

Driver for SAP User Management Implementation Guide

Novell® Identity Manager

4.0

October 15, 2010

www.novell.com



Legal Notices

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

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

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

Copyright © 2005-2010 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	9
1 Understanding the SAP User Management Driver	11
1.1 Supported SAP Versions	11
1.2 Driver Concepts	11
1.2.1 Publisher Channel	12
1.2.2 Subscriber Channel	14
1.2.3 Attribute Mapping from the SAP User Management Database to the Identity Vault	14
1.2.4 Associations	15
1.3 Driver Components	15
1.3.1 Driver Packages	16
1.3.2 Driver Shim	16
1.3.3 SAP User Java Connector Test Utility	16
1.4 Support for Standard Driver Features	16
1.4.1 Local Platforms	16
1.4.2 Remote Platforms	17
1.4.3 Entitlements	17
1.4.4 Account Tracking	17
1.4.5 Role Mapping Administrator	17
2 Installing the Driver Files	19
3 Configuring the SAP System	21
3.1 Defining Sending and Receiving Systems	21
3.1.1 Creating a Logical System	22
3.1.2 Assigning a Client to the Logical System	22
3.2 Creating a Distribution Model	22
3.3 Creating a Port Definition	23
3.3.1 Creating a TRFC Port Definition	23
3.3.2 Creating a File Port Definition	24
3.4 Configuring SAP Gateway Ports	25
3.5 Generating Partner Profiles	25
3.5.1 Generating a Profile	25
3.5.2 Modifying the Port Definition	25
3.6 Activating Central User Administration	26
3.7 Creating a Communication (CPIC) User	26
4 Testing the SAP JCO Client Connection	29
4.1 About the Utility	29
4.1.1 Utility Prerequisites	29
4.1.2 Components	30
4.1.3 Running and Evaluating the Test	30
4.1.4 Understanding Test Error Messages	32
5 Creating a New Driver	35
5.1 Creating an SAP User Account	35

5.2	Creating the Driver in Designer	35
5.2.1	Importing the Current Driver Packages	35
5.2.2	Installing the Driver Packages	36
5.2.3	Configuring the Driver	40
5.2.4	Deploying the Driver	40
5.2.5	Starting the Driver	41
5.3	Creating the Driver in iManager	41
5.4	Activating the Driver	41
6	Upgrading an Existing Driver	43
6.1	Supported Upgrade Paths	43
6.2	What's New in Version 4.0	43
6.3	Upgrade Procedure	43
7	Customizing the Driver	45
7.1	Modifying the Policies and the Filter	45
7.1.1	Filter Publish Options	46
7.1.2	Filter Subscribe Options	46
7.1.3	Schema Mapping Policy	47
7.1.4	Input Transform Policy	50
7.1.5	Output Transform Policy	51
7.1.6	Publisher Placement Policy	51
7.1.7	Publisher Matching Policy	51
7.1.8	Publisher Create Policy	51
7.1.9	Subscriber Matching Policy	52
7.1.10	Subscriber Create Policy	52
7.2	Adding the Organizational Role Class	53
7.2.1	Editing the Global Configuration Values	53
7.2.2	Adding a New Placement Rule	54
7.2.3	Modifying the XSLT	55
7.2.4	Adding the Organizational Role Class to the Driver Filter	55
7.2.5	Migrating Data into the Identity Vault	56
7.3	Obtaining Company Address Data for User Objects	56
8	Using the Driver in a Central User Administration Environment	59
8.1	Overview	59
8.2	Configuring the Driver as a CUA Child System	61
8.3	Using the Driver to Provision a CUA Landscape	63
8.4	User Classification Settings (Licensing)	64
8.5	Important CUA Integration Notes	65
9	Managing the Driver	67
10	Troubleshooting the Driver	69
10.1	Troubleshooting Driver Processes	69
10.2	Driver Errors	69
10.2.1	JCo 3	69
A	Driver Properties	71
A.1	Driver Configuration	71

A.1.1	Driver Module	72
A.1.2	Driver Object Password (iManager Only)	72
A.1.3	Authentication	72
A.1.4	Startup Option	73
A.1.5	Driver Parameters	73
A.1.6	ECMAScript	76
A.1.7	Global Configurations	76
A.2	Global Configuration Values	76
A.2.1	Password Synchronization	77
A.2.2	Account Tracking	78
A.2.3	Managed System Information	79
A.2.4	SAP User Management Driver	80
B	Application Link Enabling (ALE)	81
B.1	Clients and Logical Systems	81
B.2	Message Type	81
B.3	IDoc Type	82
B.4	Distribution Model	82
B.5	Partner Profiles	82
B.6	Port	82
B.7	Port Definition	82
B.8	File Port	82
B.9	TRFC Port	83
B.10	CUA	83
C	Business Application Programming Interfaces (BAPIs)	85
D	Configuration and Deployment Notes	87
D.1	SAP Object Types	87
D.2	User Types: LOGONDATA:USTYP	87
D.3	Output Controller Options	88
D.4	Communication Types: ADDCOMREM:COMM TYPE	88
D.5	Date Formats: DEFAULTS:DATAFM	88
D.6	Decimal Formats: DEFAULTS:DCPFM	88
D.7	Computer Aided Test (CATT): DEFAULTS:CATTKENNZ	88
D.8	Communication Comment Type to Table Mappings	89
D.9	Language Codes	89
D.10	Configuration Parameters	90
D.11	Design Comments and Notes	90
D.11.1	BAPI_USER_CHANGE (ADDRESS table)	91
D.11.2	BAPI_USER_CHANGE (ADDFAX table)	91
D.11.3	BAPI_USER_CHANGE (ADDTTEL table)	91
D.11.4	BAPI_USER_CHANGE (ADDTLX table)	91
D.11.5	In BAPI_USER_CHANGE (ADDFAX table)	92
D.11.6	In BAPI_USER_CHANGE (GROUPS table)	92
D.11.7	BAPI_USER_CHANGE (ALIAS structure)	92
D.11.8	BAPI_USER_CHANGE (REF_USER structure)	92
D.11.9	BAPI_USER_CHANGE (DEFAULTS structure)	92
D.11.10	BAPI_USER_CHANGE (LOGONDATA structure)	93
D.11.11	BAPI_USER_CHANGE (GROUPS table)	93
D.11.12	BAPI_USER_CHANGE (ADDCOMREM table)	93

E	Example XML Document Received from the Driver	95
F	Structured Format Example	97
G	Setting and Clearing Granular Locks	99
G.1	Examples	99
H	Using Wildcard Search Capabilities	101

About This Guide

This manual is for Novell Identity Manager administrators, SAP developers and administrators, and others who implement the Identity Manager Driver for User Management of SAP Software.

The guide contains the following sections:

- ♦ Chapter 1, “Understanding the SAP User Management Driver,” on page 11
- ♦ Chapter 2, “Installing the Driver Files,” on page 19
- ♦ Chapter 3, “Configuring the SAP System,” on page 21
- ♦ Chapter 4, “Testing the SAP JCO Client Connection,” on page 29
- ♦ Chapter 5, “Creating a New Driver,” on page 35
- ♦ Chapter 6, “Upgrading an Existing Driver,” on page 43
- ♦ Chapter 7, “Customizing the Driver,” on page 45
- ♦ Chapter 8, “Using the Driver in a Central User Administration Environment,” on page 59
- ♦ Chapter 9, “Managing the Driver,” on page 67
- ♦ Chapter 10, “Troubleshooting the Driver,” on page 69
- ♦ Appendix A, “Driver Properties,” on page 71
- ♦ Appendix B, “Application Link Enabling (ALE),” on page 81
- ♦ Appendix C, “Business Application Programming Interfaces (BAPIs),” on page 85
- ♦ Appendix D, “Configuration and Deployment Notes,” on page 87
- ♦ Appendix E, “Example XML Document Received from the Driver,” on page 95
- ♦ Appendix F, “Structured Format Example,” on page 97
- ♦ Appendix G, “Setting and Clearing Granular Locks,” on page 99
- ♦ Appendix H, “Using Wildcard Search Capabilities,” on page 101

Feedback

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

Documentation Updates

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

Additional Documentation

For documentation on using Identity Manager and the other drivers, see the [Identity Manager 4.0 Documentation Web site \(http://www.novell.com/documentation/idm40\)](http://www.novell.com/documentation/idm40).

Understanding the SAP User Management Driver

1

The Identity Manager Driver for SAP User Management, subsequently referred to as the SAP User driver, creates an automated link between the Identity Vault and SAP User Management systems (BASIS or Web Application Server.) This technology enables data flow within a business enterprise based on its own unique requirements, and eliminates the labor-intensive and error-prone practice of re-entering the same data into multiple databases. As User object records are added, modified, deactivated (disabled), or deleted in SAP or the Identity Vault, network tasks associated with these events can be processed automatically.

The driver allows administrators to propagate User data between SAP systems and other business applications and databases without the need for custom integration solutions. Administrators can decide what data will be shared and how data will be presented within their enterprises.

In this section:

- ♦ [Section 1.1, “Supported SAP Versions,” on page 11](#)
- ♦ [Section 1.2, “Driver Concepts,” on page 11](#)
- ♦ [Section 1.3, “Driver Components,” on page 15](#)
- ♦ [Section 1.4, “Support for Standard Driver Features,” on page 16](#)

1.1 Supported SAP Versions

The driver supports the following SAP versions:

- ♦ SAP R/3 version 4.5B or higher
- ♦ mySAP

1.2 Driver Concepts

The driver is a bidirectional synchronization product between SAP R/3 and Enterprise R/3 systems and the Identity Vault. This framework uses XML and XSLT to provide data and event transformation capabilities that convert Identity Vault data and events into SAP data and vice-versa.

The Identity Vault acts as a hub, with other applications and directories publishing their changes to it. The Identity Vault then sends changes to the applications and directories that have subscribed for them. This results in two main flows of data: the Publisher channel and the Subscriber channel.

- ♦ [Section 1.2.1, “Publisher Channel,” on page 12](#)
- ♦ [Section 1.2.2, “Subscriber Channel,” on page 14](#)
- ♦ [Section 1.2.3, “Attribute Mapping from the SAP User Management Database to the Identity Vault,” on page 14](#)
- ♦ [Section 1.2.4, “Associations,” on page 15](#)

1.2.1 Publisher Channel

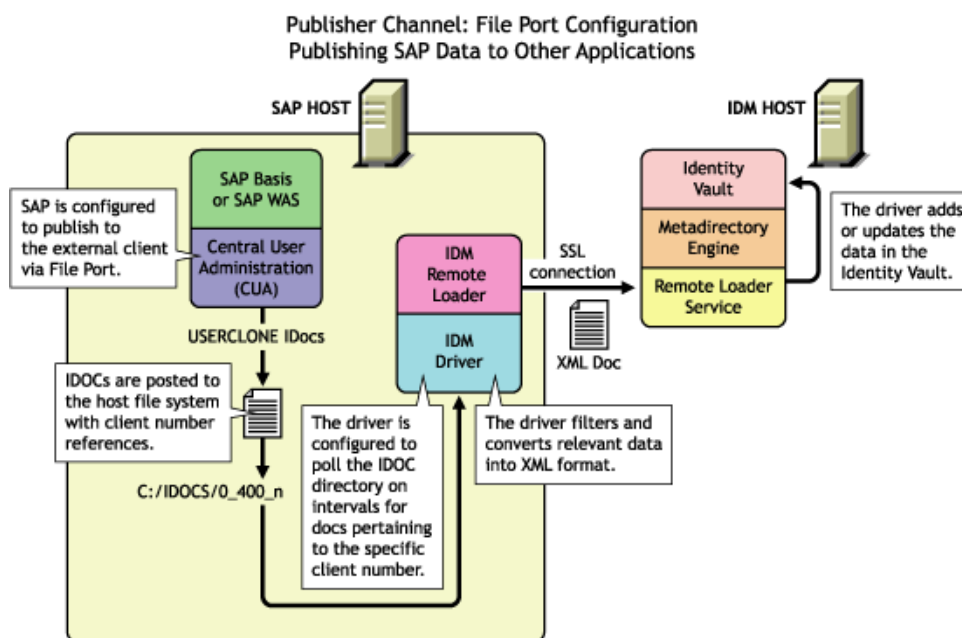
The SAP system publishes User object information in the form of USERCLONE IDocs using Application Link Enabling (ALE) and Central User Administration (CUA) technology. If desired and properly configured, the SAP system can propagate all Add, Delete, Lock, Unlock, and Modify User event data to the Identity Vault. The driver consumes the IDoc data and converts it into XML format. For more information on how the driver handles IDoc processing, refer to “[IDoc Consumption by the Driver](#)” on page 13.

The Publisher channel then submits XML-formatted documents to the Metadirectory engine for publication into the Identity Vault. By using Identity Manager and other Identity Manager drivers, the data can be shared with other business applications and directories. These other applications can add additional data, which in turn can be transferred back into the SAP User records using the standard SAP Business Application Programming Interface (BAPI).

Depending on the ALE port configuration you choose, the Publisher channel either polls the SAP database for changes via a file port or it receives the data via a TRFC connection.

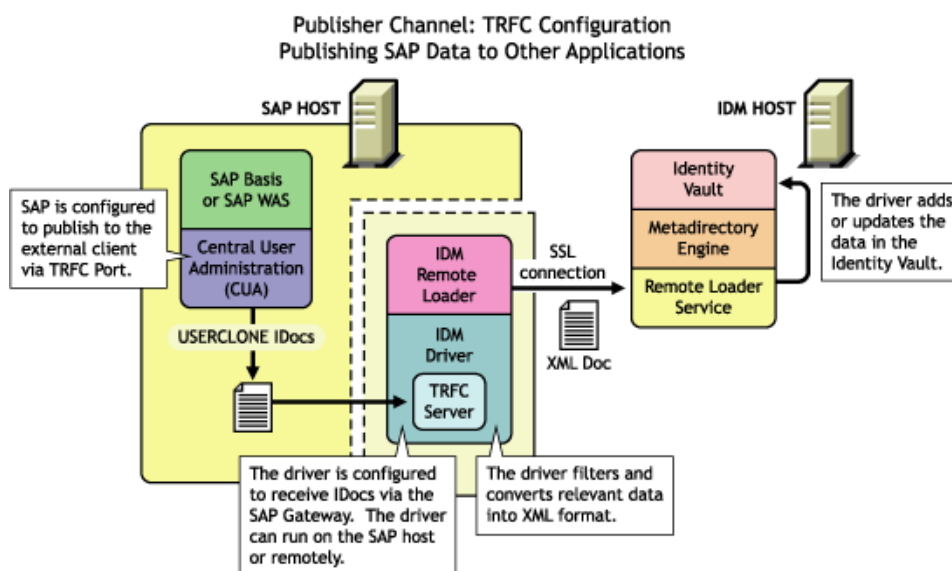
The following diagram illustrates the file port configuration. With the file port configuration, the entire IDoc is stored on the SAP host system.

Figure 1-1 Publishing Data to the Identity Vault by using the File Port Configuration



The following diagram illustrates the TRFC port configuration. When you use the TRFC configuration, a minimal “trigger” IDoc is stored on the driver host system. The driver handles the parsing of the IDoc data and uses the information to read the current User object. The driver then parses the appropriate data fields specified by the driver configuration, and provides secure transport of the data to the Identity Vault. Only data elements specifically selected by the system administrator are transported from the SAP host system to the Identity Vault.

Figure 1-2 Publishing Data to the Identity Vault by using the TRFC Configuration



IDoc Consumption by the Driver

The driver consumes only Output IDoc files with the client number that is specified by the driver configuration, thus ensuring the privacy of other IDocs that might be generated by another driver configuration or ALE integration. Only the IDoc attributes that have been specified in the driver Publisher filter are published to the Identity Vault.

The format of a successfully published IDoc file is:

`<(I)npud or (O)utput>_<client number>_<consecutive IDoc number>`

For example:

`O_300_0000000000001001`

After the IDoc has been processed and specified attributes have been published, the filename of the IDoc file is modified to reflect the status of the publication processes. The following table lists the IDoc status and corresponding extension:

IDoc Status	Filename Extension
Processing but not published	.proc
Processed successfully and published	.done
Processed with an error or warning	.fail or .warn
Processed and retained for future-dated processing	.futr
Processed with corrupt or illegitimate data	.bad

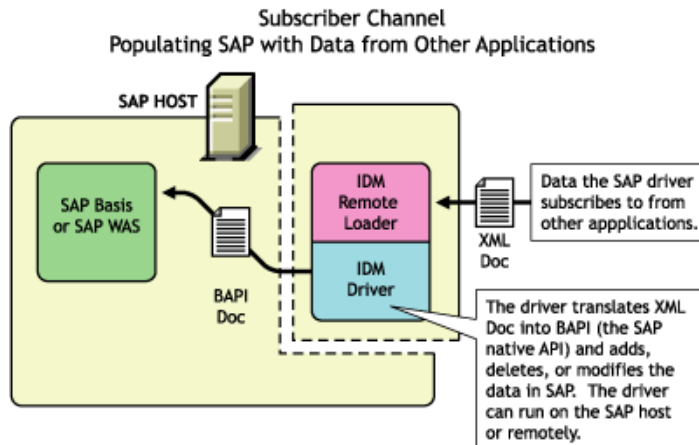
You should determine what action is required, if any, after IDoc publication is complete.

NOTE: Removing the filename extension makes the IDoc available for re-processing.

1.2.2 Subscriber Channel

The Subscriber channel receives XML-formatted Identity Vault events from the Metadirectory engine. The driver converts these documents to an appropriate data format, and updates SAP via the BAPI interface. The Identity Vault sends changes only to the applications that subscribe to receive them.

Figure 1-3 *Populating SAP with Data*



For data to flow from the Identity Vault to the SAP system, the driver uses the SAP BAPI functions. The level of functionality is based upon the R/3 release level. By default, the driver is configured to support a SAP 4.6C system using USERCLONE03 messages. (To determine the level of USERCLONE messages available on your SAP system, run transaction WE60 and specify object name USERCLONEnn.) As a SAP administrator, you can select which attributes from the infotypes can be modified.

1.2.3 Attribute Mapping from the SAP User Management Database to the Identity Vault

Schema mapping is used by Identity Manager to translate data elements as they flow between the SAP User Management database and the Identity Vault. The SAP User object schema is based on the SAP USERCLONE message type. The schema map contains all attributes of the various data infotypes of the USERCLONE message type.

Several of the USERCLONE infotypes can be instantiated multiple times on the User records. Infotypes such as ADDTEL (Telephone Number) and ACTIVITYGROUPS (Roles) are *Table* fields and can contain multiple values. Other infotypes such as ADDRESS and LOGONDATA are *Structure* fields and are instantiated only once but have multiple fields associated with them. Still other fields are *simple* field types that contain only a single data field element.

The Identity Vault (eDirectory) system administrator can configure the driver to receive any of these various data fields, and can also configure the driver to handle the data in multiple ways. The Schema Map represents the data elements that can be synchronized in the SAP system.

The map elements have the following format:

```
<Table or Structure Name>:<Field>    // Field
```

or

<Table Name> // Map to entire table or structure

Below are a few examples of maps between SAP User attributes and Identity Vault attributes.

Identity Vault Attribute	SAP User Attribute
Given Name	ADDRESS:FIRSTNAME
Surname	ADDRESS:LASTNAME
sapRoles	ACTIVITYGROUPS:AGR_NAME
buildingName	ADDRESS:BUILDING_P
floor	ADDRESS:FLOOR_P
Internet EMail Address	ADDSMTP:E_MAIL
OU	ADDRESS:DEPARTMENT
Pager	ADDPAG:PAGER
sapAlias	ALIAS:USERALIAS
DirXML-sapLocRoles	LOCACTIVITYGROUPS

The driver can synchronize multiple-instance data (such as TELEPHONE), but it cannot guarantee the specification of a primary value. It is also possible to specify only the Table name in a schema mapping. This is useful if you want to synchronize all data fields in a Table to the Identity Vault. You must use policies to parse desired fields from the Table data. Refer to [Appendix E, “Example XML Document Received from the Driver,” on page 95](#) to see how various formats are represented in modify events.

1.2.4 Associations

Associations are created between SAP and Identity Vault objects during the synchronization process. For the SAP User object, a unique 12-character name (per client) must be created. However, the Identity Vault and other applications do not need to share this same unique ID. Identity Manager allows the various naming policies in an organization to be applied to objects by using the DirXML-Association attribute.

The DirXML-Association attribute is multivalued. Therefore, if Identity Manager is being used to synchronize an object among multiple applications, all of the object’s unique IDs (or associations) can be stored in this attribute on the Identity Vault object.

The unique ID association links objects in SAP to their objects in the Identity Vault. When an Add or Matching event occurs, the association is made. This association allows the driver to perform subsequent tasks on the appropriate object.

The DirXML-Associations field is stored on the Identity Vault object on the Identity Manager property page.

1.3 Driver Components

This sections contains information about the following driver components.

- ♦ [“Driver Packages” on page 16](#)

- ♦ [“Driver Shim” on page 16](#)
- ♦ [“SAP User Java Connector Test Utility” on page 16](#)

1.3.1 Driver Packages

After you install Identity Manager and the driver, you create one or more Driver objects. Each Driver object represents an instance of the SAP User driver. The driver packages gets you up and running with a minimum of customization by letting you create a Driver object with preconfigured policies, filters, and driver parameters.

1.3.2 Driver Shim

The driver shim handles communication between the SAP User database and the Metadirectory engine.

1.3.3 SAP User Java Connector Test Utility

In order to use the driver, you must download the SAP JCO and install it. The SAP User Java Connector (JCO) Test utility enables you to check for JCO installation and configuration issues prior to configuring the driver. You can use the JCO test utility to validate correct installation of the JCO client and configuration issues prior to configuring the driver.

You can use the JCO test utility to validate correct installation of the JCO client and connectivity to the SAP host system, as well as testing for accessibility of the User Management BAPIs used by the driver. For more information, refer to [Chapter 4, “Testing the SAP JCO Client Connection,” on page 29](#).

1.4 Support for Standard Driver Features

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

- ♦ [Section 1.4.1, “Local Platforms,” on page 16](#)
- ♦ [Section 1.4.2, “Remote Platforms,” on page 17](#)
- ♦ [Section 1.4.3, “Entitlements,” on page 17](#)
- ♦ [Section 1.4.4, “Account Tracking,” on page 17](#)
- ♦ [Section 1.4.5, “Role Mapping Administrator,” on page 17](#)

1.4.1 Local Platforms

A local installation is an installation of the driver on the same server as the Metadirectory engine, Identity Vault, and SAP User application. Both systems that the driver needs to communicate with (Metadirectory engine and SAP User application) are local to the driver.

The SAP User driver can be installed on the same operating systems supported by the Metadirectory server. For information about the operating systems supported by the Metadirectory server, see [“System Requirements”](#) in the *Identity Manager 4.0 Integrated Installation Guide*.

1.4.2 Remote Platforms

The SAP User driver must reside on the same server as the SAP User application. 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 while having the Metadirectory engine and Identity Vault on another server.

The SAP User driver can be installed on the same operating systems supported by the Remote Loader. For information about the operating systems supported by the Remote Loader, see “[System Requirements](#)” in the *Identity Manager 4.0 Integrated Installation Guide*.

1.4.3 Entitlements

The SAP User driver does not have entitlement functionality defined with the default configuration file. The driver does support entitlements, if there are policies created for the driver to consume.

1.4.4 Account Tracking

The SAP User driver supports account tracking that is a feature of the Novell Compliance Management Platform. For more information, see the [Novell Compliance Management Platform Web site](http://www.novell.com/products/compliancemanagementplatform/) (<http://www.novell.com/products/compliancemanagementplatform/>).

1.4.5 Role Mapping Administrator

The SAP User driver supports the Roles Mapping Administrator that comes with Identity Manager. For more information, see the *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide*.

Installing the Driver Files

2

By default, the SAP User driver files are installed on the Metadirectory server at the same time as the Metadirectory engine. The installation program extends the Identity Vault's schema and installs the driver shim and the driver configuration file. It does not create the driver in the Identity Vault (see [Chapter 5, “Creating a New Driver,” on page 35](#)) or upgrade an existing driver's configuration (see [Chapter 6, “Upgrading an Existing Driver,” on page 43](#)).

The SAP User driver must be located on the same server as the SAP User application. If the driver is not on that server, you have the following options:

- ♦ Install the Metadirectory server (Metadirectory engine and drivers) to the SAP server. This requires eDirectory to be installed on the server. See the instructions in “[Installing Identity Manager](#)” in the *Identity Manager 4.0 Integrated Installation Guide*.
- ♦ Install the Remote Loader (required to run the driver on a non-Metadirectory server) and the SAP User driver files to the SAP server. This assumes that you already have a Metadirectory server installed on another server in your environment. See “[Installing Identity Manager](#)” in the *Identity Manager 4.0 Integrated Installation Guide*.

As part of the Metadirectory installation, select the *Utilities* option and install the SAP Utilities. This installs the SAP Java Connector Test utility that you can use to ensure that the driver has connection to the SAP system. If you've already installed the driver files but did not install the SAP Utilities, you can run the installation program again to install only the SAP Utilities.

Installing the SAP Java Connector Client

The server where the SAP driver is installed must have the SAP Java Connector (JCO) client technology version 1.1.x, 2.x, and 3.x to provide the driver with connectivity to the SAP system.

This JCO client is available to SAP customers and developer partners through SAP, and is provided for most popular server operating systems. You can download the JCO from the [SAP Connectors site \(http://service.sap.com/connectors\)](http://service.sap.com/connectors).

Configuring the SAP System

3

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. This configuration must be completed before you create the driver. Make sure you have sufficient rights to configure the distribution model and to distribute user data via ALE.

Novell follows SAP's general guidelines for configuring BAPI (Business Application and Programming Interface) and ALE technologies for this integration solution. For information about BAPI, see [Appendix C, "Business Application Programming Interfaces \(BAPIs\)," on page 85](#). For information about ALE, see [Appendix B, "Application Link Enabling \(ALE\)," on page 81](#).

Complete the steps in the following sections in the order listed. The instructions are for SAP version 4.6C. If you are using a previous version of SAP, the configuration process is the same; however, the SAP interface will be different.

- ♦ [Section 3.1, "Defining Sending and Receiving Systems," on page 21](#)
- ♦ [Section 3.2, "Creating a Distribution Model," on page 22](#)
- ♦ [Section 3.3, "Creating a Port Definition," on page 23](#)
- ♦ [Section 3.4, "Configuring SAP Gateway Ports," on page 25](#)
- ♦ [Section 3.5, "Generating Partner Profiles," on page 25](#)
- ♦ [Section 3.6, "Activating Central User Administration," on page 26](#)
- ♦ [Section 3.7, "Creating a Communication \(CPIC\) User," on page 26](#)

3.1 Defining Sending and Receiving Systems

The sending and receiving systems must be defined for messaging. 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.

3.1.1 Creating a Logical System

- 1 In SAP, type 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: *systemIDCLNTclient 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.

3.1.2 Assigning a Client to the Logical System

- 1 In SAP, type 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 the *sender* logical system you want to assign to this client (such as `ADMCLNT100`).
- 6 Save your entry.

3.2 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 on 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 Specify the short text to describe the distribution model (such as Client 100 Distribution to Identity Manager).
- 5 Specify the technical name for the model (such as `SAP2IDM`).
- 6 Accept the default Start and End dates or specify valid values, then 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, specify the name of the *sender* logical system (such as `ADMCLNT100`).

- 9 In the *Receiver/Client* field, specify the name of the *receiver* logical system (such as DRVCLNT100).
- 10 In the *Obj. Name/Interface* field, specify the USER object name.
Ensure that you specify the USER object name with all capital letters.
- 11 In the *Method* field, specify 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, specify Clone.
- 19 Click the check mark icon to save your BAPI entries.
- 20 Save the Distribution Model entries.

3.3 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 default driver configuration assumes that you use the TRFC port configuration.

- ♦ [Section 3.3.1, “Creating a TRFC Port Definition,” on page 23](#)
- ♦ [Section 3.3.2, “Creating a File Port Definition,” on page 24](#)

3.3.1 Creating a TRFC Port Definition

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

- ♦ [“Creating the RFC Destination” on page 23](#)
- ♦ [“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, specify transaction code SM59.
- 2 Click the *Create* icon.
- 3 Name the RFC destination (use the driver’s logical system name, for example, DRVCLNT100.)
- 4 Select *T* as the connection type (for a TCP/IP connection.)
- 5 Specify 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*. Specify the program ID to be used for the driver. In the default driver configuration, 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, specify transaction code *WE21*.
- 2** Select *Transactional RFC*, then click the *Create* icon.
- 3** Select *Own Port Option Name*.
 - 3a** Specify a port name (such as IDMPORT).
 - 3b** Specify 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.

3.3.2 Creating a File Port Definition

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

- 1** In SAP, specify transaction code *WE21*.
- 2** Select *File*, then click the *Create* icon.
 - 2a** Specify a port name (such as IDMPFILE).
 - 2b** Specify 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.
Specify the directory where the outbound files are written, for example:
`\\sapdev\nov\sys\global\sapndsconnector.`
 - 3b** Specify the function module. 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).

3.4 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 auto configuration of these ports is prohibited in SUSE Linux Enterprise Server. The ports must be manually configured in the `/etc/services` file.

For example, if the SAP System is 01, you must add the following entry to the `/etc/services` file.:

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

3.5 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.

3.5.1 Generating a Profile

- 1 In SAP, specify 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.

3.5.2 Modifying the Port Definition

For your system to work properly, you might need to modify the port definition.

- 1 In SAP, specify 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.
 - 9** (Optional) If you want to distribute company address data, add the necessary information:
 - 9a** Click the *Create Outbound Parameter* icon, then select message type *CCLONE*.
 - 9b** Modify the receiver port so it is the *file* or *TRFC port name* you created earlier (such as *IDMPORT* or *IDMFILE*.)
 - 9c** (Conditional) If you are using a TRFC port, modify the packet size. Select Packet Size = 1.
 - 9d** Under *Output Mode*, select *Transfer IDoc Immediately* to send IDocs immediately after they are created.
 - 9e** In the *IDoc type* section, select *Basic type* and the appropriate *CCLONE*. (For all SAP versions, select *CCLONE01*.)
 - 9f** Save your entries.

3.6 Activating Central User Administration

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

- 1** In SAP, specify 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.

3.7 Creating a Communication (CPIC) User

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

- 1** In SAP, specify transaction code *SU01*.
- 2** From *User Maintenance*, specify a username in the *User* dialog box (such as *IDM_CPIC*), then click the *Create* icon.
- 3** Click the *Address tab*, then specify 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. Specify 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.

Testing the SAP JCO Client Connection

4

The driver uses the SAP Java Connector (JCO) 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 R/3 system. After the driver is connected to the R/3 system, it calls methods on business objects within the R/3 system 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 1.3.1 or later.

The following sections apply to JCO versions 1.1x, 2.x, and 3.x:

In this section:

- ♦ [“About the Utility” on page 29](#)
- ♦ [“Running and Evaluating the Test” on page 30](#)
- ♦ [“Understanding Test Error Messages” on page 32](#)

4.1 About the Utility

The JCO Test utility completes the following checks:

- ♦ Ensures that the `sapjco3.jar` file, which contains the exported JCO interface, is present.
- ♦ 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.

4.1.1 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 \(http://www.sap-ag.de/services\)](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 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 SAP User driver.

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.

4.1.2 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 is listed separately for the `UserJCO3Test.class` file.

UserJCO3Test.class: The `sapjco3.jar` is in the executable directory of the `UserJCO3Test.class` file and the batch file.

```
Win32 jco3test.bat file
java -classpath %CLASSPATH%;. UserJCO3Test
```

```
Unix jco3test file
java User3JCOTest
```

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.

4.1.3 Running and Evaluating the Test

- ♦ [“Running the Test” on page 30](#)
- ♦ [“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 In Windows Explorer, double-click `UserJCO3Test.bat`.
or
In a command prompt, run the `UserJCO3Test.bat` script.

To run the JCO Test utility on a UNIX platform:

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

NOTE: When you run the test program, an error message sometimes appears 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):

```
**All expected platform support is verified correct.
```

```
JCO Test Summary
```

```
-----
```

```
Full JCO/BAPI Functionality has been verified.
```

```
The following parameters may be used for 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
```

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

****There are <number> required BAPI functions NOT supported on this platform.**

JCO Test Summary

JCO/BAPI functionality issues have been detected that will prevent proper driver functionality.

Post-Test Procedures

After the JCO Test utility has successfully passed all tests, you can create the driver. See [Chapter 5, “Creating a New Driver,” on page 35](#) for more information. 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.

4.1.4 Understanding Test Error Messages

Use the information in this section to analyze error messages that might display during the User JCO Test. Some errors are applicable to all platforms, and other errors are platform-specific.

The test has been run on the platforms listed below. Other UNIX platforms supported by the JCO are configured in a similar manner and errors generated by improper JCO installation and configuration should be similar to the errors described below. Because of periodic modifications of the JCO, messages might not be exactly as shown.

JCO3 General Errors

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

Error Message	Problem
Caught Exception during connection: java.lang.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).

Error Message	Problem
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 login) on <host> sysnr <system number>	Invalid credentials (JCo 3.0.2+).
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.nativeCpicGetVerstio n([I)I Verify proper installation of JCo Native support libraries packaged with JCo client	Exception while initializing JCo client 3.0.2+.

Creating a New Driver

5

After the SAP User driver files are installed on the server where you want to run the driver (see [Chapter 2, “Installing the Driver Files,” on page 19](#)), and after you have configured the SAP system and tested the SAP JCo client ([Chapter 3, “Configuring the SAP System,” on page 21](#) and [Chapter 4, “Testing the SAP JCO Client Connection,” on page 29](#)), 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 5.1, “Creating an SAP User Account,” on page 35](#)
- ♦ [Section 5.2, “Creating the Driver in Designer,” on page 35](#)
- ♦ [Section 5.3, “Creating the Driver in iManager,” on page 41](#)
- ♦ [Section 5.4, “Activating the Driver,” on page 41](#)

5.1 Creating an SAP User Account

The driver requires an administrative account for access to the SAP User system. You can use an existing administrative account; however, we recommend that you create an administrative account exclusively for the driver.

5.2 Creating the Driver in Designer

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

- ♦ [Section 5.2.1, “Importing the Current Driver Packages,” on page 35](#)
- ♦ [Section 5.2.2, “Installing the Driver Packages,” on page 36](#)
- ♦ [Section 5.2.3, “Configuring the Driver,” on page 40](#)
- ♦ [Section 5.2.4, “Deploying the Driver,” on page 40](#)
- ♦ [Section 5.2.5, “Starting the Driver,” on page 41](#)

5.2.1 Importing the Current Driver Packages

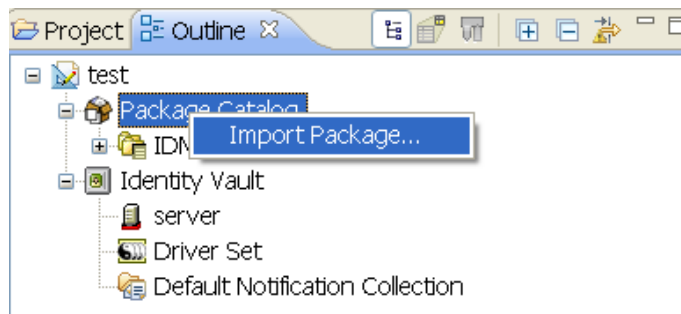
The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package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

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

- 1 Open Designer.
 - 2 In the toolbar, click *Help > Check for Package Updates*.
 - 3 Click *OK* to update the packages
- or

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

- 4 In the Outline view, right-click the Package Catalog.
- 5 Click *Import Package*.



- 6 Select any SAP User Management 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 5.2.2, “Installing the Driver Packages,”](#) on page 36.

5.2.2 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 driver. All options are selected by default.

Default Configuration: These packages contain the default configuration information for the SAP User Management 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. If you are using the fan-out configuration, you should be using the [Identity Manager 4.0 Fan-Out Driver for SAP User Management Implementation Guide](#).

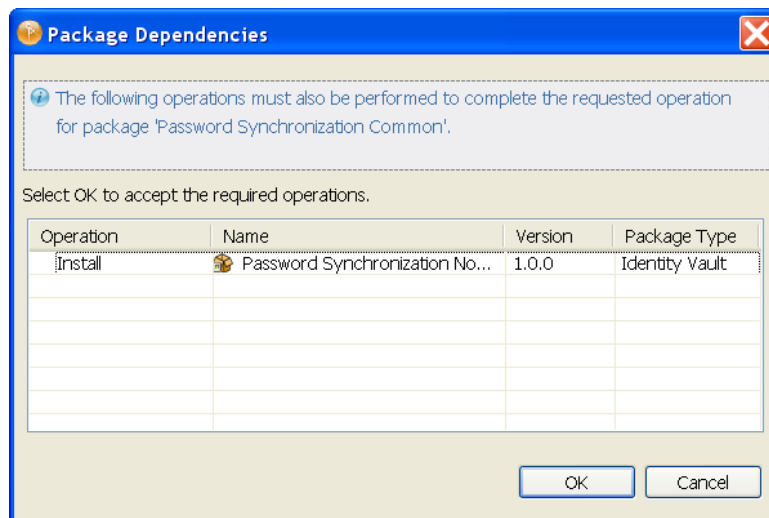
Password Synchronization: These packages contain the policies required to enable password synchronization. Leave this option selected if you want to synchronize passwords to the SAP system.

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](#).

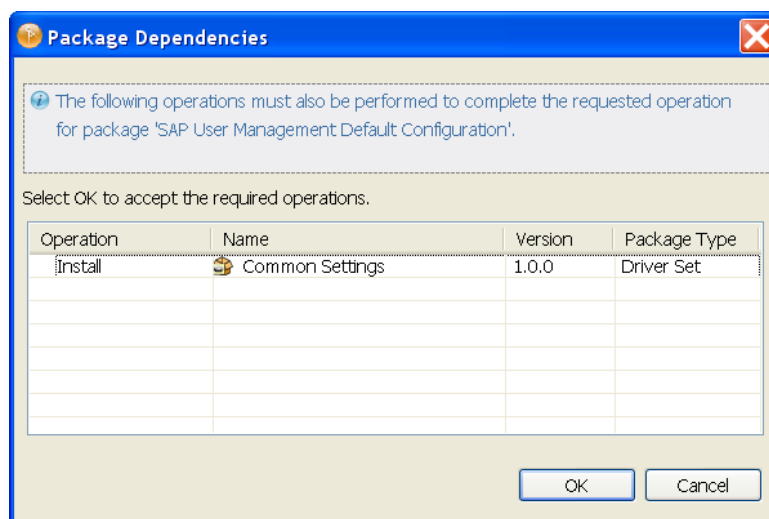
Account Tracking: This group of packages contain the policies that enables account tracking information for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the [Identity Reporting Module Guide](#).

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 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.
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 uses 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 is 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 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 Data 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
- ♦ Other

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
- ♦ Other

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*.
- 23 Continue with [Section 5.2.3, “Configuring the Driver,” on page 40](#).

5.2.3 Configuring the Driver


After importing the driver configuration file, you need to configure the driver before it can run. Complete the following tasks to configure the driver:

- ♦ **Ensure that the driver can authenticate to the SAP UM system:** Make sure that you have established an SAP User administrative account for the driver (see [Section 5.1, “Creating an SAP User Account,” on page 35](#)) and that the correct authentication information, including the User ID and password, is defined for the driver parameters (see [Section A.1.3, “Authentication,” on page 72](#)).
- ♦ **Configure the driver parameters:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to configure the driver parameters located on the Driver Configuration page. For information about the driver parameters, see [Section A.1.5, “Driver Parameters,” on page 73](#).
- ♦ **Customize the driver policies and filter:** Modify the driver policies and filter to implement your business policies. For instructions, see [Chapter 7, “Customizing the Driver,” on page 45](#).
- ♦ **Configure the driver for use in a Central User Administration Environment:** If you want to integrate the driver into a Central User Administration (CUA) environment, see [Chapter 8, “Using the Driver in a Central User Administration Environment,” on page 59](#).

Continue with the next section, [Deploying the Driver](#).

5.2.4 Deploying the Driver

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

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select *Live > Deploy*.
- 3 If you are authenticated to the Identity Vault, skip to [Step 5](#), otherwise, specify the following information:
 - Host:** Specify the IP address or DNS name of the server hosting the Identity Vault.
 - Username:** Specify the DN of the user object used to authenticate to the Identity Vault.
 - Password:** Specify the user’s password.
- 4 Click *OK*.
- 5 Read the deployment summary, then click *Deploy*.

6 Read the message, then click *OK*.

7 Click *Define Security Equivalence* to assign rights to the driver.

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

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

7b Click *OK* twice.

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

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

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

8b Click *OK*.

8c Repeat [Step 8a](#) and [Step 8b](#) for each object you want to exclude.

8d Click *OK*.

9 Click *OK*.

5.2.5 Starting the Driver

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

To start the driver:

1 In Designer, open your project.

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

3 Continue with [Section 5.4, "Activating the Driver,"](#) on page 41.

5.3 Creating the Driver in iManager

Drivers are created with packages, and iManager does not support packages. In order to create or modify drivers, you must use Designer. See [Section 5.2, "Creating the Driver in Designer,"](#) on page 35.

5.4 Activating the Driver

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

If you create the driver in a driver set where you have already activated a driver that comes with the Integration Module for Enterprise, the SAP User driver inherits the activation. If you created the SAP User 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 stops working.

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

- ♦ Driver for SAP Business Logic
- ♦ Driver for SAP Portal
- ♦ Driver for SAP HR
- ♦ Driver for PeopleSoft
- ♦ Driver for SAP User Management

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

Upgrading an Existing Driver

6

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

- ♦ [Section 6.1, “Supported Upgrade Paths,” on page 43](#)
- ♦ [Section 6.2, “What’s New in Version 4.0,” on page 43](#)
- ♦ [Section 6.3, “Upgrade Procedure,” on page 43](#)

6.1 Supported Upgrade Paths

You can upgrade from any 3.x version of the SAP User driver. Upgrading a pre-3.x version of the driver directly to version 4.0 is not supported.

6.2 What’s New in Version 4.0

- ♦ The SAP User driver content is delivered in packages instead of through a driver configuration file.
- ♦ The SAP User driver uses SAP JCO3 APIs.

The SAP JCO2 APIs were used in the previous versions.

6.3 Upgrade Procedure

The process for upgrading the SAP User driver is the same as for other Identity Manager drivers. For detailed instructions, see “[Upgrading Drivers to Packages](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

Customizing the Driver

7

The policies and filter included in the driver packages provide bidirectional creation, deletion, and modification of User information between the Identity Vault and the SAP system. The driver is configured to synchronize more information from the Identity Vault to SAP (Subscriber channel) than from SAP to the Identity Vault (Publisher channel).

The following sections explain how the default driver packages use policies and the filter. You can use this overview as a basis to create your own policies and filters for specific business implementations.

- ♦ [Section 7.1, “Modifying the Policies and the Filter,” on page 45](#)
- ♦ [Section 7.2, “Adding the Organizational Role Class,” on page 53](#)
- ♦ [Section 7.3, “Obtaining Company Address Data for User Objects,” on page 56](#)

7.1 Modifying the Policies and the Filter

You must modify the policies and the filter to work with your specific business environment. We recommend that you make modifications in this order:

1. Modify the Filter (publish and subscribe options) to include additional attributes you want synchronized.
2. Modify the Schema Mapping policy to include all attributes specified in the Subscriber and Publisher channel filters.
3. Modify the Input Transform policy
4. Modify the Output Transform policy
5. Modify the Publisher policies
6. Modify the Subscriber policies

Refer to the following sections for information:

- ♦ [Section 7.1.1, “Filter Publish Options,” on page 46](#)
- ♦ [Section 7.1.2, “Filter Subscribe Options,” on page 46](#)
- ♦ [Section 7.1.3, “Schema Mapping Policy,” on page 47](#)
- ♦ [Section 7.1.4, “Input Transform Policy,” on page 50](#)
- ♦ [Section 7.1.5, “Output Transform Policy,” on page 51](#)
- ♦ [Section 7.1.6, “Publisher Placement Policy,” on page 51](#)
- ♦ [Section 7.1.7, “Publisher Matching Policy,” on page 51](#)
- ♦ [Section 7.1.8, “Publisher Create Policy,” on page 51](#)
- ♦ [Section 7.1.9, “Subscriber Matching Policy,” on page 52](#)
- ♦ [Section 7.1.10, “Subscriber Create Policy,” on page 52](#)

7.1.1 Filter Publish Options

Setting attributes in the filter to *publish* specifies which classes and attributes are published from the SAP system to the Identity Vault.

The default driver configuration publishes the following User class attributes in the filter.

Class	Attributes
User	DirXML-sapLocRoles
	DirXML-sapLocProfiles
	Given Name
	Surname
	sapProfiles
	sapRoles
	sapUsername

7.1.2 Filter Subscribe Options

Setting attributes in the filter to *subscribe* specifies which classes and attributes are synchronized from the Identity Vault to the SAP system.

The default driver configuration subscribes to the following User class attributes in the filter:

Class	Attributes
User	buildingName costCenter firstPrefix floor Full Name Given Name Initials Internet Email Address Login Disabled OU pager sapGroups sapProfiles sapRoles Surname Telephone Number Title

7.1.3 Schema Mapping Policy

The Schema Mapping policy is referenced by the driver object and applies to both the Subscriber and Publisher channel. The purpose of the Schema Mapping policy is to map schema names (particularly attribute names and class names) between the Identity Vault and the SAP User database. Any modification or removal of existing entries in the Schema Mapping policy could destroy the default configuration and policies processing behavior. Adding new attribute mappings is discretionary.

NOTE: The Application Schema definition in the default driver configuration is from a SAP R/3 version 4.7 system with Web Application Server version 6.40. If the target SAP system is a different version, the actual User object schema might be different. Refresh the application schema by using the iManager Schema Mapping editor to obtain the actual schema of the target server.

The following class mapping is included with the default driver configuration:

Identity Vault Class	SAP Class	SAP Description
User	US	USER

The User class is configured to synchronize bidirectionally between SAP and the Identity Vault. A change made in one system will transfer to the other system.

All attributes in the Publisher and Subscriber filters should be mapped unless they are used only for policy processing.

SAP User field values can be arranged in three types:

- ♦ **Simple fields:** These values are not grouped with other fields. The syntax in the schema map is `<field name>`.
- ♦ **Structure fields:** These values are grouped with other pieces of data that describe a larger collection of single-instance data. The syntax for these fields in the schema map is `<structure name>:<field name>`. For example, ADDRESS:TELEPHONE.
- ♦ **Table fields:** These values are similar to Structure fields, but there can be multiple instances of the structured data. The syntax for these fields in the schema map is `<table name>:<field name>`. For example, ADDTEL:TELEPHONE.

The following table includes common attribute mappings for the User class and their descriptions, assuming that only the primary piece of structure communication data is required (such as ADDTEL:TELEPHONE). If fields of a table are to be mapped, you should specify only the Table name in the mapping (such as LOCACTIVITYGROUPS). If you do this, the driver generates all table field values in structured format. For more information, see [Appendix F, “Structured Format Example,” on page 97](#). On the Publisher channel, the structured data must be transformed to string format.

The default mappings for the driver are as follows:

Identity Vault Attribute	SAP User Field Description	SAP User Field(s)
DirXML-sapLocRoles	Role for specified CUA logical system	LOCACTIVITYGROUPS:SUBSYSTEM LOCACTIVITYGROUPS:AGR_NAME
DirXML-sapLocProfiles	Profile for specified CUA logical system	LOCPROFILES:SUBSYSTEM LOCPROFILES:PROFILE
DirXML-sapVClass	License type classification	UCLASS:LIC_TYPE
DirXML-sapLocVClass	License type classification for specified CUA logical system	UCLASSSYS:RCVSYSTEM UCLASSSYS:LIC_TYPE
birthName	Name of person at birth	ADDRESS:BIRTH_NAME
buildingName	Building (number or code)	ADDRESS:BUILDING_P
commType	Communication type (key) (Central address management)	ADDRESS:COMM_TYPE
company	Company address, cross-system key	COMPANY:COMPANY
costCenter	Cost center	DEFAULTS:KOSTL
Facsimile Telephone Number	Fax number: dialing code+number	ADDFAQ:FAX
firstPrefix	Name prefix	ADDRESS:PREFIX1

Identity Vault Attribute	SAP User Field Description	SAP User Field(s)
floor	Floor in building	ADDRESS:FLOOR_P
Full Name	Complete personal name	ADDRESS:FULLNAME
Given Name	First name	ADDRESS:FIRSTNAME
inHouseMail	Int. mail postal code	ADDRESS:INHOUSE_ML
Initials	Middle Initial or personal initials	ADDRESS:INITIALS
InitialsSig	Short name for correspondence	ADDRESS:INITS_SIG
Internet EMail Address	Internet mail (SMTP) address	ADDSMPT:E_MAIL
Login Disabled	Lock User account	LOCKUSER
		The LOCKUSER attribute does not actually exist in SAP. This pseudo-attribute is used by the driver to determine when to call USER_LOCK and USER_UNLOCK BAPI functions.
middleName	Middle name or second forename of a person	ADDRESS:MIDDLENAME
nickname	Nickname or name used	ADDRESS:NICKNAME
OU	Department	ADDRESS:DEPARTMENT
pager	Pager number	ADDPAG:PAGER
personalTitle	Title text	ADDRESS:TITLE_P
roomNumber	Room or apartment number	ADDRESS:ROOM_NO_P
sapAlias	Internet user alias	ALIAS:USERALIAS
sapCATT	CATT: Test status	DEFAULTS:CATTKENNZ
sapClass	User group in user master maintenance	LOGONDATA:CLASS
sapDateFormat	Date format	DEFAULTS:DATFM
sapDecimalFormat	Decimal Notation	DEFAULTS:DCPFM
sapGroups	User group in user master maintenance	GROUPS:USERGROUP
sapLoginLanguage	Language	DEFAULTS:LANGU
sapParameters	Get/Set parameter ID and parameter values	PARAMETER:PAR10
sapPrintParam1	Print parameter 1	DEFAULTS:SPLG
sapPrintParam2	Print parameter 2	DEFAULTS:SPDB
sapPrintParam3	Print parameter 3	DEFAULTS:SPDA
sapProfiles	Profile name	PROFILES:BAPIPROF
sapRefUser	User name in user master record	REF_USER:REF_USER

Identity Vault Attribute	SAP User Field Description	SAP User Field(s)
sapRoles	Role Name	ACTIVITYGROUPS:AGR_NAME
sapSncGuiFlag	Unsecure communication permitted flag	SNC:GUIFLAG
sapSncName	Secure network communication printable name	SNC:PNAME
sapSpool	Spool: Output device	DEFAULTS:SPLD
sapStartMenu	Start Menu	DEFAULTS:START_MENU
sapTimeZone	Time zone	LOGONDATA:TZONE
sapUsername	User Name	USERNAME:BAPIBNAME
sapUserType	User Type	LOGONDATA:USTYP
sapValidFrom	User valid from	LOGONDATA:GLTGV
sapValidTo	User valid to	LOGONDATA:GLTGB
secondName	Second surname of a person	LOGONDATA: SECONDNAME
secondPrefix	Name prefix	ADDRESS:PREFIX2
Surname	Last name	ADDRESS:LASTNAME
Telephone Number	Telephone no.: dialing code+number	ADDTEL:TELEPHONE
telexNumber	Telex Number	ADDTLX:TELEX_NO
Title	Function	ADDRESS:FUNCTION
titleAcademic1	Academic title: written form	ADDRESS:TITLE_ACA1
titleAcademic2	Academic title: written form	ADDRESS:TITLE_ACA2

7.1.4 Input Transform Policy

You modify the Input Transform policy to implement your specific business rules. The Input Transform policy is applied to affect a transformation of the data received from the driver shim.

The policy is applied as the first step of processing an XML document received from the driver shim. The Input Transform policy converts the syntax of the SAP attributes into the syntax for the Identity Vault.

The default driver configuration includes two rules that perform the following functions:

- ♦ Transforming LOACTIVITYGROUPS from structured format to string format.
- ♦ Transforming LOCPROFILES from structured format to string format.

7.1.5 Output Transform Policy

You modify the Output Transform policy to implement your specific business rules. The Output Transform policy is referenced by the driver object and applies to both the Subscriber channel and to the Publisher channel. The purpose of the Output Transformation policy is to perform any final transformation necessary on XML documents sent to the driver by Identity Manager.

The default driver configuration:

- ♦ Transforms LOCACTIVITYGROUPS from string format to structured format.
- ♦ Transforms LOCPROFILES from string format to structured format.
- ♦ Adds the driver's LOCACTIVITYGROUPS attribute to Modify events with the from-merge attribute set.
- ♦ Transforms the pseudo-attribute LOCKUSER value from a true/false format to a 1/0 format.
- ♦ Transforms ADDFAX:FAX values from structured format to string format.
- ♦ Adds USERNAME:BAPIBNAME to the Queries style sheet (invokes the driver's wildcard search functionality; see [Appendix H, "Using Wildcard Search Capabilities,"](#) on page 101.)

7.1.6 Publisher Placement Policy

The Publisher Placement policy is applied to an Add Object event document to determine the placement of the new object in the hierarchical structure of the Identity Vault.

The Placement policy places all User objects in an Identity Vault container that you specify during installation. You can also modify this location by using the Publisher User Placement Global Configuration Variable (GCV.)

The default driver configuration:

- ♦ Appends <remove-association> to Delete events; it's used in conjunction with the Publisher Command Transformation policy.

7.1.7 Publisher Matching Policy

The Publisher Matching policy is applied to a Modify Object event document. Matching policies establish links between an existing entry in the Identity Vault and an existing entry in the SAP system. The Matching policy attempts to find an existing object that matches the object generating the event by the criteria specified in the policy.

The default driver checks for matches based on the sapUsername attribute. A fallback policy is also provided that checks for matches on the Given Name and Surname attributes.

7.1.8 Publisher Create Policy

The Publisher Create policy is applied when a new object is to be added to the Identity Vault. The default driver configuration:

- ♦ Creates a User object (Surname and Given Name attributes are required)

- ♦ Generates a unique CN based on Given Name and Surname attributes
- ♦ Sets the initial account password on creation. Allows an administrator or user to reset or change passwords.

7.1.9 Subscriber Matching Policy

The Subscriber Matching policy is applied to a Modify Object event document. Matching policies establish links between an existing entry in the Identity Vault and an existing entry in the SAP system. The Matching policy attempts to find an existing object that matches the object generating the event by the criteria specified in the policy.

The default driver checks for matches based on the values of the Given Name, Surname, and sapUsername attributes.

If you do not have an association in your query, the SAP system performs a full table scan of the user table. This might cause a long delay in receiving a reply from the matching query.

If the specified user name is known in SAP, adding an association value reduces the query to a single object. You can use the following Output Transformation policy to add the association.

```
<rule>
<description>Add association value to matching queries</description>
<conditions>
<and>
<if-operation op="equal">query</if-operation>
<if-xpath op="not-true">association</if-xpath>
<if-xpath
op="true">search-attr[@attr-name="USERNAME:BAPIBNAME"]/value</if-xpath>
</and>
</conditions>
<actions>
<do-append-xml-element expression="." name="association"/>
<do-append-xml-text expression="association">
<arg-string>
<token-text xml:space="preserve">USD</token-text>
<token-upper-case>
<token-xpath
expression='search-attr[@attr-name="USERNAME:BAPIBNAME"]/value/text()' />
</token-upper-case>
</arg-string>
</do-append-xml-text>
</actions>
</rule>
```

7.1.10 Subscriber Create Policy

The Subscriber Create policy is applied when you want to add a new object to the Identity Vault. The default driver configuration:

- ♦ Ensures that the Surname and Given Name attributes are present.
- ♦ Generates an unique CN based on the Given name and Surname attributes.
- ♦ Appends the sapUserType attribute with a value of A.
- ♦ Sets the initial password (the driver can also set and manage persistent passwords in the SAP system.)

- ♦ Sets a default sapRoles value of SAP_ESSUSER.
- ♦ Sets a default sapProfiles value of SAP_NEW.
- ♦ Adds the following sample DirXML-sapLocRole values: DRVCLNT100:, ADMCLNT100:SAP_EMPLOYEE, and ADMCLNT500:SAP_ESSUSER.
- ♦ Adds the following sample DirXML-sapLocProfiles values: DRVCLNT100:, ADMCLNT100:SAP_ALL, and ADMCLNT500:SAP_NEW.

7.2 Adding the Organizational Role Class

The SAP User driver can be queried for ACTIVITYGROUP objects and all other PDOBJECTS in the SAP User database so that they can be synchronized into the Identity Vault, and used by the administrator through a browse interface. To do this, the default class mapping must be manually changed to the following:

Identity Vault Class	SAP User Field Description	SAP User Field(s)
Organizational Role	PDOBJECT	Organizational Role

The following sections explain what you need to do to allow support for querying the Organizational Role class:

- ♦ [Section 7.2.1, “Editing the Global Configuration Values,” on page 53](#)
- ♦ [Section 7.2.2, “Adding a New Placement Rule,” on page 54](#)
- ♦ [Section 7.2.3, “Modifying the XSLT,” on page 55](#)
- ♦ [Section 7.2.4, “Adding the Organizational Role Class to the Driver Filter,” on page 55](#)
- ♦ [Section 7.2.5, “Migrating Data into the Identity Vault,” on page 56](#)

7.2.1 Editing the Global Configuration Values

To edit the Global Configuration Values (GCV), follow these steps:

- 1 In iManager, browse to the driver, then click the upper right corner of the driver icon.
- 2 Select the *Edit Properties* link.

The Driver Configuration window is displayed.

- 3 Click the *Global Config Values* tab.

A list of the existing GCV values is displayed.

- 4 Click the *Edit XML* tab to open the XML Editor window.

- 5 Select the *Enable XML Editing* check box and add the following XML code:

```
<definition display-name="Organizational Role Placement"
dn-space="dirxml" dn-type="slash" name="sap-pdobject-placement" type="dn">
  <description>
    The name of the Organizational Role object under which
    published SAP Organizational Roles will be placed.
  </description>
  <value> </value>
</definition>
```

- 6 Click *Apply* and *OK* to save the changes.

The updated GCV is now displayed in the list.

- 7 Browse and select the container in the Identity Vault where you want to place the Organizational Role.
- 8 Click *Apply and OK*.

7.2.2 Adding a New Placement Rule

A new rule is required in the placement policy, to place the Organizational Role object in. Follow these steps to create the new rule:

- 1 In iManager, click on the driver icon.

The Identity Manager Overview screen is displayed.

- 2 In the Publisher channel, click on the Placement Policies icon.

The Publisher Placement policy window is displayed.

- 3 Click the existing default Publisher Placement policy.

The Policy Rules screen is displayed.

- 4 Click the *Edit XML* tab.

The XML Editor window is displayed.

- 5 Select the *Enable XML Editing* check box and add the following XML code:

```
<rule>
  <description>Organizational Role Placement</description>
  <conditions>
    <or>
      <if-class-name op="equal">
        Organizational Role
      </if-class-name>
    </or>
    <or>
      <if-op-attr name="CN" op="available"/>
    </or>
  </conditions>
  <actions>
    <do-set-op-dest-dn>
      <arg-dn>
        <token-global-variable name="sap-pdobject-placement"/>
        <token-text xml:space="preserve">\</token-text>
        <token-escape-for-dest-dn>
          <token-op-attr name="CN"/>
        </token-escape-for-dest-dn>
      </arg-dn>
    </do-set-op-dest-dn>
  </actions>
</rule>
```

- 6 Click *Apply* and *OK* to save the changes.

- 7 Click *Close* to close the Publisher Placement Policy window.

7.2.3 Modifying the XSLT

The XSLT file must be modified so that it triggers events only for the USER class.

- 1 On the Identity Manager Driver Overview page, click on the Creation Policies icon on the publisher channel of the driver.
The Publisher Creation Policy window is displayed.
- 2 Click the *Generate User Name Style Sheet* link.
The XML Editor window is displayed.
- 3 Search for the following XML code:

```
<xsl:template match="add">
```


Replace it with the following code:

```
<xsl:template match="add[@class-name='User']">
```
- 4 Click *Apply* and *OK* to save the changes.
- 5 Click *Close* to close the Publisher Placement Policy window.

7.2.4 Adding the Organizational Role Class to the Driver Filter

To add the Organizational Role class, and to change the default class mapping, follow these steps:

- 1 On the Identity Manager Driver Overview page, click the 'Driver Filter' icon in the publisher channel.
- 2 Click the *Add Class* tab.
A pop-up window is displayed.
- 3 Click the *Show All Classes* link.
A list of the available classes is displayed in alphabetical order.
- 4 Scroll down to the class Organizational Role, and click it.
- 5 In the *Application Name* field on the right, browse and select the SAP User class PDOBJECT that will be mapped to Organizational Role.
- 6 Click *Apply* to confirm the mapping.
- 7 In the filter window, select Organizational Role, and click the *Add Attribute* tab.
A list of the available attributes is displayed.
- 8 Select the *CN* attribute and click *OK*.
- 9 In the *Application Name* field on the right, browse and select the SAP attribute *OBJECTS:EXT_OBJ_ID*
- 10 Select Organizational Role again and click the *Add Attribute* tab.
- 11 Select the *Description* attribute and click *OK*.
- 12 In the *Application Name* field on the right, browse and select the *OBJECTS:LONG_TEXT* attribute.
- 13 Click *Apply*.
- 14 In the Filter window, select the Organizational Role class.
- 15 In the text field on the right, delete PDOBJECT and replace it with AG.
- 16 Click *Apply* to save the changes.

- 17 Click *Organizational Role* and select the *Synchronize* option in the Publisher channel.
- 18 Click the *CN* attribute and select the *Synchronize* option in the Publisher channel.
- 19 Click the *Description* attribute and select the *Synchronize* option in the Publisher channel.
- 20 Click *Apply* and *OK* to save the changes, and close the Filter window.

7.2.5 Migrating Data into the Identity Vault

To migrate ACTIVITYGROUP objects into the Identity Vault:

- 1 Ensure that the driver is running.
- 2 From the Identity Manager Driver Overview window, click *Migrate > Migrate into Identity Vault*.
The Migrate Data into the Identity Vault window is displayed.
- 3 To migrate a single ACTIVITYGROUP object:
 - 3a Click the *Edit List* tab.
The Edit Migration Criteria dialog box is displayed.
 - 3b Select the *Organizational Role* class from the list on the left side of the window.
 - 3c Select the *CN* attribute and click *OK*.
The Attribute Value dialog box is displayed.
 - 3d Enter a valid value for the *CN* attribute and click *OK*.
Example of a valid attribute: `SAP_ESSUSER`
 - 3e Click *OK* to confirm the entered value and close the dialog box.
 - 3f Click *OK* again in the Migrate Data into the Identity Vault window to start the migration.
The *Success* box is now selected, indicating that migration has started.
- 4 To migrate all ACTIVITYGROUP objects, follow these steps:
 - 4a Click the *Edit List* tab.
The Edit Migration Criteria dialog box is displayed.
 - 4b Select the *Organizational Role* class from the list, then click *OK*.
 - 4c To start the migration, click *OK* again in the Migrate Data into the Identity Vault window.

To verify that the objects you selected have been migrated successfully, you can browse to the container that you specified in the *Organizational Role* placement policy. Successful migration can also be verified by looking at the *DSTRACE* window.

7.3 Obtaining Company Address Data for User Objects

There are several attributes of the SAP User object that are associated with the Company Address object assigned to the User. These attributes, by default, are never populated in BAPI or IDoc distributions of User data from the SAP application server. These fields also cannot be read from the User object in SAP. Company Address data is maintained in a table of related records of the ADDRESSORG type. The driver can retrieve this data from the ADDRESSORG table if desired.

The driver parameter to publish Company Address data `<nsap-use-addressorg>` is set to 1 by default. Setting the value to 1 retrieves the data from the ADDRESSORG table if attributes in the table exist in the Publisher filter, or if the attributes are in `<read-attr>` elements of a query document. Although this data can be retrieved from the SAP system, ADDRESSORG data cannot be added, modified, or removed from the SAP system via the driver. If the value of this parameter is set to 0, the company address fields are retrieved from the User object itself. By default, these fields don't contain any data.

To fully implement the address retrieval functionality, you must configure the driver to receive events when the ADDRESSORG table is modified. By receiving these events, the driver obtains a list of all User objects assigned to the modified ADDRESSORG table and issues Modify events with the changed data for each affected user.

To generate ADDRESSORG Modify events, you need to modify the ALE distribution model on the SAP application server to include the distribution of the Company Clone (CCLONE) BAPI. Refer to [“Creating a Distribution Model” on page 22](#) and [“Modifying the Port Definition” on page 25](#) for more information.

The following User object fields might be affected by this functionality:

NAME	HOUSE_NO2
NAME_2	STR_SUPPL1
NAME_3	STR_SUPPL2
NAME_4	STR_SUPPL3
C_O_NAME	BUILDING
CITY	DISTRICT
CITY_NO	FLOOR
DISTRICT	ROOM_NO
DISTRICT_NO	COUNTRY
POSTL_COD1	COUNTRYIOS
POSTL_COD2	LOCATION
POSTL_COD3	LANGU_ISO
PO_BOX	REGION
PO_BOX_CIT	SORT1
PBOXCIT_NO	TIME_ZONE
DELIV_DIS	TAXJURCODE
TRANSPZONE	STR_ABBR
STREET	HOUSE_NO
STREET_NO	

Using the Driver in a Central User Administration Environment

8

The following sections provide information about integrating the driver into a Central User Administration (CUA) environment. It is not intended to be a CUA configuration or administration guide. Refer to the SAP documentation and SAP help, support, and tips Web sites and journals for authoritative sources of standard CUA information.

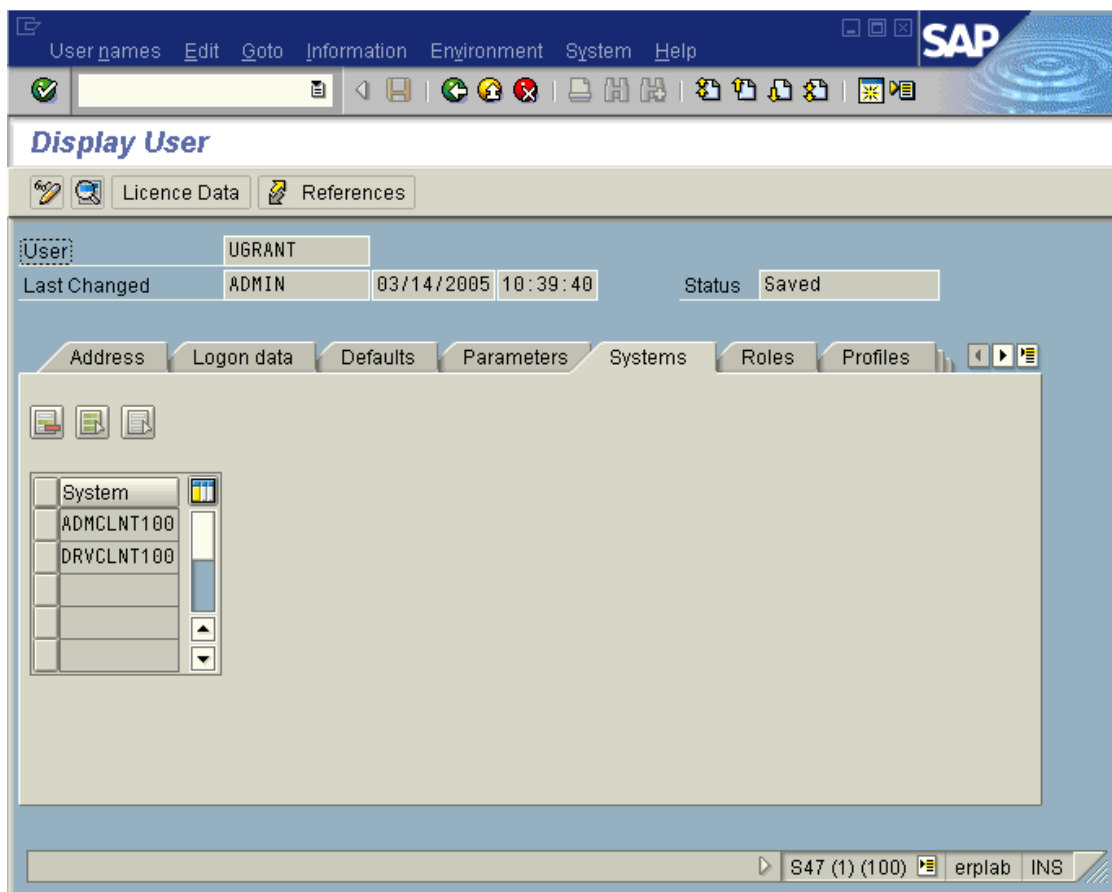
- ♦ [Section 8.1, “Overview,” on page 59](#)
- ♦ [Section 8.2, “Configuring the Driver as a CUA Child System,” on page 61](#)
- ♦ [Section 8.3, “Using the Driver to Provision a CUA Landscape,” on page 63](#)
- ♦ [Section 8.4, “User Classification Settings \(Licensing\),” on page 64](#)
- ♦ [Section 8.5, “Important CUA Integration Notes,” on page 65](#)

8.1 Overview

The driver is designed to perform User management and synchronization with any SAP Application Server. However, the most value can be derived from the driver when it is used in a CUA environment. CUA is the standard User data distribution technology provided by SAP. It is used to distribute data between logical systems on one or more application servers. In a typical CUA landscape, there is one logical system designated as the “Central” system. The Central system administrator has the capability to distribute User account information and access rights to the other Child logical systems in the landscape. There are many variations, however, of the flow of User account information, including configurations where the Child systems can locally administrate some of the User account information and distribute it back to the Central system. The information in this section focuses primarily on using the driver in a basic CUA landscape where User account information is distributed one-way from the Central system to the Child logical systems.

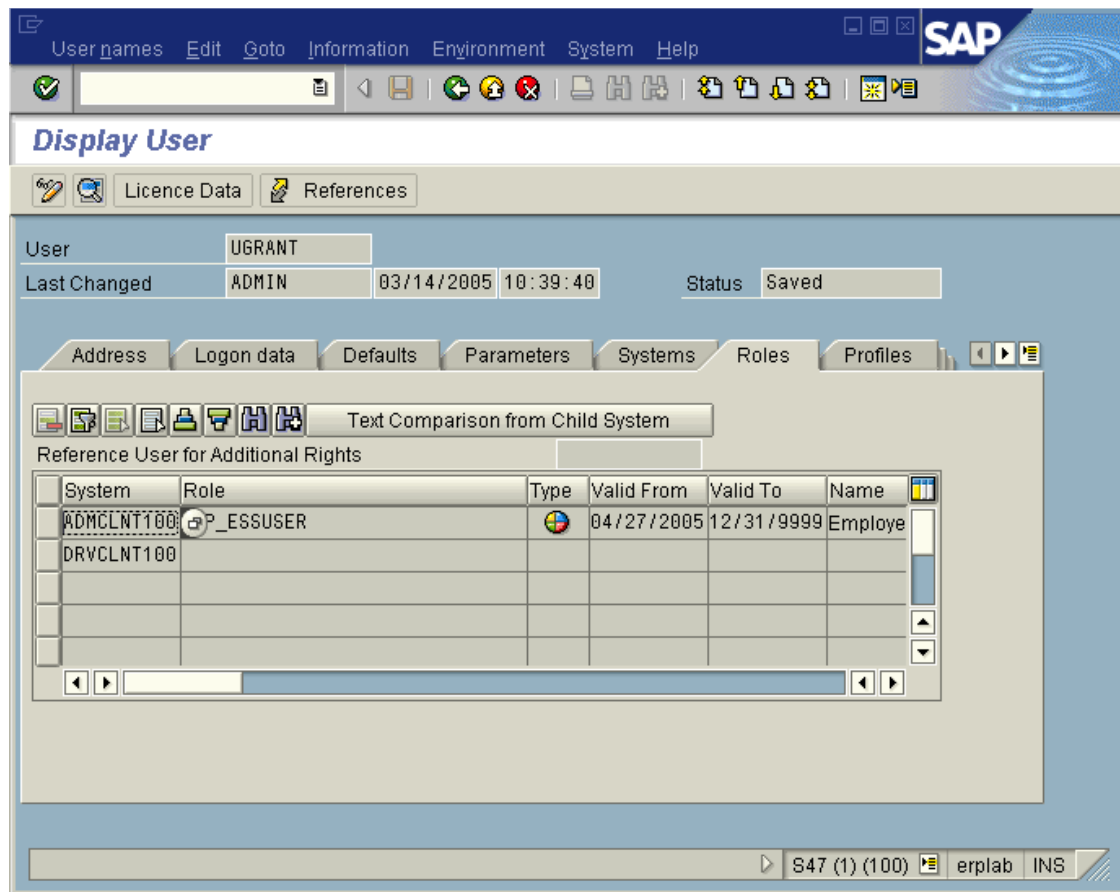
The User Maintenance transaction in SAP is SU01. The major difference between the maintenance options in a CUA environment and a non-CUA environment is the existence of the *Systems* tab. The entries under this tab indicate which logical systems to which the User account information should be distributed. The following illustration shows a User that is distributed to logical systems ADMCLNT100 and DRVCLNT100.

Figure 8-1 User Distribution to Logical Systems ADMCLNT100 and DRVCLNT100



Another difference can be seen when the Central system has been configured to maintain Role and Profile information on a Global level, which means the Central system administrator can set Role and Profile values for all logical systems in the CUA landscape. When the Global level is selected (via transaction SCUM), the Roles and Profiles for a User account are displayed with the logical system to which they are assigned. The following illustration shows a User assigned the default SAP Employee Self-Service role on logical system ADMCLNT100.

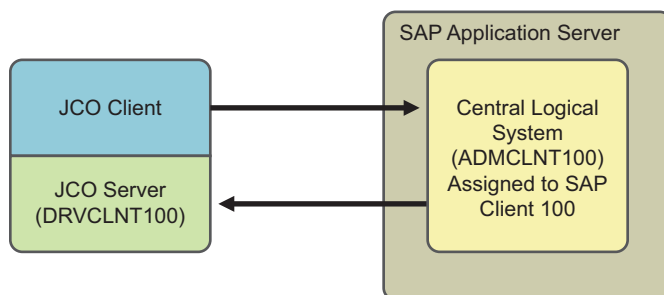
Figure 8-2 A User with the default SAP Employee Self-Service Role on Logical System ADMCLNT100



8.2 Configuring the Driver as a CUA Child System

The driver's Publisher channel functionality requires that the driver be configured as a Child logical system in a CUA environment. The configuration documentation describes a configuration as illustrated below.

Figure 8-3 CUA Child System Configuration



In this configuration, the driver acts as an administrative client to perform User administration, such as User account creation, password set, and role administration, in the CUA Central logical system ADMCLNT100. The Central system is configured to distribute the User account information to the

CUA Child logical system DRVCLNT100 that represents the driver. As seen in the diagram, the driver acts as both a SAP Client and a Server to obtain full bidirectional synchronization functionality.

After the systems are configured for synchronization, you must set the data attributes that trigger synchronization. In order to synchronize a User object, you must create a User in SAP Client 100, allow the user to log in, and establish synchronization back to the driver.

- ♦ Surname and Password are required attributes for User creation
- ♦ Set ADMCLNT100 in the *Systems* tab to allow new User to login to Client 100.
- ♦ Set DRVCLNT100 in the *Systems* tab to establish data distribution back to the driver.

Setting attributes and passwords has been part of the driver functionality since its creation. As of version 1.0.5, you can now set the *Systems* tab on the Central system by using BAPIs for setting Local ActivityGroups (Roles) and Local Profiles. These BAPIs allow the driver to set specified Roles and Profiles on specified logical systems in the CUA landscape. Because there are two component parameters required for each Local Role and Local Profile, the default configuration use a colon-delimited string syntax for the Identity Vault values. The form for these values is <Logical System Name>:<Role or Profile Name>. These values are transformed to and from the SAP structured syntax by the default Input Transform and Output Transform policies.

If you want to set the *Systems* tab for a logical system without setting a Local Role or Local Profile (this should always be done for the driver where SAP Roles and Profiles have no meaning), the string value should be set without the *Role or Profile Name* component.

A new field named FORCE_SYSTEM_ASSIGNMENT is available in newer versions of SAP in the BAPI_USER_CREATE1 function. The driver tries to use this for the *Systems* tab assignment on the Connected SAP System.

The following example shows a Create style sheet template for the setting of only the *Systems* tab for logical systems ADMCLNT100 and DRVCLNT100. Note that the attr-name used is DirXML-sapLocRoles. For this purpose, the DirXML-sapLocProfiles attribute could also be used. (In Identity Manager 3, this policy is implemented through the Policy Builder.)

```
<xsl:template name="add-systems-tab">
  <!--
    Sample CUA distribution settings.
    - Central SAP system is ADMCLNT100
    - Driver's logical system is DRVCLNT100
  -->

  <add-attr attr-name="DirXML-sapLocRoles">
    <!--
      In a CUA environment, set driver's LS name with a blank role.
      This allows
      the driver to receive events from SAP.
    -->
    <value>
      <xsl:value-of select="' DRVCLNT100:'"/>
    </value>
  <!--
    Setting the target LS name with a blank CUA role allows the
```

```

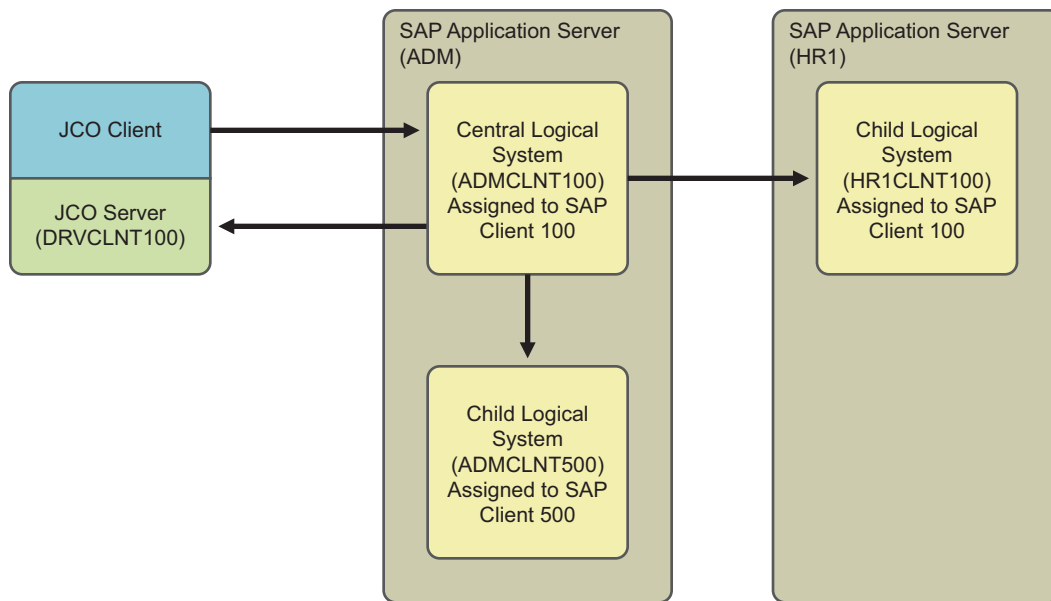
User object to log on to the target child system but receive no rights
-->
<value>
  <xsl:value-of select="'ADMCLNT100:'" />
</value>
</add-attr>
</xsl:template>

```

8.3 Using the Driver to Provision a CUA Landscape

The previous example showed a simple CUA environment where the Central system distributed User data only to the driver's logical system. This is not a typical environment. In most CUA environments, a Central system distributes data to SAP Child logical systems on multiple application servers. A small example of a typical CUA landscape looks more like this:

Figure 8-4 A Central System Distributing Data to SAP Child Logical Systems on Multiple Application Servers



As in [Figure 8-3 on page 61](#), the driver can set the distribution of User account information to the additional CUA Child systems by setting the *Systems* tab for them. However, the real power of the driver is realized when you use access controls to the various SAP clients based on the driver's policies. For example, all employees can receive employee Self-Service rights on the HR system, but an employee identified as an HR Administrator could also be granted rights to the HR administration functions. The following example shows a Create Style Sheet template for setting the *Systems* tab for logical system ADMCLNT100 and DRVCLNT100, setting the SAP_ESSUSER Role on logical system HR1CLNT100, and setting the SAP_ALL Profile on logical system ADMCLNT500. (In Identity Manager 3, this policy is implemented through the Policy Builder.)

```

<xsl:template name="add-cua-auths">
  <!--
  Sample CUA distribution settings.
  - Central SAP system is ADMCLNT100
  - Child SAP systems are: ADMCLNT500 and HR1CLNT100
  - Driver's logical system is DRVCLNT100
  -->
  <add-attr attr-name="DirXML-sapLocRoles">
    <!--
    In a CUA environment, set driver's LS name with a
    blank role. This allows the driver to receive events
    from SAP.
    -->
    <value>
      <xsl:value-of select="'DRVCLNT100:'"/>
    </value>
    <!--
    Setting the target LS name with a blank CUA role
    allows the User object to log on to the target
    child system but receive no rights.
    -->
    <value>
      <xsl:value-of select="'ADMCLNT100:'"/>
    </value>
    <!--
    The third value shows how to set a 'real' CUA role
    for a child logical system. This causes
    distribution from the Central system to the child
    system and sets the Employee Self-Service role.
    -->
    <value>
      <xsl:value-of
select="'HRCLNT100:SAP_ESSUSER'"/>
    </value>
  </add-attr>
  <!--
  Example of setting a 'real' CUA profile.
  -->
  <add-attr attr-name="DirXML-sapLocProfiles">
    <value>
      <xsl:value-of select="'ADMCLNT500:SAP_ALL'"/>
    </value>
  </add-attr>
</xsl:template>

```

8.4 User Classification Settings (Licensing)

Beginning with version SAP R/3 version 4.7, SAP added the ability to set licensing information on User records. In a CUA environment, this information is set by using table UCLASSSYS. There can be a maximum of 1 license type set for each client system in the CUA landscape. The primary data field for licensing in the LIC_TYPE field. This is a two-character code indicating the type of license utilized by the SAP User. Because the license is a system-dependent value, you must also set the RCVSYSTEM field to a valid logical system name. You can set a license value only for logical systems specified in the *Systems* tab of the User record. It is not necessary or possible to set license

values for the driver's logical system. The following example shows a Create Style Sheet template for setting a sample Employee license value for a User of logical system ADMCLNT100. (In Identity Manager 3, this policy is implemented through the Policy Builder.)

```
<xsl:template name="add-license">
  <!--
    - Sample Setting of User Classification (License) Table UCLASSSYS
    - Central SAP system is ADMCLNT100, License Type = 54
  -->
  <add-attr attr-name="DirXML-sapLocUClass">
    <value>
      <xsl:value-of select="'ADMCLNT100:54'"/>
    </value>
  </add-attr>
</xsl:template>
```

NOTE: The data sent to the driver must be in a structured format. The default Input Transformation and Output Transformation policies handle the required syntax conversions of UCLASSSYS similar to the way they handle LOCFILES and LOCACTIVITYGROUPS.

8.5 Important CUA Integration Notes

- The BAPIs utilized to perform the CUA integration are documented as being available for SAP version 4.0A in the SAP system documentation. Novell has successfully tested this functionality for SAP R/3 version 4.6C and later. This includes all versions of SAP Web Application Server. For 4.6C systems, the BAPIs are not documented by SAP in the system documentation and support might not be available.
- Password distribution to the CUA Central system can be performed for all initial set and reset operations. However, passwords provisioned to CUA Child systems from the Central system can only be initially set. Password change/reset operations cannot be distributed to Child systems. This is a SAP-designed restriction and is not a limitation of the methodology used by the driver. SAP has determined that setting a single password across systems via CUA violates client system administrative authority and security, so they recommend the use of Single Sign-On (SSO) products to perform this task. Refer to SAP's documentation related to Password Change for more explicit information on this restriction.
- User Classification (Licensing) table entries can only be made to systems listed in the *Systems* tab on the User record. If Central Licensing values are to be set while adding Users to the CUA Central System, make sure all targeted client systems are also available by setting a DirXML-sapLocRoles or DirXML-sapLocProfiles value for them in the Add event.

Managing the Driver

9

As you work with the SAP User 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 Common Driver Administration Guide*](#).

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

- ♦ [Section 10.1, “Troubleshooting Driver Processes,” on page 69](#)
- ♦ [Section 10.2, “Driver Errors,” on page 69](#)

10.1 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see [“Viewing Identity Manager Processes”](#) in the *Identity Manager 4.0 Common Driver Administration Guide*.

10.2 Driver Errors

You might see the following driver errors in the DSTrace utility. An explanation of the error is given along with recommended solutions.

10.2.1 JCo 3

- ♦ [“Error Occurs when Uninstalling the Driver” on page 69](#)

Error Occurs when Uninstalling the Driver

If you have installed the SAP User Management (JCo 3) 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 (JCo 3) driver on a server that does not have Identity Manager or the Remote Loader installed on it.

To work around the problem on Linux:

- 1 Export `PATH=<JAVA-HOME-PATH>/bin/:$PATH`.
- 2 Run the Castor Uninstall script where the `JAVA-HOME-PATH` is the JAVA or the JRE install location.

To work around the problem on Windows:

From the command prompt, go to the SAP uninstaller location and run the following command:


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

where the JAVA-HOME-PATH is the JAVA or the JRE install location.

Driver Properties

A


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

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


- ♦ [Section A.1, “Driver Configuration,” on page 71](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 76](#)

A.1 Driver Configuration

In Designer:

- 1 Open a project in the Modeler.
- 2 Right-click the driver icon  or line, then select *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 Sentinel 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 72](#)
- ♦ [Section A.1.2, “Driver Object Password \(iManager Only\),” on page 72](#)
- ♦ [Section A.1.3, “Authentication,” on page 72](#)
- ♦ [Section A.1.4, “Startup Option,” on page 73](#)
- ♦ [Section A.1.5, “Driver Parameters,” on page 73](#)
- ♦ [Section A.1.6, “ECMAScript,” on page 76](#)
- ♦ [Section A.1.7, “Global Configurations,” on page 76](#)

A.1.1 Driver Module

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

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

The name of the Java class is: `com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim`

Native: This option is not used with the SAP User 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 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 Driver Object Password (iManager Only)

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

A.1.3 Authentication

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

Authentication ID: Specify an SAP account that the driver can use to authenticate to the SAP system.

Example: `SAPUser`

Authentication Context: Specify the IP address or name of the SAP server the driver should communicate with.

Remote Loader Connection Parameters: Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, when the hostname is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090.

The `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine.

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

Application Password: Specify the password for the user object listed in the *Authentication ID* field.

Remote Loader Password: Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

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.

A.1.4 Startup Option

The Startup Option allows you to set the driver state when the Identity Manager server is started.

Auto start: The driver starts every time the Identity Manager server is started.

Manual: The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.

Disabled: The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.

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

A.1.5 Driver Parameters

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

The parameters are presented by category:

- ♦ [“Driver Options” on page 73](#)
- ♦ [“Subscriber Options” on page 75](#)
- ♦ [“Publisher Options” on page 75](#)

Driver Options

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 a 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.

Logical System Name: This value must match the Logical System Name for the client as configured in SAP if this SAP client is the central client in the CUA landscape. Otherwise, the value can be chosen freely with the one constraint that must be unique.

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.

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 a list of all of the languages installed on your SAP system. All the languages you specify into this list are made available in external application like the Role Mapping Administrator, so that the application 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. Set it to *Publish All* if all values should be synchronized.

Publish Company Address Data: By default, an SAP User record does not include Company Address information. That data is kept in a related table. Use this parameter to specify if you want the driver to retrieve the data from the appropriate company record. Regardless of the option you specify, Company Address information cannot be updated in SAP.

Set this to *Include Company Address* to populate User Company Address information for the Publisher and Subscriber channel queries. Set it to *Ignore Company Address* if you do not want this functionality.

For additional information, see [Section 7.3, “Obtaining Company Address Data for User Objects,” on page 56](#).

Change retry status to error on subscriber events: When this option is set to *Yes*, the driver shim issues an error instead of a retry on Subscriber operation results. Use this setting with caution. When you run the driver in fan-out mode, it is strongly recommended to turn this feature on; otherwise, leave it off.

Subscriber Options

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 to 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. Select *No Change Required* if you do not want user's to change passwords immediately at login.

- ♦ **Password Set Method:** Select the methodology used by the driver to set the user account passwords. Passwords can be set by the driver's administrative user account or by the affected user's account.
- ♦ **Default Reset Password:** Specify a default password reset value. It is set during the password changes if the user-supplied password is not accepted by the SAP server. There is an 8-character size limit for this value.
- ♦ **Reset Password Delay (seconds):** Specify the number of seconds between setting the Administrative default password and setting the user's new password.
- ♦ **Force Password to Upper Case:** Select an option to determine if passwords are forced to be uppercase. mySAP 2005 and later allow mixed-case passwords.

Support Password Set for Non-Dialog Users: Select if the driver sets passwords for non-Dialog user types (Communication, System, Service, and Reference) via the Subscriber channel.

Use Local Locking: Select *Yes* to lock accounts locally in this 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.

SAP Server Secondary Connection Information: If you are using a fan-out configuration, use this setting to add secondary connection profiles here. For more information, see the [Identity Manager 4.0 Fan-Out Driver for SAP User Management Implementation Guide](#).

Publisher Options

Publisher Channel Enabled: Select whether or not you want to enable the driver's Publisher channel.

Publisher Channel Port Type: Set this to TRFC if the driver will instantiate a JCO Server to receive data distribution broadcasts from the SAP ALE system. Set it to FILE if the driver will consume text file IDocs distributed by the SAP ALE system.

- ♦ **SAP Gateway ID:** Specify the SAP Gateway 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 server TRFC tracing is enabled.

Logical System for User Distribution: Specify the logical system name configured in SAP for user distribution to the Identity Manager driver. Publication works only if the Publisher channel is enabled and the driver's primary connection goes 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: Select one of the options to determine when future-dated data is published by the driver.

Publisher IDoc Directory: Specify the file system location where the SAP User IDoc files are placed by the SAP ALE system (for FILE port) or by the driver (for TRFC port).

Publisher heartbeat interval: Configures the driver shim to send a periodic status message on the Publisher channel when there has been no Publisher traffic for the given number of minutes.

A.1.6 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.1.7 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 driver includes several predefined GCVs. You can also add your own if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in iManager:


- 1 Click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit.
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.

- 3 Locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.


or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver's GCVs in Designer:

- 1 Open a project in the Modeler.
- 2 Right-click the driver icon  or line, then select *Properties > Global Configuration Values*.

or


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

The GCVs are divided into the following categories:

- ♦ [Section A.2.1, “Password Synchronization,” on page 77](#)
- ♦ [Section A.2.2, “Account Tracking,” on page 78](#)
- ♦ [Section A.2.3, “Managed System Information,” on page 79](#)
- ♦ [Section A.2.4, “SAP User Management Driver,” on page 80](#)

A.2.1 Password Synchronization

These GCVs enable password synchronization between the Identity Vault and the Active Directory 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 Password Management Guide*.

Connected System or Driver Name: Specify the name of the Active Directory system or the driver name. This value is used by the e-mail notification template to identify 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 passwords 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.2.2 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 finished 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 that the policies assume when an object is subscribed to the application and the status attribute is not set in the Identity Vault.

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

A.2.3 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 79](#)
- ♦ [“System Owner” on page 79](#)
- ♦ [“System Classification” on page 79](#)
- ♦ [“Fan-out Configuration” on page 80](#)
- ♦ [“Connection and Miscellaneous Information” on page 80](#)

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 this 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
- ♦ Other

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
- ♦ Other

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 option 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.2.4 SAP User Management Driver

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

Application Link Enabling (ALE)

B

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 configuring 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 81](#)
- ♦ [Section B.2, “Message Type,” on page 81](#)
- ♦ [Section B.3, “IDoc Type,” on page 82](#)
- ♦ [Section B.4, “Distribution Model,” on page 82](#)
- ♦ [Section B.5, “Partner Profiles,” on page 82](#)
- ♦ [Section B.6, “Port,” on page 82](#)
- ♦ [Section B.7, “Port Definition,” on page 82](#)
- ♦ [Section B.8, “File Port,” on page 82](#)
- ♦ [Section B.9, “TRFC Port,” on page 83](#)
- ♦ [Section B.10, “CUA,” on page 83](#)

Refer to [“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 usually 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 you set 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.

Business Application Programming Interfaces (BAPIs)



The following table contains a list of the BAPIs used by the driver.

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
SUSR_BAPI_USER_LOCK	<p>Used to set granular locks on an SAP USER object account. The granular lock types available are <code>LOCK_LOCAL</code> and <code>LOCK_GLOBAL</code>.</p> <p>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).</p>
SUSR_BAPI_USER_UNLOCK	<p>Used to clear granular locks on an SAP USER object account. The granular lock types available are <code>LOCK_LOCAL</code>, <code>LOCK_GLOBAL</code>, and <code>LOCK_WRONG_LOGON</code>.</p> <p>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).</p>
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.

Configuration and Deployment Notes

D

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 87](#)
- ♦ [Section D.2, “User Types: LOGONDATA:USTYP,” on page 87](#)
- ♦ [Section D.3, “Output Controller Options,” on page 88](#)
- ♦ [Section D.4, “Communication Types: ADDCOMREM:COMM TYPE,” on page 88](#)
- ♦ [Section D.5, “Date Formats: DEFAULTS:DATAFM,” on page 88](#)
- ♦ [Section D.6, “Decimal Formats: DEFAULTS:DCPFM,” on page 88](#)
- ♦ [Section D.7, “Computer Aided Test \(CATT\): DEFAULTS:CATTKENNZ,” on page 88](#)
- ♦ [Section D.8, “Communication Comment Type to Table Mappings,” on page 89](#)
- ♦ [Section D.9, “Language Codes,” on page 89](#)
- ♦ [Section D.10, “Configuration Parameters,” on page 90](#)
- ♦ [Section D.11, “Design Comments and Notes,” on page 90](#)

D.1 SAP Object Types

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

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

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
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
Croatian	HR	6
Hungarian	HU	H

Language	Two-Letter Code	One-Letter Code
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. Use the USER_SET mode with SAP 4.7 and above.

- ♦ [Section D.11.1, “BAPI_USER_CHANGE \(ADDRESS table\),” on page 91](#)

- ♦ Section D.11.2, “BAPI_USER_CHANGE (ADDFAX table),” on page 91
- ♦ Section D.11.3, “BAPI_USER_CHANGE (ADDTEL table),” on page 91
- ♦ Section D.11.4, “BAPI_USER_CHANGE (ADDTLX table),” on page 91
- ♦ Section D.11.5, “In BAPI_USER_CHANGE (ADDFAX table),” on page 92
- ♦ Section D.11.6, “In BAPI_USER_CHANGE (GROUPS table),” on page 92
- ♦ Section D.11.7, “BAPI_USER_CHANGE (ALIAS structure),” on page 92
- ♦ Section D.11.8, “BAPI_USER_CHANGE (REF_USER structure),” on page 92
- ♦ Section D.11.9, “BAPI_USER_CHANGE (DEFAULTS structure),” on page 92
- ♦ Section D.11.10, “BAPI_USER_CHANGE (LOGONDATA structure),” on page 93
- ♦ Section D.11.11, “BAPI_USER_CHANGE (GROUPS table),” on page 93
- ♦ Section D.11.12, “BAPI_USER_CHANGE (ADDCOMREM table),” on page 93

D.11.1 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.

D.11.2 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.

D.11.3 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.

D.11.4 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 `sapumshim.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.

D.11.5 In BAPI_USER_CHANGE (ADDFAX table)

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

D.11.6 In BAPI_USER_CHANGE (GROUPS table)

- ♦ The USERGROUP is the only field in this table.

D.11.7 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.

D.11.8 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)

D.11.9 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), or 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 at all. 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 89](#) 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.

D.11.10 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 87](#) or a null string (“”). Other input generates an exception and 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 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.”

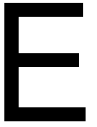
D.11.11 BAPI_USER_CHANGE (GROUPS table)

- 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.”

D.11.12 BAPI_USER_CHANGE (ADDCOMREM table)

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

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 *USdSAPobjectID*. User names 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. [“Schema Mapping Policy” on page 47](#) indicates the structure components to set for these values.

Structured Format Example

F

```
// 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>
```


Setting and Clearing Granular Locks



This 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. This is done via an attribute setting in the SAP Function Builder transaction (SE37) and must be performed by an authorized administrator.

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 is set 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.

G.1 Examples

```
//  
// 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>

```

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. This 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 its 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 alleviate 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 (ie. 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 (ie. JSmith*): Restricts attribute matching to User account names starting with JSMITH.
- ♦ “Ends-with” syntax (ie. *ith): Restricts attribute matching to User account names ending with ITH.
- ♦ “Contains” syntax (ie. *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 the matching ADDRESS:FIRSTNAME value “Joe.”