
NetIQ® Identity Manager

Driver for SAP HR Implementation Guide

February 2017

Legal Notices

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

Copyright (C) 2017 NetIQ Corporation. All rights reserved.

About this Book and the Library	7
About NetIQ Corporation	9
1 Understanding the SAP HR Driver	11
1.1 Supported SAP Versions	11
1.2 Driver Concepts	11
1.2.1 Publisher Channel	12
1.2.2 Subscriber Channel	12
1.3 Benefits	13
1.4 Driver Features.	14
1.5 Product Components	14
1.5.1 Driver Shim	15
1.5.2 SAP Java Connector Test Utility	15
1.6 Publishing to the Identity Vault	15
1.6.1 IDoc Consumption by the Driver	15
1.6.2 IDoc Object Types Consumed by the Driver	16
1.6.3 Attribute Mapping from the SAP HR Database to the Identity Vault	17
1.7 Subscribing from the Identity Vault.	18
1.8 Support for Standard Driver Features	18
1.8.1 Local Platforms	18
1.8.2 Remote Platforms	18
1.8.3 Entitlements	19
2 Upgrading an Existing Driver	21
2.1 Supported Upgrade Paths	21
2.2 What's New?	21
2.2.1 What's New in Version 4.0.1	21
2.2.2 What's New in Version 4.0.0	21
2.3 Upgrading the Driver	21
2.3.1 Upgrading the Installed Packages	22
2.3.2 Applying the Driver Patch	22
3 Installing the Driver Files	25
4 Creating a New Driver Object	27
4.1 Creating a SAP HR Account.	27
4.2 Creating the Driver Object in Designer.	27
4.2.1 Importing the Current Driver Packages	27
4.2.2 Installing the Driver Packages	28
4.2.3 Configuring the Driver Object	31
4.2.4 Deploying the Driver Object.	31
4.2.5 Starting the Driver	32
4.3 Activating the Driver	32
4.4 Adding Packages to an Existing Driver	33
5 Configuring the SAP System	35
5.1 Configuring the SAP System	35
5.1.1 Defining Sending and Receiving Systems.	35
5.1.2 Creating a Distribution Model	37
5.1.3 Creating a Port Definition.	37
5.1.4 Generating Partner Profiles	38
5.1.5 Generating an IDoc	38

5.1.6	Activating Change Pointers	39
5.1.7	Scheduling a Job for Change Pointer Processing	39
5.1.8	Scheduling a Job	39
5.1.9	Testing the Change Pointer Configuration	40
5.1.10	Creating a CPIC User	40
5.2	Using the Schema Metadata File	40
5.2.1	Creating a New Schema Metadata File	41
5.2.2	Reducing the Size of the Schema Metadata File	42
5.2.3	Extending the Schema Metadata File	42
5.3	Using the SAP Java Connector Test Utility	42
5.3.1	What Does the Utility Do?	43
5.3.2	Utility Prerequisites	43
5.3.3	Components	43
5.3.4	Running and Evaluating the Test	44
5.3.5	Understanding Test Error Messages	45
6	Customizing the Driver	47
6.1	Modifying the Policies and the Filter	47
6.1.1	The Driver Filter	48
6.1.2	The Schema Mapping Policy	49
6.1.3	The Input Transformation Policy	50
6.1.4	The Output Transformation Policy	50
6.1.5	The Publisher Placement Policy	51
6.1.6	The Publisher Matching Policy	51
6.1.7	The Publisher Creation Policy	51
6.1.8	The Publisher Command Transformation Policy	51
6.2	Using the Relationship Query	52
6.2.1	Query 1	52
6.2.2	Query 2	52
6.2.3	Query 3	54
6.3	Populating the Identity Vault with Organizational Data	55
7	Managing the Driver	57
8	Troubleshooting the Driver	59
8.1	Using the DSTrace Utility	59
8.2	Driver Load Errors	59
8.2.1	java.lang.ClassNotFoundException:com.novell.nds.dirxml.drivers.SAPshim.SAPDriver Shim59	
8.2.2	Error Occurs when Uninstalling the Driver	59
8.2.3	Error DestinationDataProvider already registered	60
8.3	Driver Initialization Errors	61
8.3.1	com/sap/conn/jco/ext/DestinationDataProvider Exception	61
8.3.2	Could not Initialize class com.sap.conn.jco.rt.JCoRuntimeFactory	61
8.3.3	Common Errors	61
A	Driver Properties	65
A.1	Driver Configuration	65
A.1.1	Driver Module	66
A.1.2	Driver Object Password	66
A.1.3	Authentication	66
A.1.4	Startup Options	67
A.1.5	Driver Parameters	67
A.1.6	ECMAScript	71
A.1.7	Global Configuration	71
A.2	Global Configuration Values	71

A.2.1	Configuration	72
A.2.2	Password Synchronization	73
A.2.3	Managed System Information	74
B	Application Link Enabling (ALE)	77
B.1	Application Link Enabling Technology	77
B.2	Clients and Logical Systems	78
B.3	Message Type	78
B.4	IDoc Type	78
B.5	Distribution Model	78
B.6	Partner Profiles	79
B.7	Port	79
B.8	Port Definition	79
B.9	File Port	79
B.10	Change Pointers	79
B.11	Change Document/IDoc Outbound Processing	79
C	Example XML Document Received from the Driver	81
D	Business Application Programming Interfaces (BAPIs)	83
E	Subscriber Change Modes and Validity Date Modes	85
E.1	Change Mode Notes	85
E.1.1	<remove-all-values>	85
E.1.2	<remove-value> without an Accompanying <add-value>	86
E.1.3	<remove-value> with an Accompanying <add-value>	86
E.1.4	<add-value> without a Prior <remove-value>	86
E.2	Validity Date Modes	87
F	Trace Levels	89

About this Book and the Library

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

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

The library provides the following information resources:

Identity Manager Setup Guide

Provides overview of Identity Manager and its components. This book also provides detailed planning and installation information for Identity Manager.

Designer Administration Guide

Provides information about designing, testing, documenting, and deploying Identity Manager solutions in a highly productive environment.

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

User Application: User Guide

Describes the user interface of the Identity Manager User Application and how you can use the features it offers, including identity self-service, the Work Dashboard, role and resource management, and compliance management.

User Application: Design Guide

Describes how to use the Designer to create User Application components, including how to work with the Provisioning view, the directory abstraction layer editor, the provisioning request definition editor, the provisioning team editor, and the role catalog.

Identity Reporting Module Guide

Describes the Identity Reporting Module for Identity Manager and how you can use the features it offers, including the Reporting Module user interface and custom report definitions, as well as providing installation instructions.

Analyzer Administration Guide

Describes how to administer Analyzer for Identity Manager.

Identity Manager Common Driver Administration Guide

Provides information about administration tasks that are common to all Identity Manager drivers.

Identity Manager Driver Guides

Provides implementation information about Identity Manager drivers.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Understanding the SAP HR Driver

The Identity Manager Driver for SAP Human Resources (HR), subsequently referred to as the SAP HR driver, creates an automated link between the SAP HR database and the Identity Vault. 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 new records are added, modified, or deactivated (disabled) in SAP, network tasks associated with these events can be processed automatically.

Because the SAP HR system is the authoritative source of personnel information, the driver allows administrators to propagate this data to other non-SAP 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.

The following sections explain the concepts you should understand before attempting to implement the SAP HR driver in your environment:

- ◆ [Section 1.1, “Supported SAP Versions,” on page 11](#)
- ◆ [Section 1.2, “Driver Concepts,” on page 11](#)
- ◆ [Section 1.3, “Benefits,” on page 13](#)
- ◆ [Section 1.4, “Driver Features,” on page 14](#)
- ◆ [Section 1.5, “Product Components,” on page 14](#)
- ◆ [Section 1.6, “Publishing to the Identity Vault,” on page 15](#)
- ◆ [Section 1.7, “Subscribing from the Identity Vault,” on page 18](#)
- ◆ [Section 1.8, “Support for Standard Driver Features,” on page 18](#)

1.1 Supported SAP Versions

The driver supports the following SAP versions:

- ◆ SAP R/3 version 4.5B or higher (SAP NetWeaver 7.5 is the latest supported version)
- ◆ mySAP

1.2 Driver Concepts

The driver provides bidirectional synchronization between SAP systems and the Identity Vault. This framework uses XML to provide data and event transformation capabilities that convert Identity Vault data and events into SAP HR data and vice-versa.

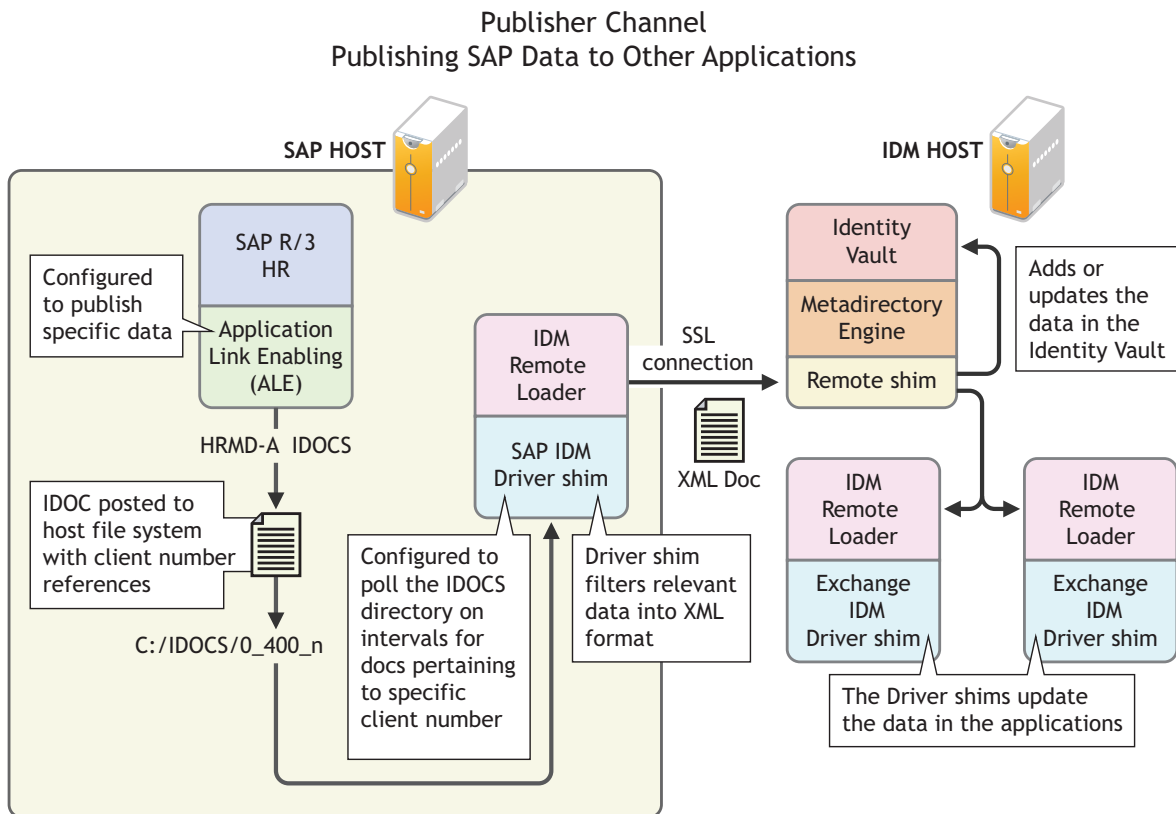
The Identity Vault acts as a hub, with other applications and directories publishing their changes to it. The Identity Vault then sends changes to the applications and directories that have subscribed for them. This results in two main flows of data: the Publisher channel and the Subscriber channel.

- ◆ [Section 1.2.1, “Publisher Channel,” on page 12](#)
- ◆ [Section 1.2.2, “Subscriber Channel,” on page 12](#)

1.2.1 Publisher Channel

The following figure illustrates how the Publisher channel synchronizes data from the SAP HR database to the Identity Vault.

Figure 1-1 Publisher Channel Process



The SAP R/3 HR database publishes information in the form of HRMD_A IDocs by using Application Link Enabling (ALE) technology. The driver is only interested in HRMD_A Message IDocs. Any object type in these IDocs can be mapped to an Identity Vault object type and subsequently synchronized. The driver consumes the IDoc files and converts the data into XML format.

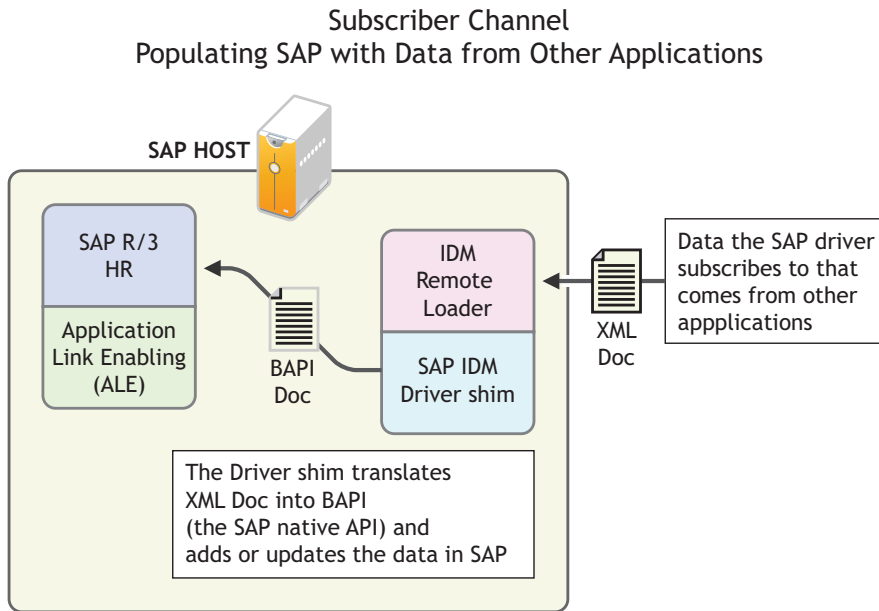
The Publisher channel polls the SAP HR database for changes, and then submits XML-formatted changes to the Metadirectory engine for publication into the Identity Vault. The engine processes the document by sequentially applying all configured policies based on standard driver process flow.

The driver can then manipulate the information using various policies and filters defined by the system administrator. The driver then submits the data to the Identity Vault. Using other Identity Manager drivers, the data can be shared with other business applications and directories. Based on business rules, these other applications can add additional data that can in turn be inserted back into the SAP HR database through Business Application Programming Interface (BAPI) technology.

1.2.2 Subscriber Channel

The following figure illustrates how the Subscriber channel synchronizes data from the Identity Vault to the SAP HR database.

Figure 1-2 Subscriber Channel Process



The Subscriber channel receives XML-formatted Identity Vault events from the Metadirectory engine. The driver then 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 have subscribed to receive them.

1.3 Benefits

As the following examples illustrate, the driver enables you to automate and maintain business processes:

- ♦ Automatically creating an Identity Vault account when an individual is hired.
- ♦ Automatically deleting or deactivate Identity Vault accounts when an employee is terminated.
- ♦ Synchronizing bidirectional data between SAP and the Identity Vault.
- ♦ Maintaining accurate and consistent Identity Vault IDs.
- ♦ Defining password policies (for example, a birth date, social security number, and first and last name combinations).
- ♦ Allowing seamless integration between SAP and multiple applications (for example, eDirectory, Lotus Notes, Netscape, Exchange, and Active Directory) by using Identity Manager and the Identity Vault.
- ♦ Creating other Identity Vault objects associated with a SAP object (for example, account codes or department records).

You can configure SAP and the SAP HR driver to enhance your organization's business processes. Before installing and configuring the driver, you evaluate and define those processes. During installation, you configure the driver's policies to automate these processes wherever possible.

1.4 Driver Features

The driver has various features to help you manipulate data:

- ◆ Publisher Channel event status processing

The Publisher channel treats each object in an IDoc as a unique event. The status of each event determines the appropriate IDoc filename extension. For example, all events with a Warning status are placed in a file with the `.warn` extension.

- ◆ Publisher Channel Only configuration options

The Publisher Channel Only option in the driver's parameters enables connectivity to a SAP host for read and query operations. The driver vetoes any subscription modifications sent to the SAP system if this option is selected.

- ◆ Publisher Connection option

This option informs the driver whether or not Publisher channel connectivity to the SAP system is desired.

- ◆ Publish History Items

This option specifies whether the driver returns data values that no longer have a current validity period.

- ◆ Future-dated IDoc processing

Future-dated IDoc processing implements a stale event data check. When future-dated events are processed, the driver attempts to confirm the validity period of the event. If no matching validity period is found for the event data, the IDoc data is considered stale and is not applied. Validity checking can only be accomplished if SAP system connectivity is established through configuring the driver's authentication parameters. Publisher Channel Only drivers without connectivity process all future-dated events at the indicated date.

- ◆ Character set encoding is used to parse data from IDocs.

The driver allows you to specify which character set encoding is used to parse data from IDocs. If nothing is specified, the driver uses the platform default encoding. If you incorrectly specify a character set, the driver initialization fails. You specify this encoding option in the driver configuration parameters.

- ◆ Subscriber channel events are applied only to the current instance of SAP Infotype data. Future-dated instances are not affected.
- ◆ The Subscriber channel offers several modes for synchronizing Communication and Internal Data infotypes. All other updates are made as changes to the current valid data.
- ◆ The JCOTEST utility validates that all JCO connectivity and authentication parameters are configured correctly.

1.5 Product Components

This section contains information about the following Identity Manager Driver for SAP HR components.

- ◆ [Section 1.5.1, "Driver Shim," on page 15](#)
- ◆ [Section 1.5.2, "SAP Java Connector Test Utility," on page 15](#)

1.5.1 Driver Shim

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

1.5.2 SAP Java Connector Test Utility

Users implementing the driver must download the SAP JCO and install it. The SAP 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 installation and connectivity to the SAP JCO client, as well as testing for accessibility to the HR BAPIs used by the driver. The JCO3 test utility file name is `JCO3Test.class`.

For more information, refer to [Section 5.3, “Using the SAP Java Connector Test Utility,”](#) on page 42.

1.6 Publishing to the Identity Vault

The SAP HR system is the authoritative source of HR data, and can propagate all Add, Delete, and Modify object event data to the Identity Vault. The Publisher channel is the component used for propagation.

For data to flow from the SAP HR system, the driver utilizes the SAP ALE technology to publish HR Master data records and captures incremental changes by using change pointers. The HRMD_A message IDocs are transported by using a File port that stores the IDocs on the SAP host system. The driver handles the parsing and filtering of the IDoc file, and provides secure transport of the data to the Identity Vault. Only data elements specifically selected by the system administrator are transported from the host system to the Identity Vault.

- ♦ [Section 1.6.1, “IDoc Consumption by the Driver,”](#) on page 15
- ♦ [Section 1.6.2, “IDoc Object Types Consumed by the Driver,”](#) on page 16
- ♦ [Section 1.6.3, “Attribute Mapping from the SAP HR Database to the Identity Vault,”](#) on page 17

1.6.1 IDoc Consumption by the Driver

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

The format of a successfully published IDoc file is:

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

For example:

```
O_300_0000000000001001.
```

After the specified attributes have been published, the filename of the IDoc file is modified to reflect the status of the publication processes. The driver caches the status of every event and associates the status with the object information in the IDoc. If multiple objects are processed from the IDoc, there might be multiple output files with different extensions created.

The following table lists the IDoc status and corresponding suffix:

IDoc Status	Filename Suffix
Processing, but not published	.proc
Processing, but not published (future date IDoc)	.futp
Processed successfully and published	.done
Processed with an error or warning	.F.fail OR W.warn
Processed with corrupt or illegitimate data	.bad
Process on date shown in timestamp	8 digit timestamp.futr

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

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

If a policy generates multiple events from one object, the worst-case status is cached for the IDoc object. For example, if an IDoc contains data for Person object 00001234 and that data triggers policy events for the Identity Vault User, his Job, and his Position, three separate `<status>` elements are returned. If two of the events have a success status, and the third status is warning, the warning status is used.

After all of the objects in the IDoc have been processed, the driver creates output files based on the status of events. If the IDoc contains warning status events, an IDoc file is generated containing all of the objects whose status was a warning. The name is a concatenation of the original IDoc name and a `W.warn` extension (for example, `O_001_0002` becomes `O_001_0002W.warn`.) In a similar fashion, if the original IDoc contains error or fatal status events, a file with an `F.fail` extension is generated with those events in it.

To reprocess the IDoc, remove the extension. The use of the `X` character before the extension helps ensure that subsequent reprocessing events do not overwrite the status files from the previous processing attempts.

1.6.2 IDoc Object Types Consumed by the Driver

Object types vary from system to system and can include objects such as Person, Job, or Organizational Unit. The driver allows the administrator to configure which object types can be processed by the driver.

Only object types specified in the configuration and object types that are in the Publisher Filter are processed. The driver parses the data for each object individually and transmits the data to the Metadirectory engine as a single transaction.

NOTE: If SAP connectivity is specified, the driver attempts to populate empty Publisher values by reading values from the SAP server. This only occurs if the Metadirectory engine requests more data (via a query request) when trying to complete an Add event operation.

1.6.3 Attribute Mapping from the SAP HR Database to the Identity Vault

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

Several of the HRMD_A infotypes could be instantiated multiple times on the HR personnel records. Infotypes such as P0006 (Private Address) and P0105 (Communication) might be used several times to indicate unique subtypes. For example, the Private Address infotype might have Home, Work, or Temporary subtypes. The Communication infotype might contain Cell, Pager, EMail or other subtypes. The Identity Vault administrator can configure the driver to receive whatever subtypes of P0006 and P0105 infotypes are desired. The SAP HRMD_A messages that are generated by the SAP HR system are posted in the form of a text file. The schema map also contains the file position offset and length of each attribute in each segment of infotype data.

This information is presented in a schema map. The map elements have the following format:

```
<Segment Infotype>:<Infotype Attribute>:<Infotype Subtype> or none: <Segment offset>:<Attribute length>
```

Table 1-1 lists a few examples of maps between SAP HRMD_A attributes and Identity Vault attributes. The Infotype P0002 attributes have no possible subtypes. Infotypes P0006 and P0105 have a configurable set of subtypes.

Table 1-1 Attribute Mapping

Identity Vault Attribute	SAP HR Attribute
Given Name	P0002:VORNA:none:134:25
Surname	P0002:NACHN:none:84:25
City	P0006:ORT01:US01:133:25
Home City	P0006:ORT01:1:133:25
Internet EMail Address	P0105:USRID:MAIL:78:30
Mobile	P0105:USRID:CELL:78:30
Pager	P0105:USRID:PAGR:78:30
Home Phone	P0006:TELNR:1:195:14

The driver only utilizes configuration for Private Address (0006) and Communication (0105) infotypes. Mapping of additional instance-specific infotype attributes might create errors caused by a many-to-one object relationship.

1.7 Subscribing from the Identity Vault

The Subscriber channel of the driver is the component responsible for synchronizing data from the Identity Vault, including data that was obtained from other authoritative data sources, into the SAP HR database. Because the SAP HR system is always viewed as an authoritative source of personnel object creation and deletion, the Subscriber channel is configured to only allow data to be queried, or read, from the SAP HR system, and to allow modification of existing object records.

The Subscriber channel is capable of synchronizing fewer data elements to SAP than the Publisher channel can synchronize to the Identity Vault. For data to flow from the Identity Vault to the SAP HR system, the driver utilizes SAP-released BAPI functions to make changes to employee records. Because of BAPI restrictions, the driver completely supports only the following infotype data:

- ◆ Personal Data (Infotype 0002)
- ◆ Private Address (Infotype 0006)
- ◆ Communication (Infotype 0105)
- ◆ Internal Data (Infotype 0032)

The system administrator specifically selects which attributes from these infotypes can be modified.

1.8 Support for Standard Driver Features

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

- ◆ [Section 1.8.1, “Local Platforms,” on page 18](#)
- ◆ [Section 1.8.2, “Remote Platforms,” on page 18](#)
- ◆ [Section 1.8.3, “Entitlements,” on page 19](#)

1.8.1 Local Platforms

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

The SAP HR 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 the instructions in [“Preparing to Install the Engine, Drivers, and Plug-ins”](#) in the *NetIQ Identity Manager Setup Guide*.

1.8.2 Remote Platforms

The SAP HR driver must reside on the same server as the SAP HR 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 HR 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 for the Remote Loader](#) in the *NetIQ Identity Manager Setup Guide*.

NOTE: The driver is not supported with the Java Remote Loader because of the native library dependency.

1.8.3 Entitlements

The SAP HR 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.

2 Upgrading an Existing Driver

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

- ◆ [Section 2.1, “Supported Upgrade Paths,” on page 21](#)
- ◆ [Section 2.2, “What’s New?,” on page 21](#)
- ◆ [Section 2.3, “Upgrading the Driver,” on page 21](#)

2.1 Supported Upgrade Paths

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

2.2 What’s New?

- ◆ [Section 2.2.1, “What’s New in Version 4.0.1,” on page 21](#)
- ◆ [Section 2.2.2, “What’s New in Version 4.0.0,” on page 21](#)

2.2.1 What’s New in Version 4.0.1

This version provides the following key features:

- ◆ The driver supports handling of IDocs that are in processing state when the driver is restarted after a crash. For more information, see [“Publisher Options” on page 70](#).
- ◆ You can instruct the driver to process IDoc in a specific or multiple languages that the driver supports. For more information, see [“Publisher Options” on page 70](#).

2.2.2 What’s New in Version 4.0.0

This version Version 4.0.0 of the driver does not include any new features.

The driver continues to use SAP JCO3 APIs.

2.3 Upgrading the Driver

The driver upgrade process involves upgrading the installed driver packages and updating the driver files.

This section provides general instructions for updating a driver. For information about updating the driver to a specific version, search for that driver patch in the [NetIQ Patch Finder Download Page](#) and follow the instructions from the Readme file accompanying the driver patch release.

- ◆ [Section 2.3.1, “Upgrading the Installed Packages,” on page 22](#)
- ◆ [Section 2.3.2, “Applying the Driver Patch,” on page 22](#)

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

2.3.1 Upgrading the Installed Packages

- 1 Download the latest available packages.

To configure Designer to automatically read the package updates when a new version of a package is available, click **Windows > Preferences > NetIQ > Package Manager > Online Updates** in Designer. However, if you need to add a custom package to the Package Catalog, you can import the package .jar file. For more information about creating custom packages, see [Developing Packages](#) in the *NetIQ Designer for Identity Manager Administration Guide*.

- 2 Upgrade the installed packages.

- 2a Open the project containing the driver.

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

- 2c Click **Packages**.

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

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

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

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

NOTE: Designer lists all versions available for upgrade.

- 2g Click **Apply**.

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

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

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

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

For detailed information, see the [Upgrading Installed Packages](#) in the *NetIQ Designer for Identity Manager Administration Guide*.

2.3.2 Applying the Driver Patch

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

Prerequisites

Before installing the patch, complete the following steps:

- 1 Take a back-up of the current driver configuration.
- 2 (Conditional) If the driver is running with the Identity Manager engine, stop the Identity Vault and the driver instance.
- 3 (Conditional) If the driver is running with a Remote Loader instance, stop the Remote Loader instance and the driver instance.

- 4 In a browser, navigate to the [NetIQ Patch Finder Download Page](#).
- 5 Under **Patches**, click **Search Patches**.
- 6 Specify **Identity Manager *nn* SAP HR Driver *nn*** in the search box.
- 7 Download and unzip the contents of the patch file to a temporary location on your server.
For example, `IDM402_SAPHR_4002.zip`.

Applying the Patch as a Root User

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

1 Update the driver files:

- ♦ **Linux:** Log in to your server as `root` and run the following commands in a command prompt:

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

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

For example, `rpm -Uvh <IDM402_SAPHR_4003.zip>/linux/novell-DXMLSaphrjco.rpm`

- ♦ **Windows:** Navigate to the `<Extracted Driver Patch File Temporary Location>\windows` folder and copy the following files to `<IdentityManager installation>\NDS\lib` or `<IdentityManager installation>\RemoteLoader\<architecture>\lib` folder:

- ♦ `jco3environment.jar`

- ♦ `SAPHRshim.jar`

- ♦ **Solaris:** To install the driver files on Solaris, contact NetIQ Support.

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

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

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

Applying the Patch as a Non-Root User

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

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

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

```
ROOTDIR=<non-root eDirectory location>
```

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

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

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

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

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

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

3 Installing the Driver Files

By default, the SAP HR 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 4, "Creating a New Driver Object," on page 27](#)) or upgrade an existing driver's configuration (see [Chapter 2, "Upgrading an Existing Driver," on page 21](#)).

The SAP HR driver must be located on the same server as the SAP HR 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 HR server. This requires eDirectory to be installed on the server. See the instructions in ["Preparing to Install the Engine, Drivers, and Plug-ins"](#) in the *NetIQ Identity Manager Setup Guide*.
- ◆ Install the Remote Loader (required to run the driver on a non-Metadirectory server) and the SAP HR driver files to the SAP HR server. This assumes that you already have a Metadirectory server installed on another server in your environment. See [System Requirements for the Remote Loader](#) in the *NetIQ Identity Manager Setup Guide*.

As part of the installation, select the **Utilities** option and install the SAP Utilities. If you have 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 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).

4 Creating a New Driver Object

After the SAP HR driver files are installed on the server where you want to run the driver (see [Chapter 3, “Installing the Driver Files,” on page 25](#)), you can create the driver object in the Identity Vault. You do so by importing the basic driver configuration file and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- ◆ [Section 4.1, “Creating a SAP HR Account,” on page 27](#)
- ◆ [Section 4.2, “Creating the Driver Object in Designer,” on page 27](#)
- ◆ [Section 4.3, “Activating the Driver,” on page 32](#)
- ◆ [Section 4.4, “Adding Packages to an Existing Driver,” on page 33](#)

4.1 Creating a SAP HR Account

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

4.2 Creating the Driver Object in Designer

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

- ◆ [Section 4.2.1, “Importing the Current Driver Packages,” on page 27](#)
- ◆ [Section 4.2.2, “Installing the Driver Packages,” on page 28](#)
- ◆ [Section 4.2.3, “Configuring the Driver Object,” on page 31](#)
- ◆ [Section 4.2.4, “Deploying the Driver Object,” on page 31](#)
- ◆ [Section 4.2.5, “Starting the Driver,” on page 32](#)

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

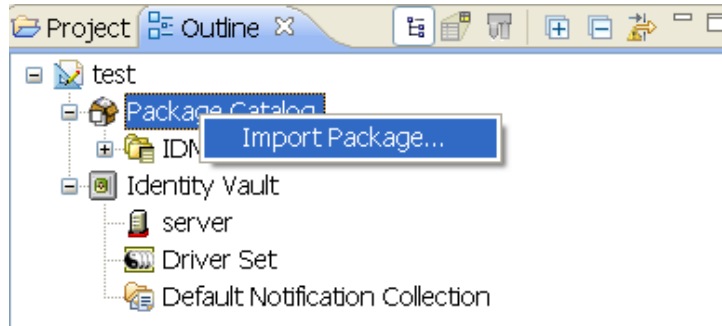
4.2.1 Importing the Current Driver Packages

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 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 HR 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 4.2.2, “Installing the Driver Packages,” on page 28](#).

4.2.2 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 HR Integration Base**, then click **Next**.
- 4 Select the optional features to install for the SAP HR driver, then click **Next**. All options are selected by default. The options are:
 - Default Configuration:** This package contains the default configuration information for the SAP HR driver. Always leave this option selected.
 - Password Synchronization:** This package contains the policies that enable the SAP HR driver to synchronize passwords. If you want to synchronize passwords, verify that this option is selected. For more information, see the [NetIQ Identity Manager Password Management Guide](#).
 - 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 [NetIQ Identity Reporting: User’s Guide to Running Reports](#).
- 5 (Conditional) If there are package dependencies for the packages you selected to install, you must install them to install the selected packages. Click **OK** to install the package dependencies.

- 6 (Conditional) If more than one type of package dependency must be installed, you are presented with these packages separately. Continue to click **OK** to install any additional package dependencies.
- 7 (Conditional) The Common Settings page is displayed only if the Common Settings package is installed as a dependency. On the Install Common Settings page, fill in the following fields:
 - User Container:** Select the Identity Vault container where the SAP HR accounts will be added if they don't already exist in the vault. This value becomes the default 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 where the SAP HR accounts will be added if they don't already exist in the vault. This value becomes the default 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.
- 8 Click **Next**.
- 9 On the Driver Information page, specify a name for the driver, then click **Next**.
- 10 On the Install SAP HR Integration page, fill in the following fields, then click **Next**:
 - SAP User ID:** Specify SAP user ID this driver uses for SAP Logon. This is referred to as the User in the SAP Logon screen.
 - SAP User Password:** Specify the password for the SAP user ID.
 - SAP Application Server:** Specify the hostname or IP address for connecting to the appropriate SAP Application server. This is referred to as the Application Server in the SAP Logon properties.
 - SAP System Number:** Specify the SAP system number on the SAP application server. This is referred to as the System Number in the SAP logon properties. Use this option only if the driver is configured for SAP Connectivity.
 - 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. Use this option only if the driver is configured for SAP Connectivity.
 - Metadata File Directory:** Specify the file system location where the SAP Metadata definition file resides. By default this is in the `SAPUTILS` subdirectory of the driver shim installation directory.
 - IDoc File Directory:** Specify the file system location where the SAP HR IDoc files are placed by the SAP ALE system.
- 11 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 ["Configuring the Remote Loader and Drivers"](#) in the *NetIQ Identity Manager Setup Guide*.

If you select **No**, skip to [Step 12](#). 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.

- 12 (Conditional) The Install SAP HR Integration Managed System Information page is displayed only if you selected to install the Data Collection and Account Tracking packages. Fill in the following fields to define your SAP HR system, then click **Next**:

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

Description: Specify a brief description for this SAP HR system. The description is displayed in reports.

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

Vendor: Leave SAP as the vendor of this SAP HR system. This information is displayed in reports.

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

- 13 (Conditional) The Install SAP HR Integration Managed System Information page is displayed only if you selected to install the Data Collection and Account Tracking packages. Fill in the following fields to define the classification of the SAP HR system, then click **Next**:

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

- ◆ Mission-Critical
- ◆ Vital
- ◆ Not-Critical
- ◆ Other

If you select **Other**, you must specify a custom classification for the SAP HR system.

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

- ◆ Development
- ◆ Test
- ◆ Staging
- ◆ Production
- ◆ Other

If you select **Other**, you must specify a custom classification for the SAP HR system.

- 14 (Conditional) The Install SAP HR Integration Managed System Information page is displayed only if you selected to install the Data Collection and Account Tracking packages. Fill in the following fields to define the ownership of the SAP HR system, then click **Next**:

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

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

- 16 After you have installed the driver, you must change the configuration for your environment. Proceed to [Section 4.2.3, "Configuring the Driver Object," on page 31](#).

4.2.3 Configuring the Driver Object


After installing the driver packages, you should complete the following tasks to configure the driver object before it can run:

- ♦ **Ensure that the driver can authenticate to the SAP HR system:** Ensure that you have established an SAP HR administrative account for the driver (see [Section 4.1, “Creating a SAP HR Account,” on page 27](#)) 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 66](#)).
- ♦ **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 67](#).
- ♦ **Configure the driver policies and filter:** Modify the driver policies and filter to implement your business policies. For instructions, see [Chapter 6, “Customizing the Driver,” on page 47](#).

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

4.2.4 Deploying the Driver Object

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

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select **Live > Deploy**.
- 3 If you are authenticated to the Identity Vault, skip to [Step 4](#); otherwise, specify the following information, then click **OK**:

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 Read through the deployment summary, then click **Deploy**.
- 5 Read the successful message, then click **OK**.
- 6 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.

6a Click **Add**, then browse to and select the object with the correct rights.

6b Click **OK** twice.

For more information about defining a Security Equivalent User in objects for drivers in the Identity Vault, see [Establishing a Security Equivalent User](#) in the [NetIQ Identity Manager Security Guide](#).

- 7 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.

7a Click **Add**, then browse to and select the user object you want to exclude, then click **OK**.

7b Repeat [Step 7a](#) for each object you want to exclude.

7c Click **OK**.

8 Click **OK**.

4.2.5 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 If you are using the Remote Loader with the driver, ensure the Remote Loader driver instance is running.

For instructions, see [Starting a Driver Instance in the Remote Loader](#) in the *NetIQ Identity Manager Setup Guide*.

2 In Designer, open your project.

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

For information about management tasks with the driver, see [Chapter 7, "Managing the Driver,"](#) on [page 57](#).

4.3 Activating the Driver

The Identity Manager driver for SAP HR is part of the Identity Manager Integration Module for SAP Enterprise. This integration module includes the following drivers:

- ♦ Identity Manager driver for SAP Portal
- ♦ Identity Manager driver for SAP User Management (the SAP User Management Fan-Out driver uses the same shim)
- ♦ Identity Manager driver for SAP HR

This integration module requires a separate activation. After purchasing the integration module, you will receive activation details in your NetIQ Customer Center.


If you create a new SAP HR driver in a driver set that already includes an activated driver from this integration module, the new driver inherits the activation from the driver set.

If you create the driver in a driver set that has not been previously activated with this integration module, the driver will run in the evaluation mode for 90 days. You must activate the driver with this integration module during the evaluation period; otherwise, the driver is disabled.

If driver activation has expired, `ndstrace` displays an error message indicating that you need to reactivate the driver to use it. For information on activation, refer to [Activating Identity Manager](#) in the *NetIQ Identity Manager Setup Guide*.

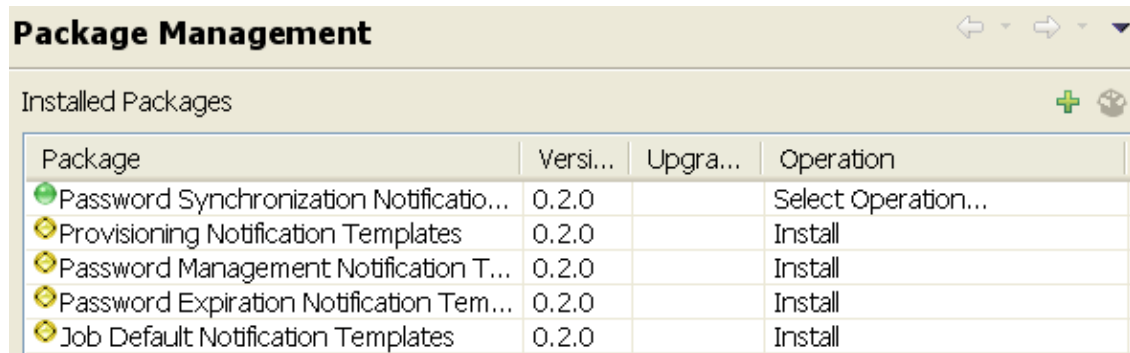
4.4 Adding Packages to an Existing Driver

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

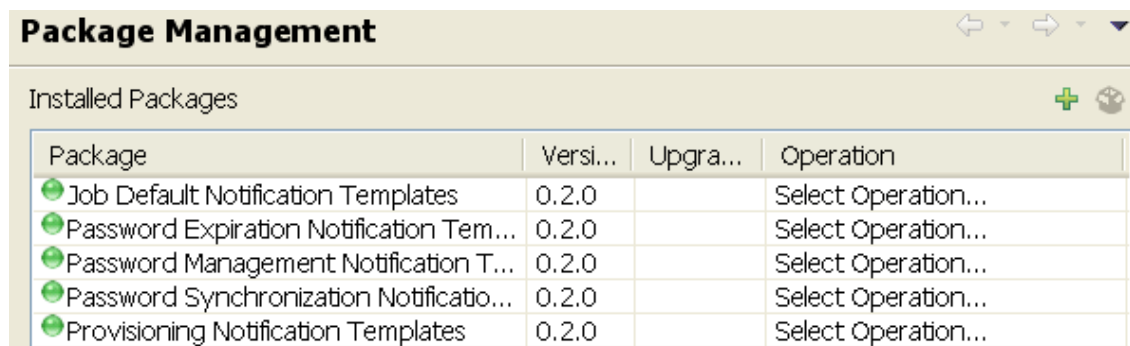
- 1 Right-click the driver, then click **Properties**.
- 2 Click **Packages**, then click the **Add Packages** icon .
- 3 Select the packages to install. If the list is empty, there are no available packages to install.
- 4 (Optional) Deselect the **Show only applicable package versions** option, if you want to see all available packages for the driver, then click **OK**.

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

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



- 6 (Conditional) Fill in the fields with appropriate information to install the package you selected for the driver, then click **Next**.
- 7 Read the summary of the installation, then click **Finish**.
- 8 Click **OK** to close the Package Management page after you have reviewed the installed packages.



- 9 Repeat [Step 1](#) through [Step 8](#) for each driver where you want to add the new packages.

5 Configuring the SAP System

You must configure the SAP system parameters to enable Application Link Enabling (ALE) processing of HRMD_A IDocs. This allows for data distribution between two application systems, also referred to as messaging. NetIQ follows SAP's general guidelines for configuring BAPI (Business Application and Programming Interface) and ALE technologies.

For information about ALE, see [Appendix B, "Application Link Enabling \(ALE\)," on page 77](#). For information about BAPI, see [Appendix D, "Business Application Programming Interfaces \(BAPIs\)," on page 83](#).

To configure the SAP system, refer to the information in the following sections:

- [Section 5.1, "Configuring the SAP System," on page 35](#)
- [Section 5.2, "Using the Schema Metadata File," on page 40](#)
- [Section 5.3, "Using the SAP Java Connector Test Utility," on page 42](#)

5.1 Configuring the SAP System

As part of configuring the SAP system, you should complete the following steps in this order:

1. ["Defining Sending and Receiving Systems" on page 35](#)
2. ["Creating a Distribution Model" on page 37](#)
3. ["Creating a Port Definition" on page 37](#)
4. ["Generating Partner Profiles" on page 38](#)
5. ["Generating an IDoc" on page 38](#)
6. ["Activating Change Pointers" on page 39](#)
7. ["Scheduling a Job for Change Pointer Processing" on page 39](#)
8. ["Scheduling a Job" on page 39](#)
9. ["Testing the Change Pointer Configuration" on page 40](#)
10. ["Creating a CPIC User" on page 40](#)

NOTE: The following 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 is different.

5.1.1 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.

You must assign a client to the sending logical system. Because the receiving logical system is an external system, there is no need to assign it to a client. You should never assign the same client to more than one logical system.

For this particular solution, we recommend defining two logical systems. One logical system acts as the receiver and the other logical system acts as the sender. Although only one of these logical systems is used as a data source process (that is, the client/logical system where employee data is stored and “actions” occur), the second logical system is needed to represent the receiving process (in this case, the driver.)

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 HRMD_A message type to a previously configured model view. For more information, see [“Creating a Distribution Model” on page 37](#).

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.

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 HR 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 `IDM HR Integration`).
- 7 Save your entry.

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 and select the *sender* logical system you want to assign to this client (such as `ADMCLNT100`).
- 6 Save your entry.

5.1.2 Creating a Distribution Model

The distribution model contains essential information about message flow. The model view defines the systems that communicate with each other and the messages that 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, type transaction code `BD64`. Ensure that you are in Change mode (click **Table View** > **Display** > **Change**.)
- 3 Click **Edit** > **Model View** > **Create**.
- 4 Type the short text to describe the distribution model (such as `Client 100 Distribution to IDM`).
- 5 Type the technical name for the model (such as `SAP2IDM`).
- 6 Accept the default **Start** and **End** dates or specify valid values. Click the check mark icon to save your entry.
- 7 Select the view you created, then click **Add Message Type**.
- 8 Define the sender/logical system name.
- 9 Define the receiver/server name.
- 10 Define the Message Type you want to use (`HRMD_A`), then click **Continue**.
- 11 Click **Save**.

5.1.3 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. You should configure a file port for this solution. The file port is used to determine the directory and the file location to which IDocs are sent.

To create a file port definition:

- 1 Type transaction code `WE21`.
- 2 Select **File**, then click the **Create** icon. Specify information for the following fields:
 - Name port:** Specify the port name.
 - Port description:** Specify a description of the port.
 - Version:** Select SAP release 4.X.
- 3 On newer SAP servers, the database might be Unicode. If this is true, select the **Unicode Format** check box on the **System Setting** tab.
- 4 Define the outbound file:
 - 4a 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\.`
 - 4b Specify the function module. This names the IDoc file in a specific format. Always use the following format: `EDI_PATH_CREATE_CLIENT_DOCNUM`.
- 5 Save your changes.

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

5.1.4 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 HRMD_A message type.

Generating a Profile

- 1 Type transaction code `BD82`.
- 2 Select the model view. This should be the model view previously created in [“Creating a Distribution Model” on page 37](#).
- 3 Ensure that the **Transfer IDoc immediately** and **Trigger Immediately** option buttons are selected.
- 4 Select a reasonable packet size value to ensure that IDoc files are not too large to process. We recommend a value of 100.
- 5 Click **Execute**.

Modifying the Port Definition

When you generated a partner profile, the port definition might have been entered incorrectly. For your system to work properly, you need to modify the port definition.

- 1 Type transaction code `WE20`.
- 2 Select **Partner Type LS**.
- 3 Select your receiving partner profile.
- 4 Select **Outbound Parameters**, then click **Display**.
- 5 Select message type `HRMD_A`.
- 6 Click **Outbound Options**, then modify the receiver port so it is the file port name you created in [“Creating a Port Definition” on page 37](#).
- 7 In the Output Mode section, select **Transfer IDoc Immediately** to send IDocs immediately after they are created.
- 8 In the IDoc Type section, select the latest version available for your system.
- 9 Click **Continue/Save**.

5.1.5 Generating an IDoc

- 1 Type transaction code `PFAL`.
- 2 Insert the **Object Type P** for person objects.
- 3 Enter an employee’s ID for the **Object ID** or select a range of employees.
Under the **Parallel Processing** tab, set **Number of Objects per Process** to **100** if you select a range of employees.
- 4 Click **Execute**.

Ensure that the status is set to **Passed to Port Okay**.

The IDoc has been created. Go to the directory where IDocs are stored (it was defined in the file port setup) and verify that the IDoc text file was created.

5.1.6 Activating Change Pointers

To activate change pointers globally:

- 1 Type transaction code `BD61`.
- 2 Enable the **Change Pointers Active** tab.

To activate change pointers for a message type:

- 1 Type transaction code `BD50`.
- 2 Scroll to the **HRMD_A message type**.
- 3 Select the **HRMD_A** check box, then click **Save**.

5.1.7 Scheduling a Job for Change Pointer Processing

- 1 Type transaction code `SE38` to begin defining the variant.
- 2 Select the **RBDMIDOC program**, select **Variant**, then click the **Create** icon.
- 3 Name the variant and give it a description.
Make note of the variant name so you can use it when you schedule the job.
- 4 Select the **HRMD_A** message type, then click **Save**.
You are prompted to select variant attributes.
- 5 Select the background processing attribute.
- 6 Click **Save**.

5.1.8 Scheduling a Job

- 1 Type transaction code `SM36`.
- 2 Name the job.
- 3 Assign a Job Class.
Job Class is the priority in which jobs are processed. Class **A** is the highest priority and is processed first. For a production environment, we recommend assigning the class to **B** or **C**.
- 4 Schedule a start time. Click the **Start Condition** tab, then click **Date and Time**. Specify a scheduled start time, which must be a future event.
 - 4a Mark the job as a periodic job, click the **Periodic Values** tab, schedule how frequently you want the job to run, then press **Enter**. For testing purposes, we recommend setting this period to 5 minutes.
 - 4b Click **Save**.
- 5 Define the job steps:
 - 5a Type the ABAP program name: `RBDMIDOC`.
 - 5b Select the variant you created in the previous step.
- 6 Click **Save**.

IMPORTANT: Click **Save** once; otherwise, the job is scheduled to run multiple times.

5.1.9 Testing the Change Pointer Configuration

- 1 In the SAP client, hire an employee.
- 2 Ensure that an IDoc was created.

You can verify IDoc creation in two locations:

- ♦ Type transaction code `WE02`
- ♦ Go to the IDoc file locations

5.1.10 Creating a CPIC User

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

- 1 In **User Maintenance in SAP**, specify a username in the user dialog box, then click the **Create** icon.
- 2 Click the **Address** tab, then specify data in the **Last Name** and **Format** fields.
- 3 Click the **Logon Data** tab, then define the initial password and set the user type to **CPIC**.
- 4 Click the **Profiles** tab, then add the **SAP_ALL**, **SAP_NEW** and **S_A.CPIC** profiles.
- 5 Click **Save**.

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.

IMPORTANT: If restricted rights are assigned to the CPIC User, the Identity Manager and SAP administrators are responsible to ensure that sufficient rights are assigned to enable the configured level of integration. [Appendix D, "Business Application Programming Interfaces \(BAPIs\)," on page 83](#) contains a table describing which BAPIs the driver uses.

5.2 Using the Schema Metadata File

The driver includes three default Metadata files: `HRMD_A03.meta`, `HRMD_A05.meta`, and `HRMD_A07.meta`. These files contain the SAP metaschema definitions of the `HRMD_A03`, `HRMD_A05`, and `HRMD_A07` IDoc types, where

- ♦ `HRMD_A03` IDoc type is the standard HR Master Data IDoc for version 4.5B of SAP R/3
- ♦ `HRMD_A05` IDoc type is the standard HR Master Data IDoc for version 4.6C
- ♦ `HRMD_A07` IDoc type, which is the standard HR Master Data IDoc for version 6.0.

These files are provided for two distinct purposes:

- ♦ The driver uses a metadata file to generate an Application Schema Map policy via the **Refresh Application Schema** option in iManager.
- ♦ If a **Character Set Encoding** value is specified in the configuration, the driver opens the metadata file to determine if the encoding value specified is valid.

The following sections provide information to help you use the Metadata files:

- ♦ [Section 5.2.1, “Creating a New Schema Metadata File,” on page 41](#)
- ♦ [Section 5.2.2, “Reducing the Size of the Schema Metadata File,” on page 42](#)
- ♦ [Section 5.2.3, “Extending the Schema Metadata File,” on page 42](#)

5.2.1 Creating a New Schema Metadata File

A schema map must exist for the IDoc type that the driver consumes, if the **Master HR IDoc** configuration parameter specifies the type or if the driver selects a default type based on the version of the SAP Application server. Because the driver provides only three maps, you might need to create a new map for the IDoc type needed by the driver.

You can simply copy the `HRMD_A07.meta` file to a new file, such as `HRMD_A08.meta`. This is acceptable as long as you do not need to publish newer infotypes not found in the `HRMD_A08` version. It is unlikely that newer infotypes are needed.

To publish newer infotypes other than the ones included in `HRMD_A07.meta` file, Identity Manager provides an XML driver configuration file that converts a SAP HR schema xml file into an HRMD file that the driver can consume. To create an HRMD file,

- 1 Export HRMD_A* schema from the SAP HR database.
 - 1a Login to SAP and go to transaction WE60, select **BASIC TYPE** option.
 - 1b Type `HRMD*` in the text field.
 - 1c Select the version you want to use (for example, `HRMD_A07`).
 - 1d Click **Documentation > XML schema** to display the schema in XML format.
 - 1e Click **XML > Download** to save the schema.
- 2 Create a Delimited Text driver by using the SAP-HRMD driver configuration file (`SAP-HRMD.xml`) in Designer. For information about importing a driver configuration file, see [“Importing a Driver Configuration File”](#) in the *NetIQ Designer for Identity Manager Administration Guide*.

The SAP-HRMD driver configuration file is present in the `SAPHRUtils` subdirectory of the driver shim installation directory. It is located in `C:\Novell\NDS\DirXMLUtilities\sap\SAPUtils` on Windows and `/opt/novell/eDirectory/lib/dirxml/rules/saphr` on Linux.

- 3 In the driver configuration (Delimited Text driver), specify the location of the schema file in the **Metadata File Directory** field. This is the file you exported in [Step 1](#).

The Delimited Text driver converts the schema file into a Metamap file that SAP HR driver can consume. It stores the file in the `SAPUtils` subdirectory of the driver shim installation directory as `HRMD_A*.meta.TEST`. Rename this file to `HRMD_A*.meta`.

5.2.2 Reducing the Size of the Schema Metadata File

The size of the metaschema definitions can create problems for your driver configuration. The schema refresh can take a long time to process, especially because a copy of the map is generated for each object type you choose to synchronize. Additionally, the size of the schema in the driver configuration can be extremely large and cumbersome to navigate. For these reasons, it is acceptable to reduce the number of infotypes in the metadata files.

You can edit the appropriate metadata file and remove all infotypes that are not used for your implementation. Simply search for the infotypes to remove (for examples, Infotype 0008 values can be found by searching for P0008) and deleting the SEGMENT: line and subsequent infotype field lines from the file. You should modify a copy of the original file. For most integrations, only 20-30 percent of the infotypes are actually used.

IMPORTANT: You must be careful that you do not remove infotypes that are useful for policies or other object types being synchronized. Two infotypes of this nature are Infotype 1000 (for Descriptions of non-person objects) and Infotype 1001 (Relationships between objects.) These are both used in the default driver configuration.

You must also avoid removing fields from infotypes that are used in your integration. Field removal is extremely hard to detect if a mistake is made or if you want to return to an earlier version.

5.2.3 Extending the Schema Metadata File

There are many situations where an IDoc is extended with custom infotypes or infotype fields. Because the schema map is based on standard SAP IDoc types, you must manually create these types of metadata extensions. There are several areas of concern:

- ♦ If the infotype is an extension to the IDoc (for example, Infotype Z0001), you must ensure that the infotype header fields are present in a standard format. These standard fields start with the field PERNR and extend through field RESE2 in data infotypes. If these fields are not present or contain no data, many of the driver features such as future-dating and history-dating do not work.
- ♦ The format of new infotypes is similar to the standard infotypes. The first field should be <5 character infotype>:PERNR:0:8. When parsing an actual IDoc, the physical offset for the PERNR field is 63 (when starting from position 0.)

You can also create schema extensions directly to the Mapping Rule without the need to update the metadata file. If you choose this option, which is often easier, remember the physical offset mentioned above when determining where your data fields of interest begin. The format for a direct mapping is described in [Section 1.6.3, “Attribute Mapping from the SAP HR Database to the Identity Vault,” on page 17](#). Selecting field names is up to you, because the driver does not use them for processing, but they should be limited to 5 characters for consistency.

5.3 Using the SAP Java Connector Test Utility

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.

This utility enables you to check for JCO installation and configuration issues prior to configuring the driver. Use the JCO test utility to validate installation and connectivity to the SAP JCO client, as well as testing for accessibility to the HR BAPIs used by the driver.

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.

There might be minor modifications to JCO components as the connector is updated by SAP. Always refer to the SAP installation documentation for proper configuration instructions.

- ♦ [Section 5.3.1, “What Does the Utility Do?,” on page 43](#)
- ♦ [Section 5.3.2, “Utility Prerequisites,” on page 43](#)
- ♦ [Section 5.3.3, “Components,” on page 43](#)
- ♦ [Section 5.3.4, “Running and Evaluating the Test,” on page 44](#)
- ♦ [Section 5.3.5, “Understanding Test Error Messages,” on page 45](#)

5.3.1 What Does the Utility Do?

The SAP 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 R/3 target system are correct.
- ♦ Ensures that the authentication parameters to the SAP R/3 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 R/3 target system.

5.3.2 Utility Prerequisites

Before you run the JCO Test utility, you must install the SAP JCO client for the desired platform. The JCO can be obtained only 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.

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

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

5.3.3 Components

The JCO Test utility includes a `JCO3Test.class` for SAPHR JCO3 driver files. You need to create a batch or script file to run the test. The format of the 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 `JCO3Test.class` files.

A sample UNIX script file and Win32 batch file is listed below for the `JCO3Test.class` file.

JCO3Test.class: The `sapjco3.jar` is in the executable directory of the `JCO3Test.class` file and the batch file.

```
Win32 jco3test.bat file
java -classpath %CLASSPATH%;. JCO3Test
```

```
Unix jco3test file
java JCO3Test
```

You must use proper slash notation when specifying pathnames and 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 `JCO3Test` test class must be specified with proper case for any platform.

5.3.4 Running and Evaluating the Test

- ◆ [“Running the Test” on page 44](#)
- ◆ [“Evaluating the Test” on page 44](#)
- ◆ [“Post-Test Procedures” on page 45](#)

Running the Test

To run the JCO Test utility on a Win32 platform:

- 1 In Windows Explorer, double-click your `.bat` file.
or
In a command prompt, run your `.bat` script.

To run the JCO Test utility on a UNIX platform:

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

When you run the test program, an error message might appear before any test output is displayed. This indicates an improper installation of the JCO client components. The error messages are documented for each platform in [“Understanding Test Error Messages” on page 45](#).

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 information for the following fields 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 (and 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 SAP HR Driver Configuration
```

```
Authentication ID: Username
```

```
Authentication Context: SAP Host Name/IP Address
```

```
Application Password: User password
```

```
Publisher Channel Only? 1
```

```
SAP System Number: System Number
```

```
SAP User Client Number: Client Number
```

```
SAP User Language: Language Code
```

```
Master HR IDoc: Default IDoc type for SAP R/3 version
```

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 SAP HR Driver functionality.
```

Post-Test Procedures

After the JCO Test Utility has passed all tests successfully, the driver can be configured to run. Ensure that the `sapjco3.jar` file is copied to the location where the `sapshim.jar` files have been installed.

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

5.3.5 Understanding Test Error Messages

Use the information in this section to analyze error messages that might display during the 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 JCO are configured in a similar manner and errors generated by improper JCO installation and configuration should be similar to the errors described for IBM-AIX and Solaris.

General Errors

Use the information in this section to analyze error messages that might display during the JCO3 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).
Caught Exception during connection: java.lang.Exception: SAP Connection Exception: com.sap.conn.jco.JCoException: (103) RFC_ERROR_LOGON_FAILURE: Name or password is incorrect (repeat logon) on <host> sysnr <system number>	Invalid credentials (JCo 3.0.2+).
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.driver.CpicDriver.nativeCpicGetVerstion(I)I Verify proper installation of JCo Native support libraries packaged with JCo client	Exception while initializing JCo client 3.0.2+.

6 Customizing the Driver

Policies are highly configurable for use within any business environment. Although each business is different, the default driver configuration is built with a scenario that involves synchronizing SAP Person (P), Organization (O), Position (S), and Job (C) objects into the Identity Vault.

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

- ◆ [Section 6.1, “Modifying the Policies and the Filter,” on page 47](#)
- ◆ [Section 6.2, “Using the Relationship Query,” on page 52](#)
- ◆ [Section 6.3, “Populating the Identity Vault with Organizational Data,” on page 55](#)

6.1 Modifying the Policies and the Filter

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

- ◆ Modify the driver filter to include desired attributes to be synchronized.
- ◆ Modify the Schema Mapping policy to include all attributes specified in the driver filter.
- ◆ Modify the Input Transformation policy
- ◆ Modify the Output Transformation policy
- ◆ Modify the Publisher Placement policy
- ◆ Modify the Publisher Matching policy
- ◆ Modify the Publisher Creation policy
- ◆ Modify the Publisher Command Transformation policy
- ◆ Modify the Subscriber Matching policy

Refer to the following sections:

- ◆ [Section 6.1.1, “The Driver Filter,” on page 48](#)
- ◆ [Section 6.1.2, “The Schema Mapping Policy,” on page 49](#)
- ◆ [Section 6.1.3, “The Input Transformation Policy,” on page 50](#)
- ◆ [Section 6.1.4, “The Output Transformation Policy,” on page 50](#)
- ◆ [Section 6.1.5, “The Publisher Placement Policy,” on page 51](#)
- ◆ [Section 6.1.6, “The Publisher Matching Policy,” on page 51](#)
- ◆ [Section 6.1.7, “The Publisher Creation Policy,” on page 51](#)
- ◆ [Section 6.1.8, “The Publisher Command Transformation Policy,” on page 51](#)

6.1.1 The Driver Filter

The driver filter contains the set of classes and attributes whose updates publish from the SAP system to the Identity Vault, and from the Identity Vault to SAP.

To use the default driver configuration, you shouldn't filter out any of the CommExec, Organizational Role, or Organizational Unit attributes. Also, do not remove the Given Name, Surname, and workforceID attributes from the User class object.

The following table lists the filter classes and attributes:

Classes	Attributes
CommExec	Description
Organizational Role	Description directReports manager Role Occupant
Organizational Unit	Description
User	employeeStatus Full Name Given Name homePhone Initials isManager Login Disabled manager managerWorkforceID mobile OU pager Physical Delivery Office Name Postal Code S SA Surname Telephone Number Title workforceID

6.1.2 The 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 HR 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 optional.

The following attribute mappings are included with the default driver configuration:

Identity Vault Class	SAP Class	SAP Description
CommExec	C	Job
Organizational Role	S	Position
Organizational Unit	O	Organization
User	P	Person

The User class is configured to synchronize bidirectionally between SAP and the Identity Vault. A change made in one system transfers to the other system. However, changes made to the CommExec, Organizational Role, and Organizational Unit attributes are synchronized from SAP to the Identity Vault only.

All attributes in the Publisher and Subscriber filters should be mapped unless they are only used for policies processing (for example, Login Disabled.)

The following table includes common attribute mappings for the User class and their descriptions:

Identity Vault Attribute	SAP Attribute Description	SAP Attribute
Given name	First Name	P0002:VORNA:none:134:25
Initials	Initials	P0002:INITS:none:74:10
Internet EMail Address	Communication ID/Number (with a mail subtype)	P0105:USRID:MAIL:78:30
NSCP:employeeNumber	Personnel Number	P0001:PERNR:none:0:8
OU	Organizational Unit	P0001:ORGEH:none:125:8
Postal Code	Postal Code (work address subtype)	P0006:PSTLZ:US01:183:10
S	Region (State, Province, or County for the work address subtype)	P0006:STATE:US01:248:3
Surname	Last Name	P0002:NACHN:none:84:25
employeeStatus	Country ISO Code (work subtype)	P0000:STAT2:none:79:1
homeCity	City (permanent address subtype)	P0006:ORTO1:1:133:25
homeFax	Communication Type (permanent address subtype)	P0006:COM01:1:274:20
homePhone	Telephone Number (permanent address subtype)	P0006:TELNR:1:195:14
Title	Position	P0001:PLANS:none:133:8

Identity Vault Attribute	SAP Attribute Description	SAP Attribute
mobile	Communication ID/Number (cell phone subtype)	P0105:USRID:CELL:78:30
pager	Communication ID/Number (pager subtype)	P0105:USRID:PAGR:78:30
jobCode	Job	P0001:STELL:none:141:8
personalTitle	Other title	P0002:NAMZU:none:189:15
preferredName	Known As	P0002:RUFNM:none:234:25
workforceID	Personnel Number	P0002:PERNR:none:0:8

6.1.3 The Input Transformation Policy

You modify the Input Transformation policy to implement your specific business rules. The Input Transformation policy is applied to transform 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 Transformation policy converts the syntax of the SAP attributes into the syntax for the Identity Vault. The Input Transformation policy is implemented as an XSLT style sheet.

The default driver configuration includes templates that complete the following actions:

- ◆ Modifies the association for non-Person objects to include the Class code.
- ◆ Manipulates the OU attribute to contain a name-number syntax.
- ◆ Manipulates the Title to contain text data.
- ◆ Manipulates the Job Code to contain text data.
- ◆ Transforms Postal Address from string syntax to structure syntax.
- ◆ Translates telephone numbers from a numerical string into a formatted telephone number.
- ◆ Translates employee status from numerical format into either an A (Active) or I (Inactive) status code.
- ◆ Adds an employee status code if it is not present in query replies.

6.1.4 The Output Transformation Policy

You modify the Output Transformation policy to implement your specific business rules. The Output Transformation 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 and returned to the driver by Identity Manager. The Output Transformation policy is implemented as an XSLT style sheet.

The Output Transformation policy reverses the logic of the Input Transformation policy. The default driver configuration includes templates that complete the following actions:

- ◆ Transforms Postal Address from structure syntax to string syntax.
- ◆ Returns telephone numbers to string format.
- ◆ Removes the Class code from non-Person object associations.

6.1.5 The 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. Only the Publisher channel utilizes the Placement policy.

The Placement policy uses the employeeStatus attribute value and the values of driver object placement Global Configuration Values (GCVs) to place objects in specified Identity Vault containers.

6.1.6 The 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 primarily on the workforceID attribute. A secondary rule is provided to attempt matching by Surname and Given Name values.

6.1.7 The Publisher Creation Policy

The Publisher Creation policy is applied when a new object is to be added to the Identity Vault. The Creation policy is implemented by using both Policy Builder and XSLT style sheets.

The default driver configuration has Creation policies for the following:

- ◆ Organizational Unit (if a Description attribute is present).
 - ◆ Creates a name for the object based on its Description.
 - ◆ Creates the OU attribute.
- ◆ Organizational Role Object (if a Description attribute is present).
 - ◆ Creates a name for the object based on its Description.
 - ◆ Creates the CN attribute.
- ◆ CommExec Object (if the Description attribute is present).
 - ◆ Creates a name for the object based on its Description.
 - ◆ Creates the CN attribute.
- ◆ User Object (the Surname and Given Name are transferred).
 - ◆ Generates an object name based on Given Name and Surname.
 - ◆ Sets the initial password to the user's Surname.

6.1.8 The Publisher Command Transformation Policy

The Publisher Command Transformation policy is used to apply any remaining business logic to event documents received from the driver. The default driver performs the following transformations:

- ◆ Creates and maintains User object Manager and Direct Reports organizational relationships.
- ◆ Sets the Login Disabled attribute based on employee status.

- ♦ Maintains proper Group Membership for an Employee or Manager group based on a User's position, employee status, and GCV group name values.
- ♦ Handles placement of User objects in Active or Inactive containers based on employee status and GCV user placement values.

6.2 Using the Relationship Query

The SAP HR system is a relational database. Individual HR objects, such as the Person object, do not contain all of the information that is typically needed to describe the function of the Person within an organization. Organizational and Position information is contained in different objects that are related to the Person object for a specified period of time. The name of a Position a Person holds, the name of the Organization he or she belongs to, and the Organizational hierarchy to which a person belongs can only be determined by traversing the various relationships between objects.

The SAP driver has a special capability that allows a query to be made for the object relationships between an SAP object being processed in the Publisher channel and other SAP objects. This information is contained in Infotype 1001 (Object relationships) in the HRMD_A IDoc. (The documentation for the meaning of the various fields of this Infotype can be found on the SAP system by using transaction WE60.) Because this relationship information cannot be easily mapped to Identity Vault attributes, and because namespace attributes are stripped out of XML documents during various phases of processing, the capability to query for the pseudo-class RELATIONSHIPS was built into the driver.

The Relationship Query uses different forms:

- ♦ [Section 6.2.1, "Query 1," on page 52](#)
- ♦ [Section 6.2.2, "Query 2," on page 52](#)
- ♦ [Section 6.2.3, "Query 3," on page 54](#)

6.2.1 Query 1

This query uses the class identifier of the last object sent by the driver to the engine. In the context of the driver's default configuration, this query provides accurate results for obtaining relationship data from Position objects as they are processed.

```
<nds dtdversion="1.0" ndsversion="8.5">
  <input>
    <query class-name="RELATIONSHIPS" event-id="0"
      scope="entry">
      <association>50000354</association>
    </query>
  </input>
</nds>
```

6.2.2 Query 2

This query utilizes the `<search-class>` element to specify the class of the object from which relationship data is desired. The driver combines the value of the element with the association to identify the proper relationship vector to return. This allows the policies to obtain relationship data from any object in the current IDoc being processed. The default driver configuration contains queries of this type to provide working examples.

```

<nds dtdversion="1.0" ndsversion="8.5">
  <input>
    <query class-name="RELATIONSHIPS" event-id="0"
      scope="entry">
      <association>50000354</association>
      <search-class class-name="S"/>
    </query>
  </input>
</nds>

```

The driver allows the return of all relationship information in a structured <value> format. This allows the style sheets to utilize any relationship data that is desired for implementing business rules. It is the responsibility of the configuration expert to determine which data is utilized, including time stamp information. The driver returns all requested fields in the 1001 (Relationships) infotype that contain a value. If a field is not populated or present, it is not returned. A sample of a reply to the RELATIONSHIPS Query 2 is presented below:

```

<nds dtdversion="1.0" ndsversion="8.5">
  <source>
<product build="INVALID_BUILD_ID" instance="SAP-HR" version="1.0.2">Identity
Manager Driver for SAP/HR</product>
  <contact>Novell, Inc.</contact>
  </source>
  <output>
    <instance class-name="RELATIONSHIPS" timestamp="20030529"
xmlns:sapshim="http://www.novell.com/dirxml/drivers/SAPShim">
      <association>50000354</association>
      <sapshim:policyAttr attr-name="RELATIONSHIPS">
        <value type="structured">
          <component name="ITXNR">00000000</component>
          <component name="BEGDA">20020225</component>
          <component name="INFTY">1001</component>
          <component name="SEQNR">000</component>
          <component name="ISTAT">1</component>
          <component name="OTYPE">S</component>
          <component name="RELAT">003</component>
          <component name="ENDDA">99991231</component>
          <component name="SCLAS">0</component>
          <component name="PLVAR">01</component>
          <component name="MANDT">001</component>
          <component name="UNAME">NOVADM</component>
          <component name="RSIGN">A</component>
          <component name="SOBID">50000127</component>
          <component name="OBJID">50000354</component>
          <component name="VARYF">0 50000127</component>
          <component name="AEDTM">20020225</components>
        </value>
        <value type="structured">
          <component name="ITXNR">00000000</component>
          <component name="BEGDA">20020225</component>
          <component name="INFTY">1001</component>
          <component name="SEQNR">000</component>
          <component name="ISTAT">1</component>
          <component name="OTYPE">S</component>
          <component name="RELAT">005</component>
          <component name="ENDDA">99991231</component>
          <component name="SCLAS">S</component>
          <component name="PLVAR">01</component>
          <component name="MANDT">001</component>
          <component name="UNAME">NOVADM</component>
          <component name="RSIGN">A</component>

```

```

<component name="SOBID">50000485</component>
<component name="OBJID">50000354</component>
<component name="VARYF">S 50000485</component>
  <component name="AEDTM">20020301</component>
</value>
<value type="structured">
  <component name="ITXNR">00000000</component>
  <component name="BEGDA">20020225</component>
  <component name="INFY">1001</component>
  <component name="SEQNR">000</component>
  <component name="ISTAT">1</component>
  <component name="OTYPE">S</component>
  <component name="RELAT">007</component>
  <component name="ENDDA">99991231</component>
  <component name="SCLAS">C</component>
  <component name="PLVAR">01</component>
  <component name="MANDT">001</component>
  <component name="UNAME">NOVADM</component>
  <component name="RSIGN">B</component>
  <component name="SOBID">50000144</component>
  <component name="OBJID">50000354</component>
  <component name="VARYF">C 50000144</component>
  <component name="AEDTM">20020225</component>
</value>
</sapshim:policyAttr>
</instance>
</output>
</nds>

```

The `<read-attr>` implementation of the driver RELATIONSHIPS query has been modified as follows:

- ♦ The lack of a `<read-attr>` element implies a request to return all components of each matching relationship value.
- ♦ An empty `<read-attr/>` element specifies that no values will be returned. This is a useless operation that is not recommended.
- ♦ `<read-attr>` elements with `attr-name` attribute values indicate which specific component values are desired for each matching relationship value.

The `<search-attr>` functionality of the XDS DTD has been added to the driver RELATIONSHIP query. This enables queries for relationships matching more exacting criteria to reduce the quantity and type of reply data. Multiple `<search-attr>` values are interpreted as a logical AND of the individual search components. The default Publisher Command Transformation policy has been modified to use the new capabilities of the driver.

6.2.3 Query 3

The following example is from the `set-roles-manager-attr` template, used to retrieve the SOBID value from any relationship with an RSIGN value of A and an SCLAS value of S:

```

<nds dtdversion="1.0" ndsversion="8.5">
  <input>
    <query class-name="RELATIONSHIPS" event-id="0" scope="entry">
      <association>
        <xsl:value-of select="$newRole-ID"/>
      </association>
      <search-class class-name="S"/>
      <search-attr attr-name="RSIGN">
        <value>A</value>
      </search-attr>
      <search-attr attr-name="SCLAS">
        <value>S</value>
      </search-attr>
      <read-attr attr-name="SOBID"/>
    </query>
  </input>
</nds>

```

6.3 Populating the Identity Vault with Organizational Data

In order to populate the Identity Vault with the organizational data, the existing data must be exported from SAP. To export your organization's hierarchical data, perform the following steps before starting the driver:

- 1 In the SAP client, enter transaction code `PFAL`.
- 2 Insert the Object Type O for Organization objects.
- 3 Specify the organizations you want to export to the Identity Vault. You can choose to export one organization, a range of organizations, or all organizations.
If you are exporting a range of objects, go to the **Parallel Processing** tab on the **HR: ALE Distribution of HR Master Data** page, then select a value of **100** or less at the **Number of Object per Process** prompt. This ensures that driver processing does not consume too much Java heap space.
- 4 Click **Execute**. Ensure that the status is set to **Passed to Port Okay**.
- 5 Repeat [Step 1](#) through [Step 4](#) for Object Type C for Job objects.
- 6 Repeat [Step 1](#) through [Step 4](#) for Object Type S for Position objects.

IMPORTANT: Export the objects in the order specified above. This ensures that the driver creates the correct relationships when users are imported into the Identity Vault.

7 Managing the Driver

As you work with the SAP HR 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 [NetIQ Identity Manager Driver Administration Guide](#).

8 Troubleshooting the Driver

This section contains potential problems and error codes you might encounter while configuring or using the driver.

- ♦ [Section 8.1, “Using the DSTrace Utility,” on page 59](#)
- ♦ [Section 8.2, “Driver Load Errors,” on page 59](#)
- ♦ [Section 8.3, “Driver Initialization Errors,” on page 61](#)

8.1 Using the DSTrace Utility

You can troubleshoot the driver by using the DSTrace utility. You should configure the utility's options by selecting **Edit > Properties > Identity Manager Drivers**.

For each event or operation received, the driver returns an XML document containing a status report. If the operation or event is not successful, the status report also contains a reason and a text message describing the error condition. If the result is fatal, the driver shuts down.

After you have configured the DSTrace utility, you can monitor your system for errors.

For more information about the DSTrace utility, see [“Viewing Identity Manager Processes”](#) in the *NetIQ Identity Manager Driver Administration Guide*.

8.2 Driver Load Errors

If the driver does not load, check DSTrace for the error messages.

- ♦ [Section 8.2.1, “java.lang.ClassNotFoundException:com.novell.nds.dirxml.drivers.SAPshim.SAPDriver Shim,” on page 59](#)
- ♦ [Section 8.2.2, “Error Occurs when Uninstalling the Driver,” on page 59](#)
- ♦ [Section 8.2.3, “Error DestinationDataProvider already registered,” on page 60](#)

8.2.1 java.lang.ClassNotFoundException:com.novell.nds.dirxml.drivers.SAPshim.SAPDriver Shim

This is a fatal error that occurs when the class name for the `SAPHRShim.jar` is incorrect. Ensure that the Java class name is set on the **Driver Module** tab in a local installation and that the `-class` parameter is set in a Remote Loader configuration.

The proper class name is `com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim`.

8.2.2 Error Occurs when Uninstalling the Driver

If you have installed the SAP HR driver on a server that does not have a Java Virtual Machine (JVM) installed on it, you receive the following error when you try 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 occurs only if you install the SAP HR Management (JCO3) driver on a server that does not have Identity Manager or the Remote Loader installed on it.

Use the following workaround on Linux:

- 1 Export PATH=<JAVA-HOME-PATH>/bin/:\$PATH.
- 2 Run the Uninstall script where the JAVA-HOME-PATH is the JAVA or the JRE install location.
For more information, see [“Removing Objects from the Identity Vault”](#) in the *NetIQ Identity Manager Setup Guide*.

Use the following workaround on Windows:

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

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

Replace JAVA-HOME-PATH with the JAVA or the JRE install location.

8.2.3 Error DestinationDataProvider already registered

The error DestinationDataProvider already registered occurs, if you are running an SAP HR driver for JCO3 and an SAP User Management driver for JCO3 on the same Metadirectory engine.

The fix is to run the SAP HR driver and the SAP User Management driver with the Remote Loader. Each driver can register as a separate instance in JCO when the drivers are running with the Remote Loader. If the drivers are running locally, JCO uses the same instance for the drivers and that is what causes the error.

Here is a sample of the error:

```
DirXML Log Event -----
  Driver:   \IDMDT-RRGIRISH\n\test\SAP-HR
  Status:   Error
  Message:  Code(-9010) An exception occurred:
java.lang.IllegalStateException: DestinationDataProvider already registered
[com.novell.nds.dirxml.driver.sapumshim.RFCJCoDestinationProvider]
  at
com.sap.conn.jco.rt.RuntimeEnvironment.setDestinationDataProvider(RuntimeEnvironment.java:132)
  at
com.sap.conn.jco.ext.Environment.registerDestinationDataProvider(Environment.java:216)
  at
com.novell.nds.dirxml.driver.SAPHRShim.BapiCommon.registerJCOProviders(BapiCommon.java:509)
  at
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim.init(SAPDriverShim.java:110)
  at com.novell.nds.dirxml.engine.Driver.startShim(Driver.java:1314)
  at com.novell.nds.dirxml.engine.Driver.initialize(Driver.java:260)
  at com.novell.nds.dirxml.engine.Driver.<init>(Driver.java:232)
  at com.novell.nds.dirxml.engine.DriverEntry.run(DriverEntry.java:551)
  at java.lang.Thread.run(Thread.java:619)
```

8.3 Driver Initialization Errors

If you have installed the SAP HR Management (JCO3) driver, you might see the following driver initialization errors in the DSTrace utility:

- ◆ [Section 8.3.1, “com/sap/conn/jco/ext/DestinationDataProvider Exception,” on page 61](#)
- ◆ [Section 8.3.2, “Could not Initialize class com.sap.conn.jco.rt.JCoRuntimeFactory,” on page 61](#)
- ◆ [Section 8.3.3, “Common Errors,” on page 61](#)

8.3.1 com/sap/conn/jco/ext/DestinationDataProvider Exception

This error occurs when the SAP Java Connector `sapjco3.jar` file or the JCO native support libraries are not present or are improperly located.

Ensure the proper platform version of `sapjco3.jar` is located in the same directory as `SAPShim.jar`. Also check the JCO native support libraries to ensure they are present and properly configured. Use the JCO3 installation instructions for the appropriate platform.

8.3.2 Could not Initialize class com.sap.conn.jco.rt.JCoRuntimeFactory

This error occurs when the SAP Java Connector (JCO) native support library is not present or is located improperly. Ensure the JCO native support libraries are present and configured properly. Use the JCO3 installation instructions for the appropriate platform.

8.3.3 Common Errors

This section contains the common errors encountered by the SAPHR JCO3 driver.

- ◆ [“Error connecting to SAP host” on page 62](#)
- ◆ [“nsap-pub-directory parameter is not a directory” on page 62](#)
- ◆ [“No connection to Remote Loader” on page 62](#)
- ◆ [“Authentication handshake failed, Remote Loader message: “Invalid loader password.”” on page 62](#)
- ◆ [“Authentication handshake failed: Received invalid driver object password” on page 62](#)
- ◆ [“Attribute Mapping Error” on page 62](#)
- ◆ [“Changes in SAP Do Not Generate an IDoc/Change Document” on page 62](#)
- ◆ [“The Driver Does Not Recognize IDocs in the Directory” on page 63](#)
- ◆ [“IDocs Are Not Written to the Directory” on page 63](#)
- ◆ [“The Driver Does Not Authenticate to SAP” on page 63](#)
- ◆ [“JCO Installation and Configuration Errors” on page 63](#)
- ◆ [“Error When Mapping Drives to the IDoc Directory” on page 63](#)
- ◆ [“Driver Configured as “Publisher-only” Still Tries to Connect to the SAP System” on page 64](#)
- ◆ [“com.novell.nds.dirxml.engine.VRDEException” on page 64](#)
- ◆ [“The Driver Fails to Delete 0105 And 0032 Infotypes On The Publisher Channel” on page 64](#)

Error connecting to SAP host

This error occurs when the SAP authentication or connection information is not configured properly. Ensure that the values for Authentication and Driver Parameters are correct for authentication to the SAP host system.

nsap-pub-directory parameter is not a directory

This error occurs when the Publisher IDoc Directory parameter in the Publisher Settings of the Driver Parameters does not specify a valid file system location. Ensure that this parameter specifies the directory on the SAP system configured in the SAP ALE subsystem for IDoc file output.

No connection to Remote Loader

This error occurs when the Remote Loader connection parameter information is incorrect. Configure the proper connection information for the remote connection to the system where the Remote Loader is running.

Authentication handshake failed, Remote Loader message: “Invalid loader password.”

This error occurs when the Remote Loader password configured on the remote system does not match the Remote Loader password on the Driver object.

Set matching passwords for both remote loaders. In iManager, ensure that both the application password and Remote Loader password are set at the same time.

Authentication handshake failed: Received invalid driver object password

This error occurs when the driver password configured on the remote system does not match the Driver object password on the Driver object. To correct this, both Driver object passwords should be identical.

Attribute Mapping Error

If the Mapping policy Add Dialog contains no data for the APP (application properties of class mappings), the driver cannot find the HRMD_A schema metafile.

You should ensure that the metafile directory and Master HR IDoc driver parameters are set to a valid file system location and contain the proper IDoc name. Validate that the metadata file for the configured IDoc type is in the file system location. For example, if Master HR IDoc is set to the default HRMD_A03, ensure that `HRMD_A03.meta` exists in the metafile directory.

Changes in SAP Do Not Generate an IDoc/Change Document

Ensure that the ALE and change pointer processes are configured properly, and that you have properly entered data.

The proper way of inserting or changing data is through using the **Edit > Create** or **Edit > Change** menus. If an error or a change is entered by overwriting an existing record and saving it, the change document is not created.

The Driver Does Not Recognize IDocs in the Directory

Verify that the driver parameters contain the correct client number and proper IDoc directory.

IDocs Are Not Written to the Directory

You should first test the ALE and IDoc interface. Refer to your SAP documentation for more information.

If the IDoc interface fails:

- ◆ Use transaction WE21, to ensure that the file port is configured properly. Validate the path to the directory and ensure that the **Transfer IDoc Immediately** option button is selected.
- ◆ Use transaction WE20, to ensure that the appropriate file port is selected in the Partner Profile. Also, verify that it is on the outbound parameters of the receiving system.

If the IDoc interface succeeds:

- ◆ Ensure that the change pointers have been configured.
- ◆ Ensure that the scheduled processes are not scheduled too closely. For example, if one job is in process and another job begins, the second job might be canceled because the first job is still running.

The Driver Does Not Authenticate to SAP

First, ensure that you have configured all of the driver parameters and that the proper passwords have been entered.

If you are using the Publisher Channel Only configuration of the driver, ensure that you have entered the correct parameters. If you have previously used a Publish and Subscribe driver, ensure that all files have been replaced by the Publish-only files.

If you are running the driver remotely, ensure that the Remote Loader has been started before you start the driver.

JCO Installation and Configuration Errors

For detailed instructions on using the JCO Test utility and analyzing error messages, refer to [Section 5.3, "Using the SAP Java Connector Test Utility," on page 42.](#)

Error When Mapping Drives to the IDoc Directory

You might see the following error in DSTrace if the IDoc directory parameter specifies an invalid local file system container or if it specifies a mapped drive on a remote system.

```
*** NDS Trace Utility - BEGIN Logging *** Fri Sep 13 15:45:59 2005
```

```
Identity Manager Log Event -----  
  Driver = \FLIBBLE_TREE\n\Driver Set\SAP-HR  
  Channel = publisher  
  Status = fatal  
  Message = <description>SAP Document Poller initialization failed:  
com.novell.nds.dirxml.driver.SAPShim.SAPDocumentPollerInitFailure: Specified  
Publisher IDoc Directory is invalid.</description>
```

```
*** NDS Trace Utility - END Logging *** Fri Sep 13 15:46:31 2005
```

This error occurs because the Windows operating system service controls the rights of the local system, not the rights of a user. Thus, the local Windows system does not have rights to access any file resources outside of its own system, including the IDoc directory.

Driver Configured as “Publisher-only” Still Tries to Connect to the SAP System

The driver is designed to use a connection to SAP even when it is configured as a Publisher-only driver. The first purpose for using this connection is to verify the version of the SAP server so that the driver can configure itself for the proper version of IDocs it will consume. Otherwise, the driver must be configured with a value for the [Master HR IDoc:](#) parameter.

This connection also verifies the validity time stamps of desired infotypes during processing of future-dated event IDocs. This is an extremely critical function that should always be enabled if future-dated processing options are chosen in the driver configuration. Disabling this capability could result in the propagation of old or stale events that have been subsequently overridden.

If you don't want a connection to the SAP server, you should remove at least one of the following connection parameters:

- SAP Application Server (see [“Authentication Context:” on page 66](#))
- SAP User ID (see [“Authentication ID:” on page 66](#)).
- SAP User Password (see [“Application Password:” on page 66](#)).

In this situation, the IDoc data being processed is used as a completely authoritative source of reliable data.

com.novell.nds.dirxml.engine.VRDEException

This error occurs when the SAP Java Connector (JCO) components cannot be located. This generally occurs if the driver or Remote Loader has not been restarted after the JCO has been configured. Restart NetIQ eDirectory if you are using a local configuration or restart the Remote Loader for a remote configuration.

The Driver Fails to Delete 0105 And 0032 Infotypes On The Publisher Channel

This occurs due to the limitations of iDoc.

To work around this issue, see the instructions in [TID 3449102](#) in the [NetIQ Support Knowledge Base](#).

A Driver Properties


This section provides information about the Driver Configuration and Global Configuration Values properties for the SAP HR 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 *NetIQ Identity Manager Driver Administration Guide* for information about the common properties.

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

- ♦ [Section A.1, “Driver Configuration,” on page 65](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 71](#)

A.1 Driver Configuration

In iManager:

- 1 Click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit:
 - 2a In the **Administration** list, click **Identity Manager Overview**.
 - 2b If the driver set is not listed on the **Driver Sets** tab, use the **Search In** field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Locate the driver icon, then click the upper right corner of the driver icon to display the **Actions** menu.
- 4 Click **Edit Properties** to display the driver’s properties page.

By default, the Driver Configuration page is displayed.

In Designer:

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

The Driver Configuration options are divided into the following sections:

- ♦ [Section A.1.1, “Driver Module,” on page 66](#)
- ♦ [Section A.1.2, “Driver Object Password,” on page 66](#)
- ♦ [Section A.1.3, “Authentication,” on page 66](#)
- ♦ [Section A.1.4, “Startup Options,” on page 67](#)
- ♦ [Section A.1.5, “Driver Parameters,” on page 67](#)
- ♦ [Section A.1.6, “ECMAScript,” on page 71](#)
- ♦ [Section A.1.7, “Global Configuration,” on page 71](#)

A.1.1 Driver Module

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

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

The Java class name for JCO3 is:

```
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim
```

Native: This option is not used with the SAP HR 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:** Select this option to include information on the Remote Loader client configuration when Designer generates documentation for the 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

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: `SAPHR`

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

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

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 service 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`

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 Options

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

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

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

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

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

A.1.5 Driver Parameters

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

The parameters are presented by category:

- ◆ [“Driver Options” on page 67](#)
- ◆ [“Subscriber Options” on page 69](#)
- ◆ [“Publisher Options” on page 70](#)

Driver Options

Publisher Channel Only: Select whether you want the driver to use the Publisher channel only or if you want it to use both the Publisher and Subscriber channels.

The driver is designed to use a connection to SAP even when it is configured as a Publisher-only driver. The first purpose for using this connection is to verify the version of the SAP server so that the driver can configure itself for the proper version of IDocs it will consume. Otherwise, the driver must be configured with a value for the [Master HR IDoc:](#) parameter.

This connection also verifies the validity time stamps of desired infotypes during processing of future-dated event IDocs. This is an extremely critical function that should always be enabled if future-dated processing options are chosen in the driver configuration. Disabling this capability could result in the propagation of old or stale events that have been subsequently overridden.

If you don't want a connection to the SAP server, you should remove at least one of the following connection parameters:

- ◆ SAP Application Server (see [“Authentication Context:” on page 66](#))

- ♦ SAP User ID (see “[Authentication ID:](#)” on page 66).
- ♦ SAP User Password (see “[Application Password:](#)” on page 66).

In this situation, the IDoc data being processed is used as a completely authoritative source of reliable data.

SAP System Number: The SAP system number on the SAP application server. This is referred to as the System Number in the SAP logon properties.

SAP User Client Number: The client number to be used on the SAP application server. This is referred to as the Client in the SAP R/3 logon screen.

SAP User Language: The language this driver uses for the SAP session. This is referred to as the Language in the SAP R/3 logon screen.

Character Set Encoding: The character set encoding used to parse data from IDocs. By default, no character set encoding is specified, which causes the driver to use the platform default encoding. If you incorrectly specify a character set, the driver initialization fails.

Metadata File Directory: The file system location in which the SAP Metadata definition file resides. By default, this is in the `SAPUTILS` subdirectory of the driver's installation directory.

Master HR IDoc: The name of the IDoc type that is generated by the SAP ALE system to publish SAP HR database Master data modification. If it is not specified, the driver determines the revision of the SAP HR system and defaults to the standard IDoc type for that revision of SAP. The default is `HRMD_A05`.

This field is optional, unless you select the Publisher Channel Only option.

Future-dated Event Handling Option: The processing of this option is determined by the Begin and End validity dates of the desired IDoc infotypes. There are four possible values for this parameter. The driver default is to Publish on Future Date.

- ♦ **Publish Immediately:** Indicates that all attributes will be processed by the driver when the IDoc is available. A time stamp is set for each attribute that represents the validity period.

With this option, all attributes including the future dated ones are processed when IDoc is used.

- ♦ **Publish on a Future Date:** Indicates that only attributes that have a current or past time stamp will be processed by the driver when the IDoc is available. Future-dated infotype attributes are cached in a `.futr` file to be processed at a future date.

With this option, the beginning date of each infotype is read from IDoc. All infotypes with the current date are processed immediately and those with a future date are stored in a new IDoc with a `.futr` extension. The name of the file remains the same as the original IDoc except for the extension. There is *only* one `.futr` file for an IDoc. When a future IDoc file is processed, infotypes with the current date (today's date) are processed first, and then if there are any future infotypes, a new IDoc file is created with a `.futr` extension to replace the old `.futr` file.

- ♦ **Publish Immediately and on a Future Date:** Indicates that the driver will blend options 1 and 2. All attributes are processed, with a time stamp, at the time the IDoc is available. All future-dated infotype attributes are also cached in a `.futr` file to be processed at a future date.

This option is useful if there are custom policies in place to perform actions based on a future event. For example, to perform some action to kick off a workflow, if there is an event from the future.

- ♦ **Publish Immediately and Daily through Future Date:** Indicates that the driver will process all events at the time the IDoc is made available. All future-dated infotype attributes are cached in a `.futr` file to be processed again on the next calendar day. This continues until the attributes are sent for a final time on the future date.

This option is used when there are custom policies in place to perform actions based on a future event. For example, to perform some action to kick off a workflow, if there is an event from the future. An example would be where you want to check every day to see if a future event of a hire date requires an action, such as creating a mailbox seven days in advance of the future date.

Future-dated Event Validity Checking Option: Specifies whether or not the driver attempts to filter out stale data in future-dated IDocs by verifying the begin and end validity dates of the data.

This option is used in scenarios, such as when a future infotype received for a new hire is cancelled. This works for many infotypes but not all, because of an SAP limitation.

Publish History Items: Specifies if data values that are no longer valid are published by the driver. The default is **Do Not Publish History Data**.

Object Type Code: A list parameter that allows an administrator to specify which HR object types are synchronized. The default list is P, S, O, and C.

Address Subtype Code: A list of configuration parameters that allows an administrator to specify which subtype of data the SAP Private Address infotype the driver synchronizes. The default is 1 and US01.

Communication Subtype Code: A list configuration parameters that allows an administrator to specify which subtype data of the SAP Communication infotype the driver synchronizes. The default is CELL, MAIL, PAGR.

Subscriber Options

Communication Change Mode: This Subscriber channel parameter specifies how the driver handles requests to change, remove, or add Communication (Infotype 0105) record instances on employees. There are three modes of operation available. For more information on the functionality of the various modes of operation, see [Appendix E, “Subscriber Change Modes and Validity Date Modes,” on page 85](#).

The options are:

- ♦ Delimit mode
- ♦ Delete mode
- ♦ Change mode (default driver mode)

Communication Validity Date Mode: This Subscriber channel parameter specifies how Beginning and Ending validity dates are set on newly created Communication record instances on employees. There are two modes of operation available. For more information on the functionality of the various modes of operation, see [Appendix E, “Subscriber Change Modes and Validity Date Modes,” on page 85](#).

The options are:

- ♦ Default Mode
- ♦ Current Date Mode

Internal Data Change Mode: This Subscriber channel parameter specifies how the driver handles requests to change, remove, or add Internal Control Data (Infotype 0032) record instances on employees. There are three modes of operation available. For more information on the functionality of the various modes of operation, see [Appendix E, “Subscriber Change Modes and Validity Date Modes,”](#) on page 85.

The options are:

- ◆ Delimit mode
- ◆ Delete mode
- ◆ Change mode (default driver mode)

Internal Data Validity Date Mode: This Subscriber channel parameter specifies how Beginning and Ending validity dates are set on newly created Internal Control Data record instances on employees. There are two modes of operation available. For more information on the functionality of the various modes of operation, see [Appendix E, “Subscriber Change Modes and Validity Date Modes,”](#) on page 85.

The options are:

- ◆ Default mode
- ◆ Current Date Mode (default driver mode)

Publisher Options

IDoc File Directory: The file system location in which the SAP HR IDoc files are placed by the SAP ALE system.

This location must be accessible to the driver shim process.

IDoc Processing Order: Select the order in which the IDoc must be processed. The options are **Filename** and **Timestamp**.

Enable all Languages for IDoc import: Specify a language in which the driver should process IDoc from the list of languages supported by the driver.

- ◆ **Enable:** Select this option to process IDoc in all the supported languages.
- ◆ **Select import languages:** Select this option to import IDoc in one or more languages.

Processing IDoc Handling Option: Specify how the driver should handle an existing unprocessed IDoc when the driver is restarted after a crash. By default, this parameter is set to **Ignore**.

- ◆ **Ignore:** Select this option to skip reprocessing an IDoc that was in the **.proc** state when the driver crashed. Other IDocs in the queue are processed.
- ◆ **Reprocess:** Select this option to reprocess an IDoc that was in the **.proc** state when the driver crashed.
- ◆ **Stop Driver:** Select this option to stop the driver. When the driver stops, it displays a message if there is an unprocessed IDoc. When you restart the driver, you can configure the driver to process the IDoc again or ignore it.

Enable or Disable Publisher Connection to the SAP Application Server: Select **Enable** if you want the Publisher channel to read data from the SAP server in addition to IDoc data.

Poll Interval (secs): When the Publisher channel has finished processing all source files, it waits the number of seconds specified in this parameter before checking for new source files to process.

Publisher Heartbeat Interval: Specify how many minutes of inactivity can elapse before this channel sends a heartbeat document. In practice, more than the number of minutes specified can elapse. That is, this parameter defines a lower bound.

A.1.6 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 Configuration


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 HR driver includes several predefined GCVs. You can also add your own if you discover that 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, “Configuration,” on page 72](#)
- ◆ [Section A.2.2, “Password Synchronization,” on page 73](#)
- ◆ [Section A.2.3, “Managed System Information,” on page 74](#)

A.2.1 Configuration

The configuration GCVs are divided into multiple categories:

- ◆ [“New User Naming” on page 72](#)
- ◆ [“Object Relationships” on page 72](#)
- ◆ [“Future Events” on page 73](#)
- ◆ [“Debugging” on page 73](#)
- ◆ [“Process Logging” on page 73](#)

New User Naming

Show New User Naming Options: Select **Show** to display the new user naming configuration options.

New User Naming: There are three options when naming newly provisioned eDirectory users:

- ◆ **Employee-Named-Based (Variable Length):** There are different variations for how the user name is generated:
 - ◆ First character of Given Name + Surname
 - ◆ First character of Given Name + first character of Initials + Surname
 - ◆ First two characters of Given Name + Surname
 - ◆ First three characters of Given Name + Surname
 - ◆ First character of Given Name + Surname + digit starting with 1 incremented until the name is unique within eDirectory.
- ◆ **Employee-Name-Based (Fixed Length):** There are different variations for how the user name is generated:
 - ◆ First character of Given Name + up to seven characters of Surname
 - ◆ First character of Given Name + first character of Initials + up to six characters of Surname
 - ◆ First two characters of Given Name + up to five characters of Surname
 - ◆ First character of Given Name + up to four characters of Surname + three digits padded with zeros if necessary, starting with 001 and incremented until the name is unique within eDirectory.
- ◆ **Attribute-Value-Based:** The CN of the user object is named by the defined naming attribute value.
 - ◆ **User Naming Attribute:** Specify the attribute value that is used to name new users. The attribute must be supplied in the event.

Object Relationships

Show Object Relationships Options: Select **Show** to display the object relationship configuration options.

Discover Relationships: Select **Yes** to discover relationships between objects in the SAP HR data model.

- ♦ **Filter:** Adds object classes to filter on to discover the relationships between objects in the SAP HR data model and eDirectory.
- ♦ **Object Class:** Specify the object class you want to discover relationships for. Class names must be in the Identity Vault name space.
- ♦ **Attributes:** Add all the relationship attributes you want to be populated. Attribute names must be in the Identity Vault name space.

Future Events

Show Future Event Options: Select **Show** to display the future event configuration options.

Record Future Events: Select **Yes** to record future events.

- ♦ **SAP Business Logic Driver:** Browse to and select the SAP Business Logic driver servicing this HR driver instance.
- ♦ **Filter:** Add all of the attributes you want to be notified of when changes happen in the future. Attribute names must be in the Identity Vault name space.

Debugging

Show Debugging Options: Select **Show** to display the debugging configuration options.

Enable logging for generated attribute names: Select **True** to enable logging for generated attribute names.

Process Logging


Show Process Logging Options: Select **Show** to display the process logging configuration options.

Enable process logging: Select **True** to enable process logging.

- ♦ **Daily Logfile:** Select **True** to create a daily log file with the name of `<YYYYmmDD>-<driver-name>-<drv.proclg.logfile>`.
- ♦ **Log file name:** Specify the final name of the driver log file.
- ♦ **Log file directory:** Specify the directory where the log file is stored.

A.2.2 Password Synchronization

These GCVs enable password synchronization between the Identity Vault and the SAP HR 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, to edit the Password management options go to **Driver Properties > Global Configuration Values**, and then edit it in your Password synchronization policy tab.

For more information about how to use the Password Management GCVs, see [Configuring Password Flow](#) in the [NetIQ Identity Manager Password Management Guide](#).

Connected System or Driver Name: Specify the name of the SAP HR 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: If **True**, allows the driver to use the password from the connected system to set the non-reversible NDS password in eDirectory.

Publish passwords to Distribution Password: If **True**, allows the driver to 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, attempts 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**, allows the driver to notify the user by e-mail of any password synchronization failures.

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 74](#)
- ◆ [“System Ownership” on page 75](#)
- ◆ [“System Classification” on page 75](#)
- ◆ [“Connection and Miscellaneous Information” on page 75](#)

General Information

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

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

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

Vendor: Specifies SAP as the vendor of this SAP HR system. This information is displayed in the reports.

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

System Ownership

Business Owner: Specifies the business owner in the Identity Vault for this SAP HR system. Ensure that a user object is selected. You must not select a role, group, or container.

Application Owner: Specifies the application owner in the Identity Vault for this SAP HR system. Ensure that a user object is selected. You must not select a role, group, or container.

System Classification

Classification: Specifies the classification of the SAP HR 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 HR system.

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

- ◆ Development
- ◆ Test
- ◆ Staging
- ◆ Production
- ◆ Other

If you select **Other**, you must specify a custom classification for the SAP HR system.

Connection and Miscellaneous Information

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

B Application Link Enabling (ALE)

Application Link Enabling (ALE) technology enables communication between SAP and external systems such as the Identity Manager Identity Vault (eDirectory). The following sections provide information about ALE to help you configure your SAP system to support the SAP driver:

- ◆ [Section B.1, “Application Link Enabling Technology,” on page 77](#)
- ◆ [Section B.2, “Clients and Logical Systems,” on page 78](#)
- ◆ [Section B.3, “Message Type,” on page 78](#)
- ◆ [Section B.4, “IDoc Type,” on page 78](#)
- ◆ [Section B.5, “Distribution Model,” on page 78](#)
- ◆ [Section B.6, “Partner Profiles,” on page 79](#)
- ◆ [Section B.7, “Port,” on page 79](#)
- ◆ [Section B.8, “Port Definition,” on page 79](#)
- ◆ [Section B.9, “File Port,” on page 79](#)
- ◆ [Section B.10, “Change Pointers,” on page 79](#)
- ◆ [Section B.11, “Change Document/IDoc Outbound Processing,” on page 79](#)

B.1 Application Link Enabling Technology

Application Link Enabling (ALE) has of various components. When you configure the SAP system to enable the driver, you should consider the following ALE components and their relationship to the driver:

- ◆ Clients and Logical Systems
- ◆ Message Types
- ◆ IDoc Type
- ◆ Distribution Model
- ◆ Partner Profiles
- ◆ Port Definition
- ◆ File Port
- ◆ Change Document/IDoc Outbound Processing

Refer to [Section 5.1, “Configuring the SAP System,” on page 35](#) for instructions on how to configure these SAP system parameters.

B.2 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. Every R/3 or SAP system needs to have a base logical system associated with a client. There is a one-to-one relationship between the client and the logical system.

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

B.3 Message Type

A message type represents the type of data that is exchanged between the two systems. For the driver, the HRMD_A 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, HRMD_A05).

B.4 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, direction, etc.

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.5 Distribution Model

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

The distribution model determines what message types can be sent from a client to another client, as well as the sending and receiving systems. Filters for IDoc segments can also be applied to distribution models.

B.6 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.7 Port

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

B.8 Port Definition

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

B.9 File Port

A file port is used when IDocs are transferred to a file.

B.10 Change Pointers

Change pointers capture a master data change in SAP for a specific message type. These changes are saved into a change document. For example, when a new employee is hired, a change is made and captured in a change document.

B.11 Change Document/IDoc Outbound Processing

A SAP variant is defined for the HRMD_A0# message type. After the variant is defined, a job is scheduled for that variant, which captures the change documents and converts them into IDocs. The outbound process is then triggered.

Multiple change documents can be captured within a single IDoc. The number of IDocs is determined by how frequently jobs are scheduled, not by the number of change documents created. For example, several records might be added, modified, or deleted within the specified job process period. All of these changes are included in a single IDoc.

C Example XML Document Received from the Driver

The following example is a typical XML document that has been parsed from HRMD_A number O_200_0000000000008134.

```
<nds dtdversion="1.0" ndsversion="8.5">
  <source>
    <product build="20050916_0956" instance="SAP-HR" version "3.5">Identity
Manager
  Driver for SAP/HR</product>
  <contact>Novell, Inc.</contact>
</source>
<input xmlns:sapshim="http://www.novell.com/dirxml/drivers/SAPShim">
  <modify class-name="P" event-id="O_200_0000000000008134" src-
dn="00000049" timestamp="20011204-99991231">
  <association>00000049</association>
  <modify-attr attr-name="P0001:STELL:none:141:8">
  <remove-all-values/>
  <add-value>
    <value timestamp="20011018-99991231">50000055</value>
  </add-value>
</modify-attr>
  <modify-attr attr-name="P0000:STAT2:none:79:1">
  <remove-all-values/>
  <add-value>
    <value timestamp="20011018-99991231">3</value>
  </add-value>
</modify-attr>
  <modify-attr attr-name="P0002:NACHN:none:84:25">
  <remove-all-values/>
  <add-value>
    <value timestamp="19960421-99991231">Jones</value>
  </add-value>
</modify-attr>
  <modify-attr attr-name="P0002:VORNA:none:134:25">
  <remove-all-values/>
  <add-value>
    <value timestamp="19960421-99991231">Paul</value>
  </add-value>
</modify-attr>
  <modify-attr attr-name="P0006:STRAS:1:103:30">
  <remove-all-values/>
  <add-value>
    <value timestamp="20010101-99991231">123 Main
Street</value>
  </add-value>
</modify-attr>
</modify>
</input>
</nds>
```

Some characteristics to note:

- ♦ All XML documents received from the SAP HR 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 class-name of the object described (that is, P= Person). The `event-id` attribute contains the IDoc number from which the data is derived. The `src-dn` attribute contains the SAP Object ID value. The `timestamp` attribute contains the date that the IDoc was processed by the driver.
- ♦ The `<association>` element data always contains the SAP Object ID.
- ♦ The `<modify-attr>` element contains the `attr-name` described in SAP format (Segment:Attribute Name:SubType:Value Offset:Value Length).
- ♦ Because multivalue attributes cannot be consistently mapped across systems, the `<remove-all-values>` element is used prior to all `<add-value>` tags. This instructs the Metadirectory engine to remove all existing values for the attribute prior to assigning the new value. If this functionality is not desired, one of the XSLT policies can be used to modify the document.
- ♦ The `<value>` element contains a `timestamp` attribute with the BEGIN VALIDITY-END VALIDITY time stamp of the attribute's data segment (that is, Segment P001 data has a time stamp of 20011018-99991231). This means the data became valid on October 18, 2001 and remains valid to the SAP maximum date. All data segments might have different or future-dated validity time stamps.
- ♦ All values are in a string format.

D Business Application Programming Interfaces (BAPIs)

The table in this section contains a list of BAPIs used by the driver. The driver supports stale Infotype data checks for:

- ♦ Infotype 0001 (providing there are no date gaps in validity dates of data rows)
- ♦ Infotype 0002
- ♦ Infotype 0006
- ♦ Infotype 0105
- ♦ Infotype 0032

It is not possible to do a stale data check on other Infotypes because of the lack of support in the SAP BAPIs. The validity checking algorithm of the driver always returns a valid status for these Infotypes.

BAPI Name	Description
BAPI_EMPLOYEE_CHECKEXISTENCE	Used to check for the existence of an employee with a specified Personnel Number (PERNR.) Only used for queries with no <read-attr> elements.
BAPI_EMPLOYEE_ENQUEUE	Used to lock employee records prior to Subscriber modifications.
BAPI_EMPLOYEE_DEQUEUE	Used to unlock employee records after Subscriber modifications.
BAPI_EMPLOYEE_GETDATA	Used to read an employee's Organizational Assignment (Infotype P0001) records. Used during processing of future-dated IDocs to verify that a key with the validity dates of Organizational Assignment instances in the IDoc still exists in the SAP server (stale data checking.)
BAPI_PERSDATA_GETLIST	Used to obtain a list of keys for an employee's Personal Data (Infotype P0002) records. Used during processing of future-dated IDocs to verify that a key with validity dates of Personal Data instances in the IDoc still exists in the SAP server (stale data checking.)
BAPI_PERSDATA_GETDETAIL	Used to read the current data field values of a specified instance of an employee Personal Data record.
BAPI_PERSDATA_CHANGE	Used to modify the current data field values of a specified instance of an employee Personal Data record.
BAPI_ADDRESSEMP_GETLIST	Used to obtain a list of keys for an employee's Address (Infotype P0006) records. Used during processing of future-dated IDocs to verify that a key with the validity dates of Address instances in the IDoc still exists in the SAP server (stale data checking.)
BAPI_ADDRESSEMP_GETDETAIL	Used to read the current data field values of a specified instance of an employee Address record.

BAPI Name	Description
BAPI_ADDRESSEMP_CHANGE	Used to modify the current data field values of a specified instance of an employee Address record.
BAPI_ADDRESSEMP_GETLIST	Used to obtain a list of keys for an employee's Communication (Infotype P0105) records. Used in SAP R/3 versions 4.6 and later. Used during processing of future-dated IDocs to verify that a key with the validity dates of Communication instances in the IDoc still exists in the SAP server (stale data checking.)
BAPI_EMPLCOMM_GETDETAIL	Used to read the current data field value of a specified instance of an employee Communication record. Used in SAP R/3 versions 4.6 and later.
BAPI_EMPLCOMM_CHANGE	Used to modify the current data field value of a specified instance of an employee Communication record. Used in SAP R/3 version 4.6 and later.
BAPI_EMPLCOMM_CREATE	Used to create a new instance of an employee Communication record. Used in SAP R/3 version 4.6 and later.
BAPI_EMPLCOMM_DELIMIT	Used to set the Ending validity period date of a current instance of an employee Communication record. It is always set to the day prior to the current date. If the Starting validity date and the Ending date are the same, the record instance is deleted. Used in SAP R/3 versions 4.6 and later.
BAPI_EMPLCOMM_DELETE	Used to delete the current instance of an employee Communication record. Used in SAP R/3 versions 4.6 and later.
BAPI_HRMMASTER_SAVE_REPL_MULT	Used to create or replace the current instance of an employee Communication record. Used in SAP R/3 version 4.5.
BAPI_INTCONTROL_GETLIST	Used to obtain a list of keys for an employee's Internal Control Data (Infotype P0032) records. Used during processing of future-dated IDocs to verify that a key with the validity dates of Internal Control Data in the IDoc still exists (stale data checking.)
BAPI_INTCONTROL_GETDETAIL	Used to read the current data field value of a specified instance of an employee Internal Control Data record.
BAPI_INTCONTROL_CREATE	Used to create a new instance of an employee Internal Control Data record.
BAPI_INTCONTROL_CHANGE	Used to modify the current data field of a specified instance of an employee Internal Control Data record.
BAPI_INTCONTROL_DELIMIT	Used to set the Ending validity period date of a current instance of an employee Internal Control Data record. It is always set to the day prior to the current data. If the Starting validity period date and the Ending date are the same, the record instance is deleted. Used in SAP R/3 versions 4.6 and later.
BAPI_INTCONTROL_DELETE	Used to delete the current instance of an employee Internal Control Data record.

E Subscriber Change Modes and Validity Date Modes

- ♦ [“Change Mode Notes” on page 85](#)
- ♦ [“Validity Date Modes” on page 87](#)

E.1 Change Mode Notes

- ♦ The field name BEGDA indicates the Starting validity date of a value
- ♦ The field name ENDDA indicates the Ending validity date of a value.
- ♦ The term “active value” indicates a value that has a BEGDA less than or equal to the current date and an ENDDA greater than or equal to the current date.
- ♦ Although the driver can handle multiple value synchronization of any particular Communication Subtype on either the Publisher or Subscriber channel, there are issues related to the IDocs generated by SAP value deletion/delimit events that make multiple-value synchronization *unadvised* and *unsupported* by the Subscriber channel. It is recommended that only one value for each Communication subtype is maintained.
- ♦ Because multiple fields are available in the Internal Control Data infotype, a remove-value operation does not result in the deletion of the record instance. The result is the removal of the specified field value from the record instance.
- ♦ For Communication values (Infotype P0105), this functionality is only available in SAP R/3 version 4.6A or later and on all Web Application Server versions. On 4.5 systems (no support prior to 4.5B) the driver uses the BAPI_HRMMASTER_SAVE_REPL_MULT function for all operations. <remove-value> and <remove-all-value> operations remove all values of the specified Communication Subtype. <add-value> operations remove all values of the Communication Subtype and create a new value with a BEGDA of (current date -1) and an ENDDA of 99991231.
- ♦ For Internal Control Data values (Infotype P0032), the DELIMIT mode is not available prior to SAP R/3 version 4.6A.

The following sections describe the driver’s behavior for each event type and change mode.

- ♦ [Section E.1.1, “<remove-all-values>,” on page 85](#)
- ♦ [Section E.1.2, “<remove-value> without an Accompanying <add-value>,” on page 86](#)
- ♦ [Section E.1.3, “<remove-value> with an Accompanying <add-value>,” on page 86](#)
- ♦ [Section E.1.4, “<add-value> without a Prior <remove-value>,” on page 86](#)

E.1.1 <remove-all-values>

The following operations occur when a <remove-all-values/> element exists in a <modify-attr> command. This is a non-standard XDS Subscriber operation that is generate by a policy.

Delimit Mode: The driver obtains a list of all active values of the specified Infotype record. The driver delimits the validity of each instance (set ENDDA) to (current date -1). This is the standard SAP delimitation method. If BEGDA is equal to the current date, the value is deleted. This is also standard functionality.

Delete Mode: The driver obtains a list of all active values of the specified Infotype record and deletes each instance.

Change Mode: The driver obtains a list of all active values of the specified Infotype record and deletes each instance.

E.1.2 <remove-value> without an Accompanying <add-value>

The following operations occur when a <remove-value> element without an accompanying <add-value> element exists in a <modify-attr> command. This is the format of a standard Subscriber value remove XDS event.

Delimit Mode: The driver obtains a list of all active values of the specified Infotype record. The driver tries to match the existing values to the removed value. If a match is found, the driver delimits the validity of the matching value to (current date -1.)

Delete Mode: The driver obtains a list of all active values of the specified Infotype record. The driver tries to match the existing values to the removed value. If a match is found, the driver deletes the matching value.

Change Mode: The driver obtains a list of all active values of the specified Infotype record. The driver tries to match the existing values to the removed value. If a match is found, the driver deletes the matching value.

E.1.3 <remove-value> with an Accompanying <add-value>

The following operations occur when a <remove-value> element with an accompanying <add-value> element exists in a <modify-attr> command. This is the format of a standard Subscriber value change XDS format.

Delimit Mode: The driver obtains a list of all active values of the specified Infotype record. The driver tries to match the existing values to the removed value. If a match is found, the driver delimits the validity of the matching value to (current date -1.) If the added value is not already an active value, the added value is created.

Delete Mode: The driver obtains a list of all active values of the specified Infotype record. The driver tries to match the existing values to the removed value. If a match is found, the driver deletes the matching value. If the added value is not already an active value, the added value is created.

Change Mode: The driver obtains a list of all active values of the specified Infotype record. The driver tries to match the existing values to the removed value. If a match is found, the driver changes the matching value to the added value. If a match is not found, the driver deletes the removed value. If the added value is not already an active value, the added value is created.

E.1.4 <add-value> without a Prior <remove-value>

If the added value is not already an active value, the driver creates the added Infotype for all modes.

This functionality is only available on SAP R/3 version 4.6A or later and on all Web Application Server versions. On 4.5 systems (no support prior to 4.5B), the driver uses the BAPI_HRMMASTER_SAVE_REPL_MULT function for all operations. <remove-value> and <remove-

`all-value`> operations remove all values of the specified Communication Subtype. `<add-value>` operations remove all values of the Communication Subtype and create a new value with a BEGDA of (current date -1) and an ENDDA of 99991231.

E.2 Validity Date Modes

The driver contains configuration parameters that allow an administrator to specify how validity begin dates (BEGDA) and validity end dates (ENDDA) are set when new Communication or Internal Control Data values are created for an Employee object. The new settings are **Communication Validity Date Mode** and **Internal Data Validity Date Mode**. They allow two modes of operation:

Current Date Mode: This mode configures the driver to set validity dates in the same manner employed by all other previous versions of the driver. The driver sets the current date for the validity begin field (BEGDA) and sets the maximum SAP date for the validity end field (ENDDA).

Default Mode: This mode configures the driver to not set any BEGDA and ENDDA field values. When these values are not set, the default validity dating scheme of the SAP server is used to set these two field values. Standard SAP configuration sets the BEGDA value to the date that the Employee record was created and sets the ENDDA value to the maximum SAP date value.

F Trace Levels

The driver supports the following trace levels:

Table F-1 Supported Trace Levels

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

For information about setting driver trace levels, see [“Viewing Identity Manager Processes”](#) in the *NetIQ Identity Manager Entitlements Guide*.

