied to the location where the `sapumshim.jar` file has been installed.

On UNIX systems, ensure that the environment variables used for the successful completion of the User JCo Test are also in the environment of the driver. If these conditions are met, there should be no driver errors that are related to the JCo.

5.1.4 Understanding Test Error Messages

Use the information in this section to analyze error messages that might display during the User JCo Test.

Table 5-1 *General Errors*

Error Message	Problem
`Caught Exception during connection: java.ang.Exception: SAP Connection Exception: com.sap.coon.jco.JCoException: (102) RFC_ERROR_COMMUNICATION: Connect to SAP gateway failed`	Bad address or system number.
`Caught Exception during connection: java.lang.Exception: SAP Connection Exception: com.sap.conn.jco.JCoException: (101) RFC_ERROR_PROGRAM: ‘client’ needs to be a three digit number string instead of ‘<input>’`	Bad client number format.
`Caught Exception during connection: java.lang.Exception: SAP Connection Exception: com.sap.conn.jco.JCoException: (101) RFC_ERROR_PROGRAM: ‘sysnr’ needs to be a two digit number string instead of ‘<input>’`	Bad number format.
`Caught Exception during connection: java.lang.Exception: SAP Connection Exception: com.sap.conn.jco.JCoException: (109) RFC_ERROR_CANCELLED: Handle closed pending`	Invalid credentials (JCo 3.0.1).
`Caught Exception during connection: java.lang.Exception: SAP Connection Exception: com.sap.conn.jco.JCoException: (103) RFC_ERROR_LOGON_FAILURE: Name or password is incorrect (repeat logon) on <host> sysnr <system number>`	Invalid credentials (JCo 3.0.2+).

Error Message	Problem
`Caught Exception during connection: java.lang.Exception: SAP Connection Exception: com.sap.conn.jco.JCoException: (103) RFC_ERROR_LOGON_FAILURE: Selection one of the installed languages on <host> sysnr <system number>`	Invalid Language code.
`.java.lang.UnsatisfiedLinkError: no sapjco3 in java.library.path`	Native middleware library not installed properly 3.0.1.
`Caught Exception during connection: java.lang.Exception: SAP Connection Exception: java.lang.NoClassDefFoundError: com.sap.conn.rfc.driver.CpicDriver`	
`java.lang.ExceptionInInitializerError: Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: com.sap.conn.rfc.driverCpicDriver.nativeCpicGetVerstion([I)I Verify proper installation of JCo Native support libraries packaged with JCo client`	Exception while initializing JCo client 3.0.2+.

6 Creating a New Driver Object

After the SAP User Management driver files are installed on the server where you want to run the driver (see Chapter 3, "Installing the SAP User Management Fan-Out Driver Files," on page 19), you can create the driver in the Identity Vault. You do so by installing the driver packages and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- Section 6.1, "Creating the Driver Object in Designer," on page 35
- Section 6.2, "Activating the Driver," on page 41
- Section 6.3, "Adding Packages to an Existing Driver," on page 41

6.1 Creating the Driver Object in Designer

You create the SAP User Management Fan-Out driver object by installing the driver packages and then modifying the configuration to suit your environment. After you create and configure the driver object, you need to deploy it to the Identity Vault and start it.

- Section 6.1.1, "Importing the Current Driver Packages," on page 35
- Section 6.1.2, "Installing the Driver Packages," on page 36
- Section 6.1.3, "Using Designer to Adjust the Driver Settings," on page 40
- Section 6.1.4, "Using Designer to Deploy the Driver Object," on page 40
- Section 6.1.5, "Using Designer to Start the Driver," on page 41

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

6.1.1 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. You can upgrade any package that is installed if there is a newer version of the package available. It is recommended to have the latest packages in the Package Catalog before creating a new driver object. Designer prompts you for importing the required packages when it creates the driver object. For more information on upgrading packages, see "Upgrading Installed Packages" in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

To verify you have the most recent version of the driver packages imported into the Package Catalog:

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

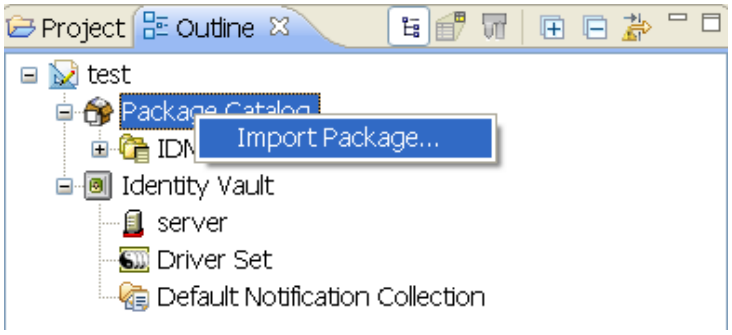
3 Click *OK* to update the packages

or

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

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

5 Click *Import Package*.



You can download the new packages from the *Designer 4.0.1 Auto-update site* (http://cdn.novell.com/cached/designer/packages/idm/updatesite1_0_0/).

6 Select any SAP User Management Fan-Out 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 6.1.2, "Installing the Driver Packages," on page 36.

6.1.2 Installing the Driver Packages

After you have imported the current driver packages into the Package Catalog, you can install the driver packages to create a new driver.

1 In Designer, open your project.

2 In the Modeler, right-click the driver set where you want to create the driver, then click *New* > *Driver*.

3 Select *SAP User Management Base*, then click *Next*.

4 Select the optional features to install for the SAP User Management Fan-Out driver. All options are selected by default. The options are:

Default Configuration: These packages contain the default configuration information for the SAP User Management Fan-Out driver. Always leave this option selected.

Fanout and Entitlement Support: These packages contain the policies and entitlements required to enable the driver for fan-out configuration. Always leave this option selected.

Password Synchronization: These packages contain the policies required to enable password synchronization. Leave this option selected if you want to synchronize passwords to the SAP system.

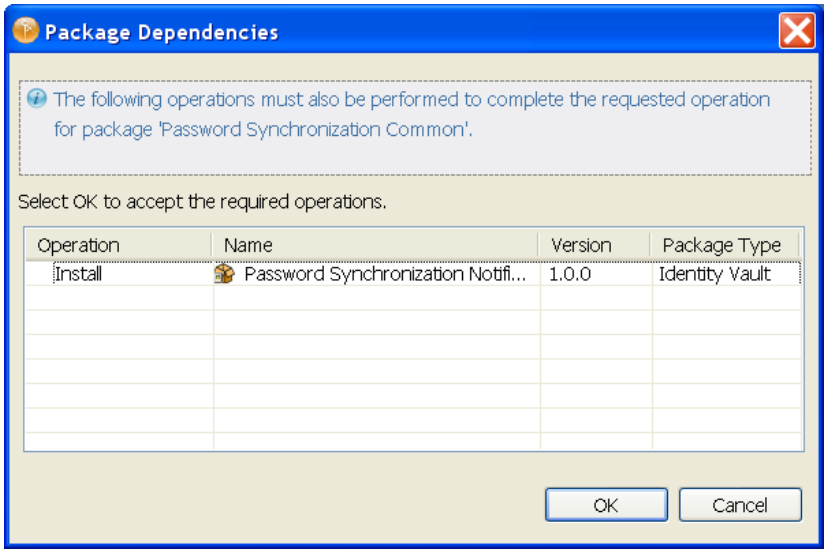
Data Collection: These packages contain the policies that enable the driver to collect data for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the *Identity Reporting Module Guide*.

Account Tracking: This group of packages contain the policies that enables account tracking information for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the *Identity Reporting Module Guide*.

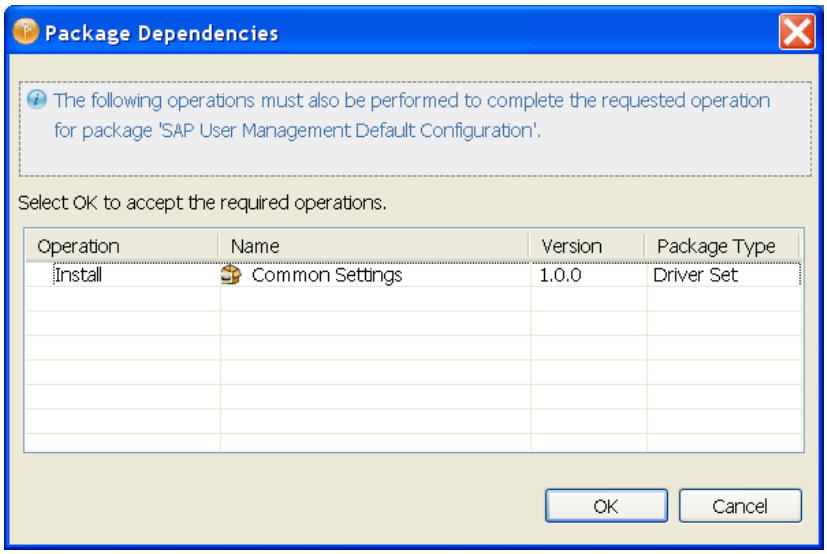
Sample Configuration: This package contains a single sample policy, which adds a user license to a user on an add event. This option is not selected by default.

5 After selecting the optional packages, click *Next*.

6 (Conditional) If there are package dependencies for the packages you selected to install, you must install these dependencies to install the selected packages. Click *OK* to install the Password Synchronization Notification package dependency.



7 (Conditional) Click *OK* to install the Common Settings package, if you have not installed any other packages into the selected driver set.



8 Click *OK* to install the Advanced Java Class package if you have not installed any other packages into the selected driver set.

9 (Conditional) Fill in the following fields on the Common Settings page:

The Common Settings page is displayed only if the Common Settings package is installed as a dependency.

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

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

Group Container: Select the Identity Vault container the groups are added if they don't already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set.

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

10 Click *Next*.

11 On the Driver Information page, specify a name for the driver, then click *Next*.

12 Fill in the following fields to configure the driver:

Authentication > SAP User ID: Specify the ID of the user the driver uses for SAP Logon. This is the *User* field in the SAP logon screen.

Authentication > SAP User Password: Specify the password the driver users for SAP Logon. This is the *Password* field in the SAP logon screen.

Authentication > SAP Application Server: Specify the hostname or IP address of the appropriate SAP Application Server. In the SAP logon properties, it is referred to as the Application Server.

Connection > System ID: Specify the SAP system ID of the SAP Application Server. The system ID is found in the SAP GUI status bar in the lower right corner of the main window.

Connection > SAP System Number: Specify the SAP system ID of the SAP Application Server. This is the System Number in the SAP logon properties. The default value is 00.

Connection > SAP User Client Number: Specify the client number on the SAP Application Server. This the *Client* field in the SAP logon screen.

Connection > Logical System Name: If this is a central client, specify the name of the logical system as it is configured in SAP. If this is not a central client, specify a unique name for the logical system.

Miscellaneous Settings > Default Reset Password: Specify a default password to be set for users when the driver resets a user's password in the SAP system. 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.

13 Click *Next*.

14 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 4.0.2 Remote Loader Guide*.

If you select *No*, skip to Step 15. 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.

15 Click *Next*.

16 (Conditional) Fill in the following fields on the Managed System Information page. This page is displayed only if you selected to install the Data Collection and Account Tracking groups of packages.

Name: Specify a descriptive name for this SAP system. The name is displayed in the reports.

Description: Specify a brief description of this SAP system. The description is displayed in the reports.

Location: Specify the physical location of this SAP system. The location is displayed in the reports.

Vendor: Select SAP as the vendor of this system. The vendor information is displayed in the reports.

Version: Specify the version of this SAP system. The version is displayed in the reports.

17 Click *Next*.

18 (Conditional) Fill in the following fields to define the ownership of this SAP system. This page is displayed only if you selected to install the Data Collection and Account Tracking groups of packages.

Business Owner: Select a user object in the Identity Vault that is the business owner of this SAP system. This can only be a user object, not a role, group, or container.

Application Owner: Select a user object in the Identity Vault that is the application owner for this SAP system. This can only be a user object, not a role, group, or container.

19 Click *Next*.

20 (Conditional) Fill in the following fields to define the classification of the SAP System. This page is only displayed if you selected to install the Dat Collection and Account Tracking groups of packages.

Classification: Select the classification of the SAP system. This information is displayed in the reports. The options are:

- Mission-Critical
- Vital
- Not-Critical
- If you select *Other*, you must specify a custom classification for the SAP system.

Environment: Select the type of environment the SAP system provides. The options are:

- Development
- Test
- Staging
- Production
- If you select *Other*, you must specify a custom classification for the SAP system.

21 Click *Next*.

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

6.1.3 Using Designer to Adjust the Driver Settings

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 55 to adjust the configuration.
3. Continue with Section 6.1.4, "Using Designer to Deploy the Driver Object," on page 40, to deploy the driver into the Identity Vault.

6.1.4 Using Designer to Deploy the Driver Object

After a driver object is created in Designer, it must be deployed into the Identity Vault, because Designer is an offline tool.

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 of DNS name of the server hosting the Identity Vault.
   - **Username:** Specify the DN of the user object used to authenticate to the Identity Vault.
   - **Password:** Specify the user's password.
4. Click *OK*.
5. Read through the deployment summary, then click *Deploy*.
6. Read the successful message, then click *OK*.
7. Click *Define Security Equivalence* to assign rights to the driver.

   The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user.

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

   7b Click *OK* twice.

   For more information about defining a Security Equivalent User in objects for drivers in the Identity Vault, see "Establishing a Security Equivalent User" in the Identity Manager 4.0.2 Security Guide.
8. Click *Exclude Administrative Roles* to exclude users that should not be synchronized.

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

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

   8b Click *OK*.

   8c Repeat Step 8a and Step 8b for each object you want to exclude.
9. Click *OK*.

6.1.5 Using Designer to Start the Driver

When a driver is created, it is stopped by default. 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 9, "Managing the Driver," on page 51.

6.2 Activating the Driver

The SAP User Management Fan-Out driver is part of the Identity Manager Integration Module for Enterprise, and this module requires a separate activation from the Identity Manager activation. After you have purchased the Integration Module for Enterprise, the new activation is available in your Novell Customer Center.

If you create the SAP User Management Fan-Out driver in a driver set where you've already activated a driver that comes with the Integration Module for Enterprise, the SAP User Management Fan-Out driver inherits the activation. If you created the SAP User Management Fan-Out 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 after 90 days.

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

- Driver for SAP HR
- Driver for SAP Portal
- Driver for SAP User Management
- Driver for SAP User Management Fan-Out
- Driver for PeopleSoft

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

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

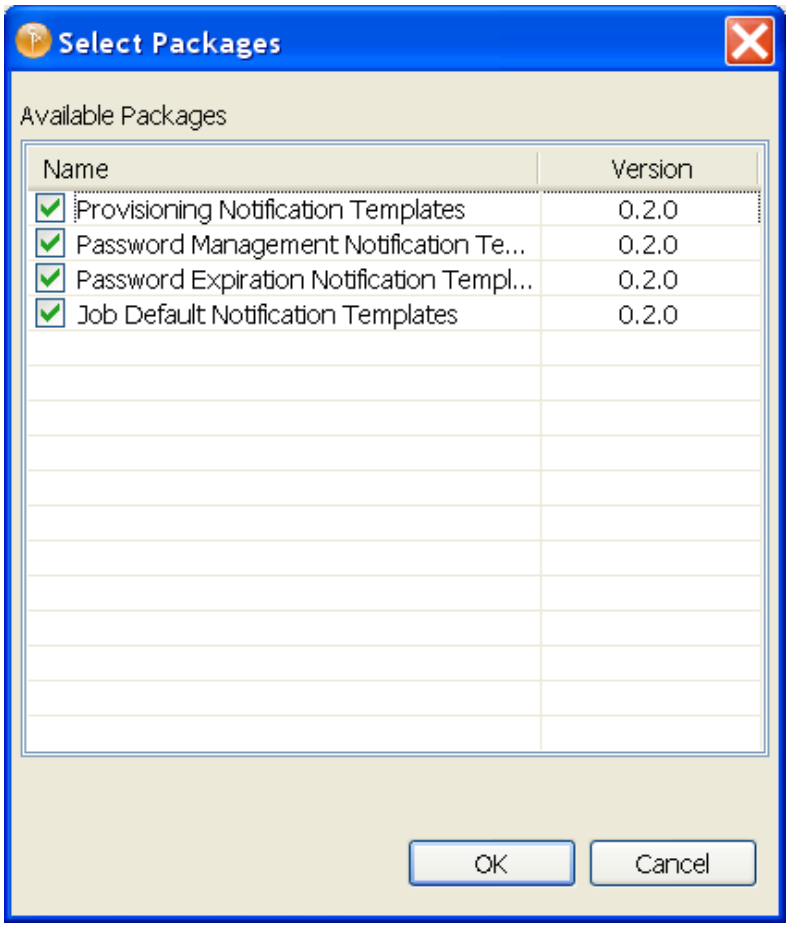
To use the driver, you must reactivate it.

For more information on activation, refer to "Activating Novell Identity Manager Products" in the *Identity Manager 4.0.2 Integrated Installation Guide*.

6.3 Adding Packages to an Existing Driver

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

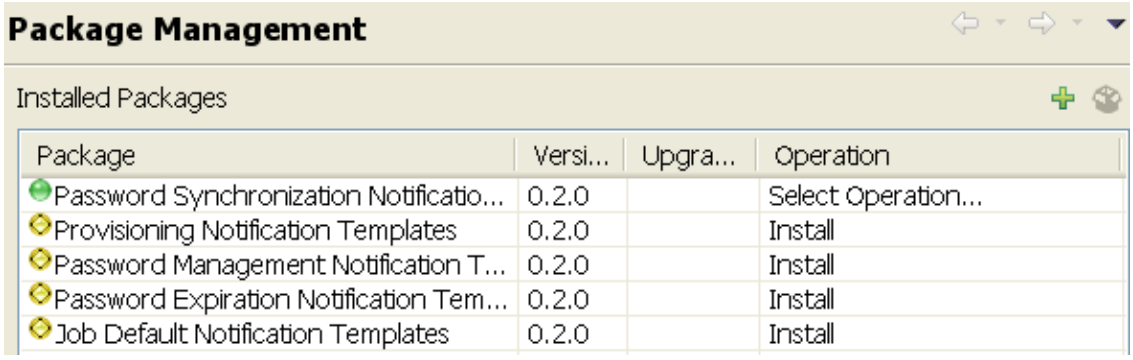
1. Right-click the driver, then click *Properties*.
2. Click *Packages*, then click the *Add Packages* icon .
3. Select the packages to install. If the list is empty, there are no available packages to install.



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

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

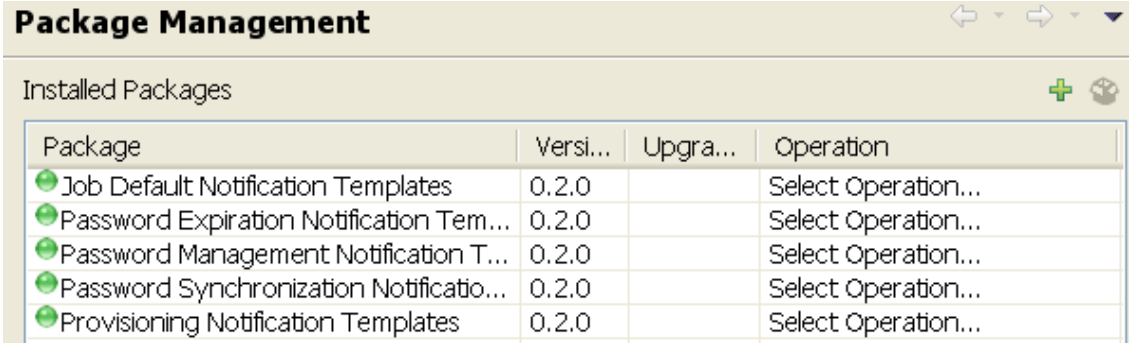
5 Click *Apply* to install all of the packages listed with the Install operation.



6 (Conditional) Fill in the fields with appropriate information to install the package you selected for the driver, then click *Next*.

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

8 Click *OK* to close the Package Management page after you have reviewed the installed packages.



9 Repeat Step 1 through Step 8 for each driver where you want to add the new packages.

7 Upgrading an Existing Driver

If you are running the driver on the Metadirectory server, the driver shim files are updated when you update the server unless they were not selected during a custom installation. If you are running the driver on another server, the driver shim files are updated when you update the Remote Loader on the server.

The 4.0.2 version of the driver shim supports drivers created by using any 3.*x* version of the driver configuration file. You can continue to use these driver configurations until you are prepared to start using packages.

The following sections provide information to help you upgrade an existing driver to version 4.0.2.

- Section 7.1, "What's New in Version 4.0.2," on page 45
- Section 7.2, "Upgrade Procedure," on page 45

7.1 What's New in Version 4.0.2

Version 4.0.2 of the driver does not include any new features.

The driver is created with packages instead of driver configuration file. For more information, see Chapter 6, "Creating a New Driver Object," on page 35.

7.2 Upgrade Procedure

The process for upgrading the SAP User Management Fan-Out driver is the same as for other Identity Manager drivers. For detailed instructions, see "Upgrading Drivers to Packages" in the *Identity Manager 4.0.2 Upgrade and Migration Guide*.

8 Implementing the Preconfigured Entitlements

Entitlements are a way to set up a list of criteria to grant or revoke user, group, and role access to resources in SAP systems. The SAP User Management Fan-Out driver comes with three preconfigured entitlements, which work with an entitlement agent. The entitlement 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 8.1, "Entitlement Agents," on page 47
- Section 8.2, "Preconfigured Entitlements," on page 48

8.1 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 User Management Fan-Out 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 to be created with policies that define the desired action. For instructions, see the "Checklist for Implementing Entitlements" in the *Identity Manager 4.0.2 Entitlements 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" in the *User Application: Administration Guide*.
- **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" in the *Identity Manager Roles Based Provisioning Module 4.0.2 User Application: Installation Guide*.

The RBPM is the only supported entitlement agent for the fan-out configuration of the driver.

8.2 Preconfigured Entitlements

- Section 8.2.1, "User Account Entitlement," on page 48
- Section 8.2.2, "Role (Activity Group) Entitlement," on page 48
- Section 8.2.3, "Profile Entitlement," on page 49

8.2.1 User Account Entitlement

Most Identity Manager drivers support the User Account entitlement as an entitlement that can only be granted once and does not take any parameters. It is like an on/off switch for the account in the application. There is a one-to-one relationship between the User Account entitlement and one account in the application. The fan-out configuration requires that a single User object in the Identity Vault be granted multiple User Account entitlements for accounts in different systems. A parameter is added to the User Account entitlement, so each time the entitlement is granted it is a unique event. The parameter indicates the system where the account 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 system.
- **Delete:** An attempt is made 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 8.1, "Entitlement Agents," on page 47.
2. Access the GCVs page for the driver.

   Designer: Right-click the driver in the Outline view or Modeler, then click *Properties* > *GCVs*.

   iManager: On the Driver Set Overview page, locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.
3. Set *User Account Entitlement* to *true*.
4. Select what to do when the user account entitlement is revoked by indicating whether you want the account disabled or deleted.
5. Click *OK* to save the changes.

The entitlement is now enabled. However, a new user account is not provisioned until the entitlement is granted through one of the entitlement agents. See Section 8.1, "Entitlement Agents," on page 47.

8.2.2 Role (Activity Group) Entitlement

The Role (activity group) entitlement adds users to the SAP roles (activity groups), and it is enabled 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 system. When the entitlement is granted with an SAP ActivityGroup as the parameter, the SAP User is added to the corresponding role.

For example, assume there is an RBPM role that contains two role 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 system.

The parameter for this entitlement differs, depending upon which entitlement agent you used. Only the RBPM agent supports the fan-out configuration.

- **RBE:** <AG name>

  For example: User Admins

  This format does not support the fan-out configuration to individual systems or to the CUA child systems.
- **RBPM:** AG=<AG name>|LSNAME=<LSNAME>

  For example: AG=User Admins|LSNAME=S7ICLNT800

  This format supports the fan-out configuration to individual systems, including the CUA child systems.

With this difference, multiple parameters are supported for multiple systems.

To manually enable this entitlement:

1. Verify that an entitlement agent that contains your list of criteria to grant or revoke role (ActivityGroup) assignments in SAP exists.

   For more information, see Section 8.1, "Entitlement Agents," on page 47.
2. Access the GCVs page for the driver.
3. Select *True* for the *Use Role (ActivityGroup) Entitlement* option.
4. 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 ActivityGroup assignments are automatically made for the user by the SAP User Management Fan-Out driver.

8.2.3 Profile Entitlement

The Profile entitlement adds users to the SAP profiles, and it is enabled by default. This entitlement contains parameters, which means it can be granted multiple times. The parameters for the entitlement differs, depending upon which entitlement agent you used. Only one agent supports the fan-out configuration.

- **RBE:** <Profile name>

  For example: SAP_NEW

  This format does not support the fan-out configuration to individual systems or to the CUA child systems.
- **RBMP:** PROF=<profile name>|LSNAME=<LSNAME>

For example: PROF=SAP_NEW|LSNAME=ADMCLNT301

This format supports the fan-out configuration to individual systems including the CUA child systems.

To manually enable this entitlement:

1. Verify that an entitlement agent that contains your list of criteria to grant or revoke profile assignments in SAP exists.

   For more information, see Section 8.1, "Entitlement Agents," on page 47.

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 on the driver.
4. Select *True* for the *User Profile Entitlement* option.
5. Click *OK* to save the changes.

The entitlement is now enabled. When a user is granted a profile entitlement through one of the entitlement agents, the SAP User Management Fan-Out driver automatically adds the user to the associated profiles.

9 Managing the Driver

As you work with the SAP User Management Fan-Out 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 4.0.2 Common Driver Administration Guide*.

For information about securing your Identity Manager system, see the *Identity Manager 4.0.2 Security Guide*.

10 Troubleshooting the Driver

- Section 10.1, "Troubleshooting the SAP User Management Fan-Out Driver," on page 53

10.1 Troubleshooting the SAP User Management Fan-Out Driver

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 4.0.2 Common Driver Administration Guide*.

10.1.1 The Account Tracking Feature Does Not Work Properly for the Existing Users

If you are using the Account Tracking feature in Fan-out configuration with Identity Manager 4.0.2 or prior, the DirXML-Accounts attribute of the existing users might contain incomplete account tracking information.

For a proper functioning of the Account Tracking feature,

1. Delete the DirXML-Accounts attribute of the existing users.
2. Apply the SAP User Management Driver 4.0.2 Patch 1.
3. Migrate the users to the SAP system to create new account tracking information.

10.1.2 Error Occurs When Uninstalling the Driver

If you have installed the SAP User Management Fan-Out 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 User Management Fan-Out driver on a server that does not have Identity Manager or the Remote Loader installed on it.

The workaround 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 Identity Manager drivers for SAP, where the JAVA-HOME-PATH is the Java or JRE installation location.

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

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

For information about uninstalling the driver, see "Uninstalling the Metadirectory Server" in the *Identity Manager 4.0.2 Framework Installation Guide*.

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the SAP User Management 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 4.0.2 Common Driver Administration Guide* for information about the common properties.

iManager is aware of packages, but does not support packages. If you change the content of the driver delivered with packages in iManager, the Package Manager features like Factory Mode or Revert Customizing no longer work. Always make driver content changes in Designer and use iManager for administrative purposes.

The information is presented from the viewpoint of Designer.

- Section A.1, "Driver Configuration," on page 55
- Section A.2, "Global Configuration Values," on page 63

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 User Management Fan-Out 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 56
- Section A.1.2, "Authentication," on page 56
- Section A.1.3, "Startup Option," on page 57

- Section A.1.4, “Driver Parameters,” on page 58
- Section A.1.5, “ECMAScript,” on page 62
- Section A.1.6, “Global Configurations,” on page 63

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.sapumshim.SAPDriverShim`
Native	This option is not used with the SAP User Management driver.
Connect to Remote Loader	Used when the driver is connecting remotely to the connected system. Designer includes two suboptions: - *Remote Loader Client Configuration for Documentation*: Includes information on the Remote Loader client configuration when Designer generates documentation for the SAP User Management Fan-Out driver. - *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.

A.1.2 Authentication

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

Table A-2 *Authentication Options*

Option	Description
Authentication ID	Specify an SAP account that the driver can use to authenticate to the SAP system. Example: `SAPUser`
Authentication Context or *Connection Information*	Specify the IP address or name of the SAP server the driver should communicate with.
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 hostname is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090. The `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine. Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`
Driver Cache Limit (kilobytes) or *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 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.1.3 Startup Option

The startup option allows you to set the driver state when the Identity Manager server is started.

Table A-3 *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 applies only 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.1.4 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment.

The parameters are presented by category:

- Table A-4, "Driver Settings," on page 59
- Table A-5, "Subscriber Settings," on page 61
- Table A-6, "Publisher Settings," on page 62

Table A-4 *Driver Settings*

Parameter	Description

System ID	Specify the SAP system ID of the SAP application server. The system ID is found in the SAP GUI status bar located in the lower right corner of the main window.
	
	This parameter is used to generate the realm for Account Tracking. The system ID is usually a three-character string that uniquely identifies a SAP system in the SAP system landscape. The realm must be unique per application type.
	
	For example:
	
	`\<system ID>\<system number>\<client number>`
	`\S71\00\800`

SAP System Number	Specify the SAP system number of the SAP application server. This is referred to as the *System Number* in the SAP logon properties. The default value is 00.
SAP User Client Number	Specify the client number to be used on the SAP application server. This is referred to as the *Client* in the SAP logon screen.
SAP Client Type	Select the client type the driver is connecting to: ◆ **Non-CUA Client:** If the client you are connecting to is not a CUA central client and is it not CUA child client, select this option. ◆ **CUA Central:** If you are connecting to the CUA central client, select this option. ◆ **CUA Child:** If you are connecting to a CUA child client, select this option. The fan-out policies must know what type of client they are communicating to so they can generate the correct events. For example, most of the attributes in a CUA child client are synchronized through the CUA central client.
SAP Client Type > CUA Child > Logical System Name of CUA Central Client	This option is displayed only if you select *CUA Child*. Specify the logical system name of the CUA central client that manages this client. The fan-out policies must know which client is the central client of a CUA child client, so that they can generate correct events. For example, most of the attributes in a CUA child client are synchronized through the CUA central client.

Parameter	Description
SAP Client Type > CUA Child > Filter	This option is displayed only if you select *CUA Child*. Add an attribute name in the Identity Vault namespace that you want to synchronize directly to the CUA child client, instead of sending it to the CUA central client. This filter is evaluated after the driver's Subscriber filter is applied. For an attribute to encounter this filter, it must also be set to Subscribe or Notify in the regular driver filter. This filter is implemented in the Event Transformation policy set. For most deployments, you should leave the two default attributes of Login Disabled and nspmDistributionPassword in the filter. The fan-out policies must know which attributes to send directly to a CUA child client.
Logical System Name	Specify the Logic System Name for the client as it appears in the SAP system, if the SAP client is the central client in a CUA landscape. Otherwise, specify a unique name for this system. The driver uses the logical system names from both the primary connection and all of the secondary connections to uniquely identify a connection. The driver looks up the connection information based on this value.
SAP User Language	Specify the language code this driver will use for the SAP session. This is referred to as the *Language* in the SAP logon screen.
Available Languages	Specify all of the languages installed on your SAP system. All of the languages you specify in the list are made available to the Role Mapping Administrator, so that Role Mapping Administrator can render the UI accordingly.
Character Set Encoding	The code for the character set to translate IDoc byte-string data into Unicode strings. An empty value causes the driver to use the host JVM default.
Publish all Communication Table Values	Set this to *Publish Primary* if only the primary value of Communicate tables should be synchronized. or Set this to *Publish All* if all values should be synchronized.
Publish Company Address Data	Select whether the driver populates the User Company Address data for the Publisher channel and for the Subscriber queues.
Change retry status to error on Subscriber events	Select *Yes* to have the driver shim issue an error instead of a retry on Subscriber operation results. Use this setting when running the driver in fan-out mode. If you are not using the fan-out mode, select *No* to disable this feature. If you are using the standard mode, select *Yes* to enable this.

Table A-5 *Subscriber Settings*

Parameter	Description
Communication Table Comments	The communication table comment is a text comment the driver adds to all Communication table entries added by the Subscriber channel. This is a useful method for determining where an entry originated from when viewing values via the SAP GUI. Leaving this field blank provides no comment for the table entries.
Require User to Change Set Passwords	This parameter specifies the methodology used by the driver to set User account passwords. Passwords can be set by the driver's administrative User account or by the affected User's account (this sets a password on new accounts or modifies passwords for existing Users.) Select *Change Required* if passwords must be changed immediately at the user's next login. or Select *No Change Required* if you do not want users to change passwords immediately at login.
Password Set Method (Conditional)	If you select the *No Change Required* option above, you should specify a Password Set Method: *Administrator Set* or *User Set.* **Administrator Set:** Passwords are set by the driver's administrative User account. This method is deprecated and does not comply with SAP security best practices. The method works only for SAP systems that are version 4.6c or older. **User Set:** Passwords are supplied by the affected users. The following parameters must be set if you select User Set: ◆ **Default Reset Password:** This parameter specifies a default password reset value. It is set during password changes if the user-supplied password is not accepted by the SAP server. There is an 8-character size limit for this value. (SAP 7.0 does not require an 8-character size limit on passwords.) ◆ **Reset Password Delay (seconds):** Specify the number of seconds between the setting of the administrative default password and the setting of the user's new password. ◆ **Force Passwords to Uppercase:** This option defines if passwords are forced to uppercase. Uppercase is the default value; however, SAP 7.0 allows for mixed-case passwords.
Support Password Set for Non-Dialog Users	Select whether to allow the driver to set password for non-dialog user types, such as Communications, System, Service, and Reference on the Subscriber channel.
Use local locking	Select *Yes* to lock accounts locally in the client. Local locking requires additional configuration in the SAP system. Select *No* to lock accounts globally, which locks all accounts in the CUA child clients if the account in the CUA central client is locked. For more information, see Appendix G, "Setting and Clearing Granular Locks," on page 87.
SAP Server Secondary Connection Information	If you are configuring the driver for fan-out, click the plus icon, then add the information for the additional SAP system. The information requested is listed in Table A-4, "Driver Settings," on page 59. Repeat this process for each system you want to fan out to from this driver.

Table A-6 Publisher Settings

Parameter	Description
Publisher Channel Enabled	Select whether or not you want to enable the driver's Publisher channel.
Publisher Channel Port Type	Select *TRFC* if the driver instantiates a JCo 3 Server to receive data distribution broadcasts from the SAP ALE system. Select *FILE* if the driver consumes text file IDocs distributed by the SAP ALE system.
SAP Gateway ID	Specify the SAP Gateway ID that distributes user data to the driver.
TRFC Program ID	Specify the registered program ID that is used by the driver. This value is specified in the SAP port definition.
Generate TRFC Trace Files	Select whether the JCo 3 server TRFC tracing is enabled.
Logical System for User Distribution	Specify the logical system name configured in the SAP system for user distribution to the Identity Manager driver. Publication only works if the Publisher channel is enabled and the driver's primary connection is to a CUA central client.
Poll Interval (seconds)	Specify how often the Publisher channel polls for unprocessed IDocs. The default value is 10 seconds.
Future-dated Event Handling Option	The behavior of this option is based on the values of the User record's Logon Data "Valid From" date (LOGONDATA:GLTGV) when IDocs are processed by the Publisher channel. This field does not need to be in the Publisher filter for this processing to occur. Choose one of the following options: ◆ **Publish Immediately:** Indicates that all attributes are processed by the driver when the IDoc is available. No future-dated processing is performed. ◆ **Publish on Future Date:** Indicates that only attributes that have a current or past time stamp are processed by the driver when the IDoc is available. Future-dated infotype attributes are cached in a `.futr` file to be processed at a future date. ◆ **Publish Immediately and on Future Date:** Indicates that the driver blends the first two options. All attributes with a current or past time stamp are processed at the time the IDoc is available. All future-dated infotype attributes are cached in a `.futr` file to be processed at a future date. ◆ **Publish Immediately and Daily through Future Date:** Indicates that the driver processes all events at the time the IDoc is made available. All future-dated infotype attributes are cached in a `.futr` file to be processed again on the next calendar day. This continues until the attributes are sent for a final time on the future date.
Publisher IDoc Directory	Specify the file system location where the SAP User IDoc files are placed by the SAP ALE system (file port configuration) or by the driver (TRFC configuration.) This setting is only used if the Publisher channel is enabled.
Publisher Heartbeat Interval	Specify how many minutes of inactivity can elapse before this channel sends a heartbeat document. In practice, more than the number of minutes specified can elapse. That is, this parameter defines a lower bound.

A.1.5 ECMAScript

Displays an ordered list of ECMAScript resource files. The files contain extension functions for the driver that Identity Manager loads when the driver starts. You can add additional files, remove existing files, or change the order the files are executed.

A.1.6 Global Configurations

Displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads when the driver is started. You can add or remove the Global Configuration objects, and you can change the order in which the objects are executed.

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The SAP User Management Fan-Out 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 divided into categories:

- Section A.2.1, "Entitlements," on page 64
- Section A.2.2, "Password Synchronization," on page 66
- Section A.2.3, "Account Tracking," on page 66
- Section A.2.4, "Managed System Information," on page 67
- Section A.2.5, "SAP User Management Driver," on page 68

A.2.1 Entitlements

There are multiple sections in the *Entitlements* tab. Depending on which packages you installed, different options are enabled and displayed. This section documents all of the options.

- "Entitlements Options" on page 64
- "Data Collection" on page 64
- "Role Mapping" on page 65
- "Resource Mapping" on page 65
- "Parameter Format" on page 65
- "Entitlement Extensions" on page 65

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 4.0.2 Entitlements Guide* and Section 8.1, "Entitlement Agents," on page 47.

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.

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

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

Advanced settings: Select *show* to display all of the advanced settings. The advanced settings enable additional functionality in the driver such as data collection or enabling the driver to work with the Role Mapping Administrator. If you changes these settings from the default, you risk disabling the additional functionality.

Data Collection

Data collection enables the Identity Report Module to gather information to generate reports. For more information, see the *Identity Reporting Module Guide*.

Enable data collection: Select *Yes* to enable data collection for the driver through the Data Collection Service by the Managed System Gateway driver. If you are not going to run reports on data collected by this driver, select *No*.

Allow data collection from user accounts: Select *Yes* to allow data collection by the Data Collection Service through the Managed System Gateway driver for the user accounts.

Allow data collection from roles (ActivityGroups): Select *Yes* to allow data collection by the Data Collection Service through the Managed System Gateway driver for groups.

Allow data collection from profiles: Select *Yes* to allow data collection by the Data Collection Service through the Managed System Gateway driver for profiles.

Role Mapping

The Role Mapping Administrator allows you to map business roles with IT roles. For more information, see the *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide*.

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

Allow mapping of user accounts: Select *Yes* if you want to allow mapping of user accounts in the Role Mapping Administrator. An account is required before a role, profile, or license can be granted through the Role Mapping Administrator.

Allow mapping of roles (ActivityGroups): Select *Yes* if you want allow mapping of roles (ActivityGroups) in the Role Mapping Administrator.

Allow mapping of profiles: Select *Yes* if you want to allow mapping of profiles in the Role Mapping Administrator.

Resource Mapping

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

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

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

Allow mapping of roles (ActivityGroups): Select *Yes* if you want to allow mapping of roles (ActivityGroups) in the Roles Based Provisioning Module.

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

Parameter Format

Format for User Account entitlement: Select the parameter format the entitlement agent must use when granting this entitlement. The options are *Identity Manager 4* or *Legacy*.

Format for Role (ActivityGroup) entitlement: Select the parameter format the entitlement agent must use when granting this entitlement. The options are *Identity Manager 4* or *Legacy*.

Format for Profile entitlement: Specify the parameter format the entitlement agent must use when granting this entitlement. The options are *Identity Manager 4* or *Legacy*.

Entitlement Extensions

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

Role (ActivityGroup) extension: The content of this field is added below the entitlement element in the EntitlementConfiguration resource object.

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

A.2.2 Password Synchronization

These GCVs enable password synchronization between the Identity Vault and the SAP system.

In Designer, you must click the icon next to a GCV to edit it. This displays the Password Synchronization Options dialog box for a better view of the relationship between the different GCVs.

In iManager, you should edit the Password Management Options on the *Server Variables* tab rather than under the GCVs. The Server Variables page 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 4.0.2 Password Management Guide*.

Connected System or Driver Name: Specify the name of the SAP system or the driver name. This valued is used by the e-mail notification template to identity the source of the notification message.

Application accepts passwords from Identity Manager: If *True*, allows passwords to flow from the Identity Manager data store to the connected system.

Identity Manager accepts passswords from application: If *True*, allows passwords to flow from the connected system to Identity Manager.

Publish passwords to NDS password: Use the password from the connected system to set the non-reversible NDS password in eDirectory.

Publish passwords to Distribution Password: Use the password from the connected system to set the NMAS Distribution Password used for Identity Manager password synchronization.

Require password policy validation before publishing passwords: If True, applies NMAS password policies during publish password operations. The password is not written to the data store if it does not comply.

Reset user's external system password to the Identity Manager password on failure: If True, on a publish Distribution Password failure, attempt to reset the password in the connected system by using the Distribution Password from the Identity Manager data store.

Notify the user of password synchronization failure via e-mail: If True, notify the user by e-mail of any password synchronization failures.

A.2.3 Account Tracking

Account tracking is part of the Identity Reporting Module. For more information, see the *Identity Reporting Module Guide*.

Enable Account Tracking: Set this to *True* to enable account tracking policies. Set it to *False* if you do not want to execute account tracking policies.

Mode Of Operation: Select whether this driver runs in standard (one-to-one) or in fan-out (many-to-one) mode.

Realm Lookup-Key Source: Select the source of the key you want to use to look up the realm. The only option available is *Association*.

Realm Key Extractor: Specify a regular expression that extracts the key from the realm lookup key source.

Show Subscriber Operation Mapping Configuration: Select *show* to display the Subscriber operation mapping configuration for fan-out.

Replication Wait Time (in seconds): Specify the number of seconds the driver waits before expecting the application to have completed replication. By default, the value is 10 seconds.

Subscriber Operation Mappings > Operation: Select the operation triggered by this mapping. The options are *Add Account*, *Delete Account*, *Enable Account*, and *Disable Account*.

Subscriber Operation Mappings > Trigger: Specify an XPath 1.0 expression that identifies the operation you are mapping to.

Subscriber Operation Mappings > Realm Lookup-Key Source: Specify an XPath 1.0 expression that extracts the source of the key you want to use to look up the item.

Subscriber Operation Mappings > Realm Key Extractor: Specify a regular expression that extracts the key from the realm lookup key source.

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

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

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

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

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

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

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

A.2.4 Managed System Information

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

- "General Information" on page 67
- "System Owner" on page 68
- "System Classification" on page 68
- "Fan-out Configuration" on page 68
- "Connection and Miscellaneous Information" on page 68

General Information

Name: Specify a descriptive name for this SAP system. This name is displayed in the reports.

Description: Specify a brief description of this SAP system. This description is displayed in the reports.

Location: Specify the physical location of this SAP system. This location is displayed in the reports.

Vendor: Select SAP as the vendor of the SAP system. This information is displayed in the reports.

Version: Specify the version of this SAP system. This version information is displayed in the reports.

System Owner

Business Owner: Browse to and select the business owner in the Identity Vault for this SAP system. You must select a user object, not a role, group, or container.

Application Owner: Browse to and select the application owner in the Identity Vault for this SAP system. You must select a user object, not a role, group, or container.

System Classification

Classification: Select the classification of the SAP system. This information is displayed in the reports. The options are:

- Mission-Critical
- Vital
- Not-Critical
- If you select *Other*, you must specify a custom classification for the SAP system.

Environment: Select the type of environment the SAP system provides. The options are:

- Development
- Test
- Staging
- Production
- If you select *Other*, you must specify a custom classification for the SAP system.

Fan-out Configuration

Logical Instances: Click the plus icon to add logical instances of each additional SAP system.

Connection and Miscellaneous Information

Connection and miscellaneous information: This options is always set to *hide*, so that you don't make changes to these options. These options are system options for reporting to work. If you make any changes, reporting stops working.

A.2.5 SAP User Management Driver

Logical System for User Distribution: Specify the logical system name configured in the SAP system for user data distribution to the Identity Manager driver. Publication only works if the Publisher channel is enabled and the driver's primary connection is to a CUA central client.

B Application Link Enabling (ALE)

Application Link Enabling (ALE) technology enables communication between SAP and external systems such as the Identity Vault (eDirectory). ALE is comprised of various components. If you want to distribute User modification data automatically from the SAP system to the Identity Vault, you must configure the ALE and CUA systems. If your integration requires only reading and writing data to the SAP system, this configuration is not necessary.

When you configure the SAP system to enable the driver, you should consider the following ALE components and their relationship to the driver:

- Section B.1, "Clients and Logical Systems," on page 69
- Section B.2, "Message Type," on page 70
- Section B.3, "IDoc Type," on page 70
- Section B.4, "Distribution Model," on page 70
- Section B.5, "Partner Profiles," on page 70
- Section B.6, "Port," on page 70
- Section B.7, "Port Definition," on page 70
- Section B.8, "File Port," on page 71
- Section B.9, "TRFC Port," on page 71
- Section B.10, "CUA," on page 71

Refer to Chapter 4, "Configuring the SAP System," on page 21 for instructions on how to configure these SAP system parameters.

B.1 Clients and Logical Systems

In the SAP configuration for the driver, a logical system is a representation of either a SAP system or an external system. The logical system is used to distribute data to and from SAP. To use ALE, every SAP system needs to have a base logical system associated with a client. There is a one-to-one relationship between the client and the logical system.

The driver uses an outbound ALE interface. In an outbound ALE interface, the base logical system becomes the *sender* for outbound messages and the *receiver* of inbound messages. A SAP user is probably logged into the base logical system/client when making changes to the database (for example, modifying User profiles or logon preferences). A logical system/client must also be defined for the receiving client. This logical system acts as the receiver of outbound messages.

B.2 Message Type

A message type represents the type of data that is exchanged between the two systems. For this driver, the USERCLONE message type is used. A message type characterizes data being sent across the systems and relates to the structure of the data, also known as an IDoc type (for example, USERCLONE03).

B.3 IDoc Type

Intermediate Document (IDoc) Type represents the structure of the data associated with a message type. ALE technology uses IDocs to exchange data between logical systems. An IDoc is an object with the data of a specific message type in it. IDocs consist of three record types:

- The control record
- The data record
- The status record

The control record contains information about the IDoc, such as what IDoc type it is, the message type, the sending and receiving systems, or the direction.

The data record contains the application data. Data records consist of several fields that describe the content of the specific object.

The status record contains data on the state of the processing of the IDoc.

B.4 Distribution Model

The distribution model is a tool that stores information about the flow of message types between systems. A distribution model must be configured when setting up the driver. After the two logical systems have been defined and you have a general understanding of message types and IDocs, you can configure your distribution model.

The distribution model determines what message types can be sent from a logical system to another logical system.

B.5 Partner Profiles

Partner profiles specify the components used in an outbound process. Some of these components include the IDoc type, message type, IDoc size, mode, and the person to be notified in case of errors.

B.6 Port

A port is the communication link between the two logical systems.

B.7 Port Definition

A port definition is used in an outbound process to define how documents are transferred to the destination system.

B.8 File Port

A file port can be used in the integration solution. IDocs are transferred to a file in a specified file system location accessible by the SAP host system.

B.9 TRFC Port

A Transactional Remote Function Call (TRFC) can be used in the integration solution. IDocs are transferred to a specified application process (such as the driver) via the SAP Gateway.

B.10 CUA

Central User Administration (CUA) is a process provided by SAP to distribute and manage User object data between a Central SAP logical system and one or more Client logical systems. The client logical systems might be SAP or external systems. The base technology used for the CUA is ALE.

C Business Application Programming Interfaces (BAPIs)

A BAPI is an Business Application Programming Interface (BAPI). SAP has business APIs for the SAP business object types.

Table C-1 contains a list of the BAPIs used by the driver.

Table C-1 *Driver BAPIs*

BAPI Name	Description
BAPI_PDOTYPES_GET_DETAILEDLIST	Used to obtain lists and minimal detailed information for SAP USER objects and other specified business object types.
BAPI_USER_ACTGROUPS_ASSIGN	Used to assign the Activity Groups (Roles) to SAP USER objects in a non-CUA landscape.
BAPI_USER_ACTGROUPS_DELETE	Used to delete the Activity Groups (Roles) from SAP USER objects in a non-CUA landscape.
BAPI_USER_PROFILES_ASSIGN	Used to assign Profiles to SAP USER objects in a non-CUA landscape.
BAPI_USER_PROFILES_DELETE	Used to delete Profiles from SAP USER objects in a non-CUA landscape.
BAPI_USER_CHANGE	Used to modify SAP USER object attributes (fields, structures, and general tables) and non-persistent passwords.
BAPI_USER_CREATE1	Used to create a new SAP USER object.
BAPI_USER_DELETE	Used to delete an SAP USER object.
BAPI_USER_GETDETAIL	Used to read the current data field values, structures, and general table attributes of an SAP USER object.
BAPI_ADDRESSORG_GETDETAIL	Used to read the Company Address attributes of an SAP USER object.
BAPI_USER_LOCK	Used to lock an SAP USER object account. On a CUA Central system this is a global lock. On a CUA child system or on a non-CUA system, this is a local lock.
BAPI_USER_UNLOCK	Used to unlock an SAP USER object account. On a CUA Central system this is a global lock. On a CUA child system or on a non-CUA system this is a local lock.

BAPI Name	Description
BAPI_USER_SYSTEM_ASSIGN	Used to assign the user to the specified logical system in a CUA landscape.
SUSR_BAPI_USER_LOCK	Used to set granular locks on an SAP USER object account. The granular lock types available are `LOCK_LOCAL` and `LOCK_GLOBAL`. By default, this BAPI is not a remote-enabled module and is thus not accessible to the driver. An ABAP developer must modify the Processing Type attribute of the BAPI on the target SAP system. This is accomplished via the SAP Function Builder (Transaction SE37).
SUSR_BAPI_USER_UNLOCK	Used to clear granular locks on an SAP USER object account. The granular lock types available are `LOCK_LOCAL`, `LOCK_GLOBAL`, and `LOCK_WRONG_LOGON`. By default, this BAPI is not a remote-enabled module and is thus not accessible to the driver. An ABAP developer must modify the Processing Type attribute of the BAPI on the target SAP system. This is accomplished via the SAP Function Builder (Transaction SE37).
SUSR_USER_CHANGE_PASSWORD_RFC	Used to set a persistent password for an SAP USER object.
BAPI_USER_LOCACTGROUPS_ASSIGN	Used to assign client-specific Activity Groups (Roles) to SAP USER objects in a CUA landscape.
BAPI_USER_LOCACTGROUPS_READ	Used to read the current client-specific Activity Groups (Roles) assignments of SAP USER objects in a CUA landscape.
BAPI_USER_LOCACTGROUPS_DELETE	Used to delete the client-specific Activity Groups (Roles) assignments from SAP USER objects in a CUA landscape.
BAPI_USER_LOCPROFILES_ASSIGN	Used to assign client-specific Profiles to SAP USER objects in a CUA landscape.
BAPI_USER_LOCPROFILES_READ	Used to read the current client-specific Profile assignments of SAP USER objects in a CUA landscape.
BAPI_USER_LOCPROFILES_DELETE	Used to delete the client-specific Profile assignments from SAP USER objects in a CUA landscape.
BAPI_USER_CLONE	Sent from the SAP ALE subsystem to communicate SAP-initiated changes of USER objects to the driver Publisher channel.
BAPI_COMPANY_CLONE	Sent from the SAP ALE subsystem to communicate SAP-initiated changes of company address information to the driver Publisher channel.

D Configuration and Deployment Notes

The following information can be valuable when modifying the driver configuration or when trying to understand SAP system behavior. Many of these notes relate to data value restrictions on the User record. You should investigate the system configuration thoroughly, because some values might have been modified or extended by the SAP administrator.

- Section D.1, "SAP Object Types," on page 75
- Section D.2, "User Types: LOGONDATA:USTYP," on page 75
- Section D.3, "Output Controller Options," on page 76
- Section D.4, "Communication Types: ADDCOMREM:COMM TYPE," on page 76
- Section D.5, "Date Formats: DEFAULTS:DATAFM," on page 76
- Section D.6, "Decimal Formats: DEFAULTS:DCPFM," on page 76
- Section D.7, "Computer Aided Test (CATT): DEFAULTS:CATTKENNZ," on page 77
- Section D.8, "Communication Comment Type to Table Mappings," on page 77
- Section D.9, "Language Codes," on page 77
- Section D.10, "Configuration Parameters," on page 78
- Section D.11, "Design Comments and Notes," on page 78

D.1 SAP Object Types

The following SAP object types of interest might be referenced in <query> operations to SAP.

User Profile	Pseudo-object type: PROFILE
USER	Object Type: US
Activity Groups	Object Type: AG
Standard Roles	Object Type: AC
Company	Object Type: U
User Groups	Object Type: UG

D.2 User Types: LOGONDATA:USTYP

- A - Dialog
- C - Communication (CPIC)

- B - System (BDC)
- S - Service
- L - Reference

D.3 Output Controller Options

Output Controller Options	
G - Output immediately	DEFAULTS: SPDB
H - Don't output immediately	DEFAULTS: SPDB
D - Delete after output	DEFAULTS: SPDA
K - Don't delete after output	DEFAULTS: SPDA

D.4 Communication Types: ADDCOMREM:COMM TYPE

- INT - EMail Address type (SMTP)
- LET - Letter (Standard Post)
- PAG - Pager
- FAX - Facsimile
- PRT - Printer
- RML - Remote Mail
- TEL - Telephone
- TLX - Telex
- TTX - Teletex
- SSF - Secure Store and Forward

D.5 Date Formats: DEFAULTS:DATAFM

1. DD.MM.YYYY
2. MM/DD/YYYY
3. MM-DD-YYYY
4. YYYY.MM.DD
5. YYYY/MM/DD
6. YYYY-MM-DD

D.6 Decimal Formats: DEFAULTS:DCPFM

- "X" - The decimal divider is a dot, and the thousands divider is a comma (NN,NNN.NN)
- "Y" - The decimal divider is a comma, and the thousands divider is a blank (NNN NNN,NN)
- " " - The decimal divider is a comma, and the thousands divider is a dot (NN.NNN,NN)

D.7 Computer Aided Test (CATT): DEFAULTS:CATTKENNZ

- "X" - CATT: Test status set
- " " - CATT: Test status not set
- "." - CATT: CATT status set

D.8 Communication Comment Type to Table Mappings

Table: ADDTEL	Comment Type: TEL	Key Field: TELEPHONE
Table: ADDFAX	Comment Type: FAX	Key Field: FAX
Table: ADDPAG	Comment Type: PAG	Key Field: PAGER
Table: ADDSMTP	Comment Type: INT	Key Field: E_MAIL
Table: ADDTTX	Comment Type: TTX	Key Field: TELETEX
Table: ADDPRT	Comment Type: PRT	Key Field: PRINT_DEST
Table: ADDTLX	Comment Type: TLX	Key Field: TELEX_NO
Table: ADDRML	Comment Type: RML	Key Field: R_MAIL
Table: ADDURI	Comment Type: URI	Key Field: URI

D.9 Language Codes

Language	**Two-Letter Code**	**One-Letter Code**
Language	Two-Letter Code	One-Letter Code
Afrikaans	AF	a
Arabic	AR	A
Bulgarian	BG	W
Czech	CS	C
Danish	DA	K
German	DE	D
Greek	EL	G
English	EN	E
Spanish	ES	S
Estonian	ET	9
Finnish	FI	U
French	FR	F
Hebrew	HE	B

Language	Two-Letter Code	One-Letter Code
Croatian	HR	6
Hungarian	HU	H
Indonesian	ID	i
Italian	IT	I
Japanese	JA	J
Korean	KO	3
Lithuanian	LT	X
Latvian	LV	Y
Malaysian	MS	7
Dutch	NL	N
Norwegian	NO	O
Polish	PL	L
Portuguese	PT	P
Romanian	RO	4
Russian	RU	R
Slovak	SK	Q
Slovene	SL	5
Serbian	SR	0 (zero)
Swedish	SV	V
Thai	TH	2
Turkish	TR	T
Ukrainian	UK	8
Customer Reserve	Z1	Z
Chinese Traditional	ZF	M
Chinese	ZH	1

D.10 Configuration Parameters

Comment text for configuration parameters is limited to a maximum length of 50 bytes.

D.11 Design Comments and Notes

When specifying either USER or COMPANY names in BAPI calls, the name field must be in all-caps format, even if the naming field is not specified as such.

NOTE: The ADMIN_SET mode is deprecated prior to R/3 4.7. You need to use USER_SET mode with SAP 4.7 and above.

In BAPI_USER_CHANGE (ADDRESS table)

- The COMM-TYPE attribute in SAP has defined, acceptable values. Invalid input generates an exception and an error message stating, `The communication type <commType> is not defined`. Valid fields are the abbreviations for the supported communication types on the SAP Host.
- The TITLE_ACA1 and TITLE_ACA2 attributes have predefined, acceptable values. Invalid input results in the value in SAP being set to a null string (“ ”).
- The PREFIX1 and PREFIX2 attributes have predefined, acceptable values. Invalid input results in the value in SAP being set to a null string (“ ”).
- The TEL1_NUMBR is linked to the primary, or Standard, Telephone number in the Telephone communication table.

In BAPI_USER_CHANGE (ADDFAX table)

- The Facsimile Telephone Number attribute in the Identity Vault is a structured attribute. An output transformation converts it to a single-attribute format.

In BAPI_USER_CHANGE (ADDTEL table)

- Must have a CONSNUMBER (either the number of the one you want to change or a new, non-000 number.)
- The STD_NO field must be set to X if you are synchronizing a single field or if the number is the only number present.
- The primary data field is TELEPHONE.

In BAPI_USER_CHANGE (ADDTLX table)

- By default, this table is mapped to the Organizational Person; telexNumber attribute. This syntax is OCTET_STRING, which is encoded by Identity Manager into Base64 string encoding. A Java function is provided in the driver `sapusershim.jar` file that can decode this into the proper string format in the Output Transformation prior to submission to SAP. If you are using the driver on a remote system, place the driver shim in the same file system container with the Identity Manager library in the Input Transformation for the Publisher channel.
- The primary data field is TELEX_NO.
- Other rules apply as described for the ADDTEL table.

In BAPI_USER_CHANGE (ADDFAX table)

- The primary data field is FAX.
- Other rules apply as described for the ADDTEL table.

In BAPI_USER_CHANGE (GROUPS table)

- The USERGROUP is the only field in this table.

In BAPI_USER_CHANGE (ALIAS structure)

- The USERALIAS is the only field in this table.
- The SAP system guarantees that alias names are unique among all users. If an alias value is already assigned to another user, the modification fails.

In BAPI_USER_CHANGE (REF_USER structure)

- The REF_USER is the only field in this table.
- The value specified as REF_USER must be an existing User object on the SAP client, and the Reference User's type flag must be set to Reference (User Type L)

In BAPI_USER_CHANGE (DEFAULTS structure)

- The SPDB field can only be populated with a G (GO or Output Immediately), or an H (Hold output), or a null string " ", which sets the value to H. All other values generate an error message. This field is case sensitive.
- The SPDA field can only be populated with a D (Delete after print), a K (Keep), or a null string " ", which sets the value to K. All other values generate an error message. This field is case sensitive.
- The KOSTL (Cost center) field is automatically truncated to 8 bytes by the SAP system.
- The SPLG field does not appear to be utilized. Any value is accepted but does not relate to any attribute shown in the SAP GUI.
- The START_MENU field can be set to any value up to 30 characters whether or not a valid menu exists for the value being set.
- The SPLD (Output Controller) field accepts only a null string value (" ") or a valid output device that is available via the SAP GUI drop-down list for this field. Invalid selections return an error.
- The LANGU field must be set to one of the one-letter language codes defined in Section D.9, "Language Codes," on page 77 or to a null string (" "). The null string defaults to the language of the SAP system default language. This field is case sensitive. Non-defined fields result in an error.

In BAPI_USER_CHANGE (LOGONDATA structure)

- The USTYP field only accepts the valid User Types defined in Section D.2, "User Types: LOGONDATA:USTYP," on page 75 or a null string (" "). Other input generates an exception and an error message stating `Invalid user type<type>`.
- The TZONE field accepts only valid, selectable fields from the SAP GUI drop-down list. Invalid input generates an exception and an error message stating `Invalid time zone`. The Time Zone setting is displayed under the *Defaults* tab in the SAP client Display User dialog box.
- The CLASS field represents the User's User Group for the Authorization Check setting. Only fields that are selectable from the SAP GUI drop-down list are accepted. Invalid input generates an exception and error message stating `User group <class> does not exist`.
- The GLTGV (Validity Begin Date) and GLTGB (Validity End Date) values exist as a set of data.
- The Begin Date must always be less than the End date.
- Invalid date input generates an exception and an error message stating `Invalid time interval: Begin date after end date`.

In BAPI_USER_CHANGE (GROUPS table)

- Only valid groups that exist in the SAP User Groups table can be added to a user. Invalid input generates an exception and an error message stating `User group<name> does not exist`.

In BAPI_USER_CHANGE (ADDCOMREM table)

- The LANGU and LANGU_ISO fields are set with the driver's language parameter value.

E Example XML Document Received from the Driver

The following example is a typical XML document received from the default driver configuration.

```
<nds dtdversion="1.0" ndsversion="8.5">
       <source>
               <product build="20050509_1030" instance="SAP-USER-REMOTE-46C"
version="1.0">Identity
     Manager Driver for User Management of SAP Software</product>
<contact>Novell, Inc.</contact>
       </source>
       <input xmlns:sapshim="http://www.novell.com/dirxml/drivers/sapusershim">
              <modify class-name="US" event-id="O_001_0000000000216097" src-
dn="SSAMPLE"
          timestamp="20030509">
                     <association>USdJSMITH</association>
                  <modify-attr attr-name="PROFILES:BAPIPROF">
                           <remove-all-values/>
                     </modify-attr>
                     <modify-attr attr-name="USERNAME:BAPIBNAME">
                           <remove-all-values/>
                     </modify-attr>
                 <modify-attr attr-name="ACTIVITYGROUPS:AGR_NAME">
                           <remove-all-values/>
                     </modify-attr>
                     <modify-attr attr-name="PROFILES:BAPIPROF">
                           <add-value>
                                  <value>SAP_ALL</value>
                                  <value>SAP_NEW</value>
                           </add-value>
                     </modify-attr>
                       <modify-attr attr-name="USERNAME:BAPIBNAME">
                              <add-value>
                                    <value>JSMITH</value>
                              </add-value>
                       </modify-attr>
                       <modify-attr attr-name="ACTIVITYGROUPS:AGR_NAME">
                              <add-value>
                                      <value>SAP_EMPLOYEE</value>
                              </add-value>
                        </modify-attr>
                  </modify>
          </input>
</nds>
```

Some characteristics to note:

- All XML documents received from the SAP system are translated into `<modify>` documents. This translation occurs because it is not possible to determine whether the object described by the document has been modified or is new. Additional modification or translation of the document is accomplished through policies and the Metadirectory engine.

- The `<modify>` element contains the classname of the object described in the SAP namespace (that is, US=User). The event-id attribute contains the IDoc number from which the data is derived. The src-dn attribute contains the SAP Object name value. The timestamp attribute contains the date that the IDoc was processed by the driver.
- The `<association>` element data always contains the format USd*SAPobjectID*. Usernames in SAP are always uppercase.
- The `<modify-attr>` element contains the attr-name described in SAP format (Structure or Table name:Attribute Name).
- Because multivalue attributes cannot be consistently mapped across systems, the `<remove-all-values>` element is used prior to all `<add-value>` tags on Publisher channel documents. This instructs the Metadirectory engine to remove all existing values for the attribute prior to assigning the new values. If this functionality is not desired, one of the policies can be used to modify the document.
- All values are in a string format.
- All values for DirXML-locSapRoles and DirXML-locSapProfiles require that you set two fields in SAP. In order to map from a single string value to a structured format, default policies use a colon ":" delimiter in the Identity Vault values (such as ADMCLNT100:SAP_ESSUSER), which are then transformed to (or from) the SAP structured format. The Schema Mapping policy indicates the structure components to set for these values.

F Structured Format Examples

```
// Single value field
//
<modify-attr attr-name="LOCKUSER">
     <add-value>
          <value>1</value>
     </add-value>
</modify-attr>
//
// Single field from Structure
//
<modify-attr attr-name="ADDRESS:E_MAIL">
     <add-value>
          <value>UGRANT@uniongenerals.org</value>
     </add-value>
</modify-attr>
//
// Single field, multi-values from Table
//
<modify-attr attr-name="ACTIVITYGROUPS:AGR_NAME">
     <add-value>
          <value>SAP_ESSUSER</value>
          <value>SAP_EMPLOYEE</value>
     </add-value>
</modify-attr>
//
// All fields, multi-values from Table
//
<modify-attr attr-name="LOCACTIVITYGROUPS">
     <add-value>
          <value type="structured">
                 <component name="FROM_DAT">2005-04-01</component>
                 <component name="TO_DAT">9999-12-31</component>
                 <component name="ORG_FLAG"></component>
                 <component name="AGR_NAME">SAP_ESSUSER</component>
                 <component name="SUBSYSTEM">ADMCLNT500</component>
                 <component name="AGR_TEXT"></component>
          </value>
          <value type="structured">
                 <component name="FROM_DAT">2005-04-01</component>
                 <component name="TO_DAT">9999-12-31</component>
                 <component name="ORG_FLAG"></component>
                 <component name="AGR_NAME">SAP_EMPLOYEE</component>
                 <component name="SUBSYSTEM">ADMCLNT100</component>
                 <component name="AGR_TEXT"></component>
          </value>
     </add-value>
</modify-attr>
```

G Setting and Clearing Granular Locks

The granular lock functionality is available for SAP systems that support the concept of granular locks via the `SUSR_BAPI_USER_LOCK` and `SUSR_BAPI_USER_UNLOCK` functions. These locks relate to the account locking mechanisms that are available from the Central System of an SAP Central User Administration (CUA) environment.

This functionality is only available through the SAP User Management driver if the BAPI functions are configured to be a Remote-Enabled Module and the driver is configured to support locking.

- Section G.1, "Configuring the SAP System for Granular Locking," on page 87
- Section G.2, "Configuring the Driver for Locking," on page 89

G.1 Configuring the SAP System for Granular Locking

To enable the SAP system for locking, you must enable two BAPIs for remote access by setting the Remote-Enabled Module attribute in the SAP Function Builder transaction (SE37) on each BAPI. The BAPIs are:

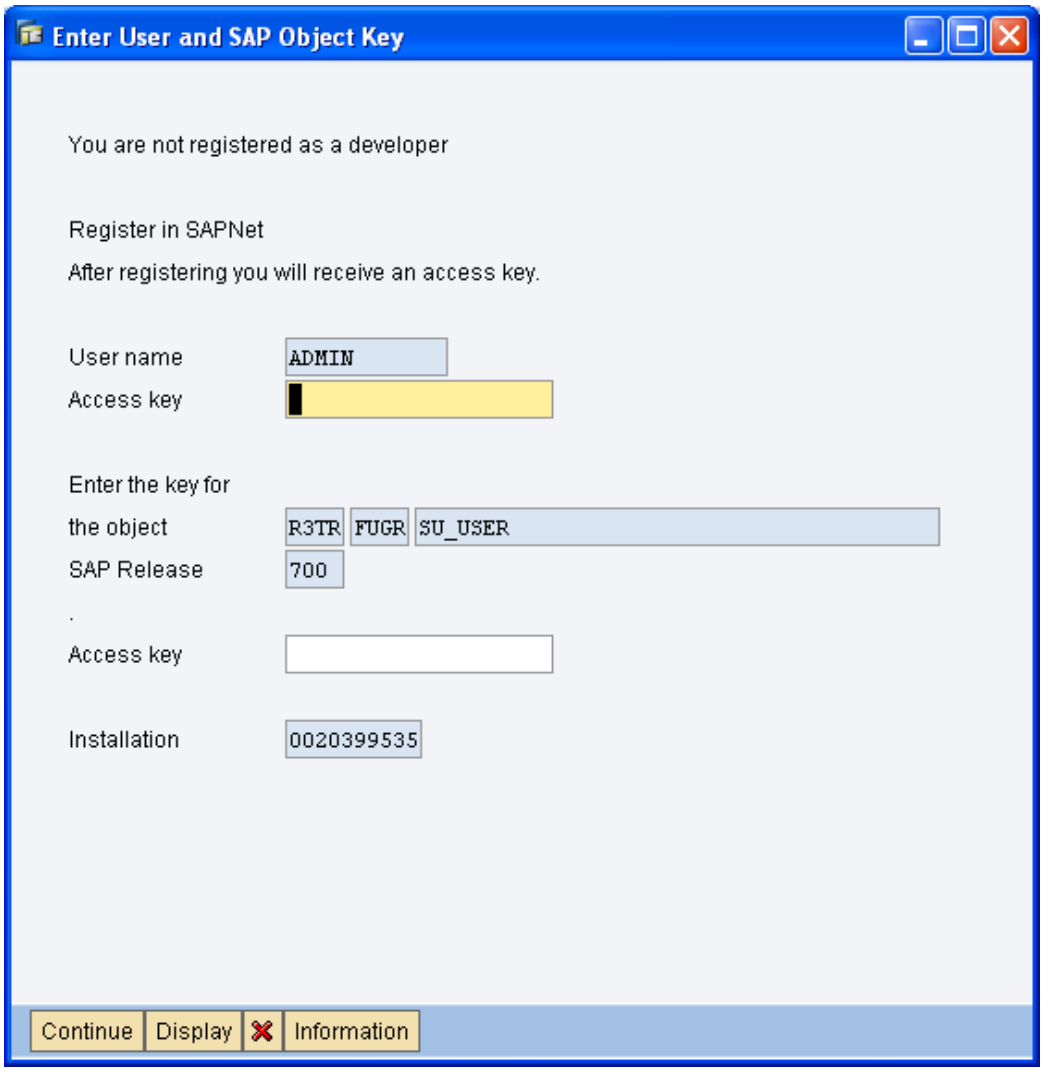
- SUSR_BAPI_USER_LOCK
- SUSR_BAPI_USER_UNLOCK

You must add this attribute to each SAP system that you want to enable locking for.

Use the following steps to configure the BAPIs:

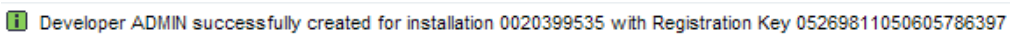
1. In the SAP GUI, specify *SE37* in the search field to launch the Function Builder, then press Enter.
2. In the Function Builder, specify *SUSR_BAPI_USER_LOCK*, then click *Change* to search for this BAPI.

3 Leave this page up and make note of the username, the installation number, and the object key number.



Now you need to register the developer and an object on the SAP Service Marketplace Web site.

1 From a Web browser, access the SAP Support Portal, then log in to your account.
2 Click *Keys and Requests* > *SSCR Keys*.
3 Click *Register Developer*.
4 Specify the user ID from Step 3 on page 88.
5 Specify the installation number from Step 3 on page 88.
6 Click *Register*.
7 Record the Registration Key number that appears at the bottom of the screen.



8 Click the *SSCR Keys* link at the top of the page to return to the main page.
9 Click *Register an Object*.

10 In the *PgmID Type Object name* field, specify the object key number `R3TR FUGR SU_USER` from Step 3 on page 88, then click *Check*.

11 Select the base release number for your system.

12 Select the Installation number from Step 3 on page 88.

13 Click *Register*.

14 Record the registration number that appears at the bottom of the screen.

15 Log out of the SAP Service Market place Web site.

16 Back in the Function Builder, specify the developer registration number in the *Access Key* field under the *User name* field.

17 Specify the registration number for the object in the *Access Key* field under the *SAP Release* field.

18 Click *Continue*, then click *Continue* in the warning message.

19 Click the *Attributes* tab, then click *Remote Enable Object* under the Processing Type.

20 Click *Save* in the toolbar.

21 If you are the system user, skip to Step 22. If you are not the system user, click *Own Requests* to create a work bench request.

This prompt appears only if you are not the system user.

21a Click *Create Request*.

21b Specify a description, then click *Save*.

21c Select the request, then click *Choose*.

21d Click *Continue*.

22 In the toolbar, click *Function Module* > *Activate* to activate the BAPI.

23 Click the *Back* icon in the toolbar to access the Function Builder.

24 Specify *SUSR_BAPI_USER_UNLOCK*, then click *Change*.

25 Click the *Attributes* tab, then click *Remote Enable Object* under the Processing Type.

26 Click *Save* in the toolbar.

27 Click *Continue*.

28 In the toolbar, click *Function Module* > *Activate* to activate the BAPI.

G.2 Configuring the Driver for Locking

After the SAP systems are configured for locking, you need to configure the driver. This is a driver setting on the Subscriber channel.

1 In Designer or iManager, access the properties of the driver.

2 Access the *Subscriber Settings*, under the *Driver Options*.

3 Set the *User Local Locking* option to *Yes*.

4 Click *OK* to save the change, then restart the driver for the change to take effect.

The driver can set or clear the supported lock types by using two pseudo-attributes called `SETGRANULARLOCKS` and `CLEARGRANULARLOCKS`.

The supported lock types for SETGRANULARLOCKS are:

- LOCK_LOCAL
- LOCK_GLOBAL

The supported lock types for CLEARGRANULARLOCKS are:

- LOCK_LOCAL
- LOCK_GLOBAL
- LOCK_WRONG_LOGON

To set or clear a particular lock, simply use a value of X or x for the desired lock type value. Any unspecified lock type sets to a value of ' ', which implies the lock type is not set or cleared.

NOTE: It is not valid to use these pseudo-attributes in a <remove-value> element.

The following is an example of what to add to a policy in a driver, if you did not set the Subscriber parameter.

```
//
// Example - Set Local Lock on User
//
<modify-attr attr-name="SETGRANULARLOCKS">
  <add-value>
    <value type="structured">
      <component name="LOCK_LOCAL">X</component>
    </value>
  </add-value>
</modify-attr>

//
// Example - Set Local and Global Locks on User
//
<modify-attr attr-name="SETGRANULARLOCKS">
  <add-value>
    <value type="structured">
      <component name="LOCK_LOCAL">X</component>
      <component name="LOCK_GLOBAL">X</component>
    </value>
  </add-value>
</modify-attr>

//
// Example - Clear Local and Wrong Logon Locks on User
//
<modify-attr attr-name="CLEARGRANULARLOCKS">
  <add-value>
    <value type="structured">
      <component name="LOCK_LOCAL">X</component>
      <component name="LOCK_WRONG_LOGON">X</component>
    </value>
  </add-value>
</modify-attr>
```

H Using Wildcard Search Capabilities

Releases of this driver prior to version 1.0.5 had issues related to the implementation of the default Subscriber Matching policy. The default Subscriber Matching policy issues a query to the SAP server for matches of the Given Name and Surname attributes (mapped to ADDRESS:FIRSTNAME and ADDRESS:LASTNAME) prior to processing the creation of a new User object. The following XDS query illustrates the output of this policy.

```
<nds dtdversion="1.1" ndsversion="8.6">
   <source>
      <product version="1.1.2">DirXML</product>
         <contact>Novell, Inc.</contact>
   </source>
   <input>
      <query class-name="US" event-id="0">
         <search-class class-name="US"/>
         <search-attr attr-name="ADDRESS:LASTNAME">
            <value timestamp="1114621366#3" type="string">Smith</value>
         </search-attr>
         <search-attr attr-name="ADDRESS:FIRSTNAME">
            <value timestamp="1114621375#1" type="string">Joe</value>
         </search-attr>
         <read-attr/>
      </query>
   </input>
</nds>
```

This is a problem because SAP does not provide the capability to search for a User account based on attribute values. Therefore, the driver needs to obtain a list of all User objects, then read each object, compare the FIRSTNAME and LASTNAME attributes to the search values, and return a list of matching objects. In a database with hundreds or thousands of User objects, this process takes a very long time.

To eliminate this problem, starting with version 1.0.5, the driver now has the capability to use a wildcard syntax for queries that contain the User name field (USERNAME:BAPIBNAME). This allows you to write policies that take advantage of the known account naming policies of the SAP system to reduce the number of objects that need to be read and compared during matching operations.

For example, the default Subscriber Create rule uses the first initial of the Given Name attribute value appended with the Surname attribute value to create a proposed account name. A new User with Given Name “John” and Surname “Smith” generates a proposed SAP User account name of JSMITH. Any duplicates of this proposed name are appended with numeric values (for example, JSMITH1, JSMITH2, etc.) The default Output Transformation policy now contains a template that takes advantage of the USERNAME:BAPIBNAME wildcard capabilities of the driver and appends this additional search attribute to the query. When the driver receives a query containing a USERNAME:BAPIBNAME search attribute, it determines if the value is a wildcard or a literal value. Any value that is contained within single-quote characters is evaluated for wildcard syntax. If the single-quote characters do not exist, the driver attempts to read the specified User object.

The supported variations of the wildcard syntax are:

- Starts-with syntax (for example, ‘JSmith*’). Restricts attribute matching to User account names starting with JSMITH.
- Ends-with syntax (for example, ‘*ith’). Restricts attribute matching to User account names ending with ITH.
- Contains syntax (for example, ‘*SMIT*’). Restricts attribute matching to User account names containing SMIT.

When the list of objects to be matched has been restricted, the remaining search attributes are used to determine a match.

The output from the default Output Transform policy converts the Matching Rule query shown above to the following query. This policy is only applied to queries that do not already contain a USERNAME:BAPIBNAME search attribute.

```
<nds dtdversion="1.1" ndsversion="8.6">
   <source>
      <product version="1.1.2">DirXML</product>
      <contact>Novell, Inc.</contact>
   </source>
   <input>
      <query class-name="US" event-id="0">
         <search-class class-name="US"/>
         <search-attr attr-name="ADDRESS:LASTNAME">
            <value timestamp="1114621366#3" type="string">Smith</value>
         </search-attr>
         <search-attr attr-name="ADDRESS:FIRSTNAME">
            <value timestamp="1114621375#1" type="string">Joe</value>
         </search-attr>
         <read-attr/>
         <search-attr attr-name="USERNAME:BAPIBNAME">
            <value>’JSmith*’</value>
         </search-attr>
      </query>
   </input>
</nds>
```

With this query, the driver searches only User objects whose name starts with JSMITH for the matching ADDRESS:LASTNAME value “Smith” and matching ADDRESS:FIRSTNAME value “Joe.”