
NetIQ® Identity Manager™

Driver for SAP Portal 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	5
About NetIQ Corporation	7
1 Understanding the SAP Portal Driver	9
1.1 Terminology	9
1.2 Supported SAP Versions	9
1.3 Driver Concepts	9
1.4 Support for Standard Driver Features	10
1.4.1 Local Platforms	11
1.4.2 Remote Platforms	11
1.4.3 Entitlements	11
1.4.4 Password Synchronization	11
1.4.5 Account Tracking	11
1.4.6 Identity Manager Catalog Administrator	11
2 Installing the Driver Files	13
3 Creating a New Driver Object	15
3.1 Creating the Driver Object in Designer	15
3.1.1 Importing the Current Driver Packages	15
3.1.2 Installing the Driver Packages	16
3.1.3 Using Designer to Adjust the Driver Settings	19
3.1.4 Using Designer to Deploy the Driver Object	19
3.1.5 Using Designer to Start the Driver	20
3.2 Creating an Administrative User Account for the Driver	20
3.3 Activating the Driver	20
3.4 Adding Packages to an Existing Driver	21
4 Upgrading an Existing Driver	23
4.1 What's New in Version 4.0.1.0	23
4.2 Upgrading the Driver	23
4.2.1 Upgrading the Installed Packages	23
4.2.2 Applying the Driver Patch	24
5 Implementing the Preconfigured Entitlements	27
5.1 Entitlement Agents	27
5.2 User Account Entitlement	28
5.3 Portal Role Entitlement	28
5.4 Portal Group Entitlement	29
6 Configuring the SAP System	31
7 Security Best Practices	33
8 Managing the Driver	35
9 Troubleshooting the Driver	37
9.1 Authenticating to the SPML Service	37
9.2 Troubleshooting Driver Processes	37

9.3	Error LOGONID_TOO_LONG	37
9.4	Error PASSWORD_TOO_SHORT or ALPHANUM_REQUIRED_FOR_PSWD	37
9.5	Error Occurs when Uninstalling the Driver	38

A Driver Properties 39

A.1	Driver Configuration	39
A.1.1	Driver Module	40
A.1.2	Driver Object Password	40
A.1.3	Authentication	40
A.1.4	Startup Options	41
A.1.5	Driver Parameters	41
A.1.6	ECMAScript	43
A.1.7	Global Configurations	43
A.2	Global Configuration Values	43
A.2.1	Entitlements	44
A.2.2	Account Tracking	46
A.2.3	Process Logging	46
A.2.4	Managed System Information	47
A.2.5	SAP Portal Driver	48

B Trace Levels 49

About this Book and the Library

The *Identity Manager Driver for SAP Portal Implementation Guide* provides information about the Identity Manager driver for SAP Portal.

Intended Audience

This book provides information for SAP integrators and Identity Manager administrators.

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 Portal Driver

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

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

- ◆ [Section 1.1, “Terminology,” on page 9](#)
- ◆ [Section 1.2, “Supported SAP Versions,” on page 9](#)
- ◆ [Section 1.3, “Driver Concepts,” on page 9](#)
- ◆ [Section 1.4, “Support for Standard Driver Features,” on page 10](#)

1.1 Terminology

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

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

BAPI: Business APIs for the SAP business object types.

CUA: Central User Administration.

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

UME: User Management Engine.

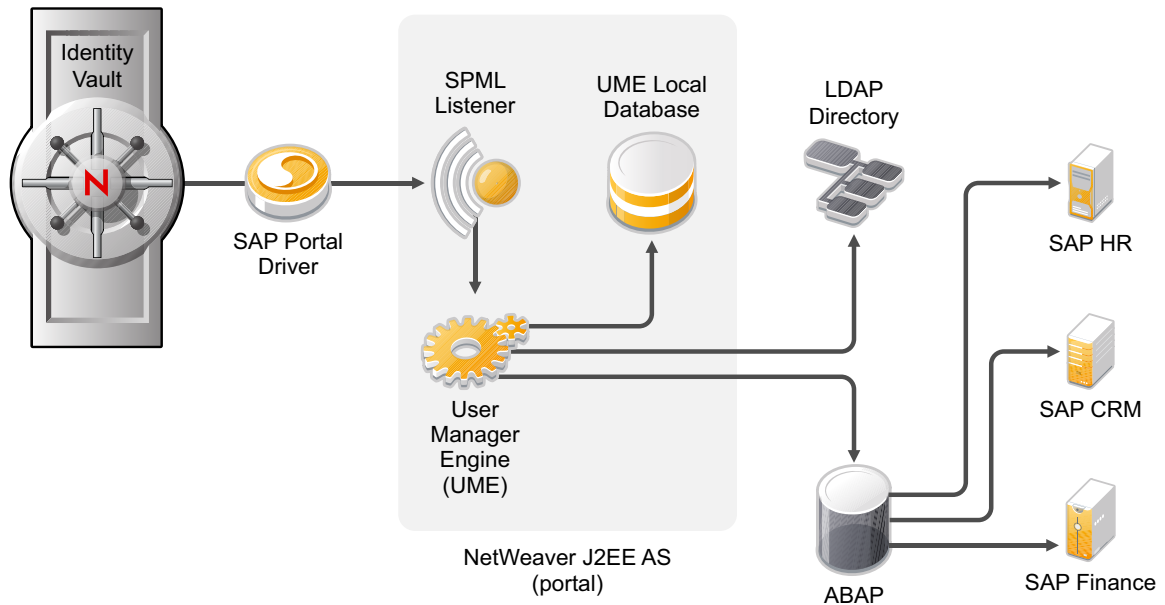
1.2 Supported SAP Versions

The SAP Portal driver supports SAP NetWeaver 7.x.

1.3 Driver Concepts

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

Figure 1-1 SAP Portal Driver



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

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

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

1.4 Support for Standard Driver Features

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

- ◆ [Section 1.4.1, "Local Platforms," on page 11](#)
- ◆ [Section 1.4.2, "Remote Platforms," on page 11](#)
- ◆ [Section 1.4.3, "Entitlements," on page 11](#)
- ◆ [Section 1.4.4, "Password Synchronization," on page 11](#)
- ◆ [Section 1.4.5, "Account Tracking," on page 11](#)
- ◆ [Section 1.4.6, "Identity Manager Catalog Administrator," on page 11](#)

1.4.1 Local Platforms

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

The SAP Portal driver can be installed on the same operating systems supported by the Metadirectory engine. For information, see [System Requirements for the Identity Manager Engine](#) in the [NetIQ Identity Manager Setup Guide](#).

1.4.2 Remote Platforms

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

The SAP Portal driver can be installed on the same operating systems supported by the Remote Loader. For information, see [System Requirements for the Remote Loader](#) in the [NetIQ Identity Manager Setup Guide](#).

1.4.3 Entitlements

Entitlements are a way to set up a list of criteria to grant or revoke access to resources for users, roles, and groups. The SAP Portal drivers contains three preconfigured entitlements. For more information, see [Chapter 5, "Implementing the Preconfigured Entitlements,"](#) on page 27.

1.4.4 Password Synchronization

The SAP Portal driver can synchronize passwords from the Identity Vault into the SAP NetWeaver server. The password synchronization is one way. For more information, see the [NetIQ Identity Manager Password Management Guide](#).

1.4.5 Account Tracking

Account Tracking allows you to manage all of the identities each user account has in each system connected to the Identity Vault. Account Tracking is a feature included with the Identity Reporting Module. For more information, see the [Administrator Guide to NetIQ Identity Reporting](#).

1.4.6 Identity Manager Catalog Administrator

The SAP Portal driver can be configured to work with the Identity Manager Catalog Administrator that allows you to map business roles to IT roles. Catalog Administrator is included with Identity Manager. For more information, see [Role and Resource Administration](#) in the [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#).

2 Installing the Driver Files

By default, the SAP Portal 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 3, "Creating a New Driver Object," on page 15](#)) or upgrade an existing driver's configuration (see [Chapter 4, "Upgrading an Existing Driver," on page 23](#)).

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

- ♦ Install the Metadirectory server (Metadirectory engine and drivers) on the SAP NetWeaver 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 Portal driver files to the SAP NetWeaver server. This assumes that you already have a Metadirectory server installed on another server in your environment. See the instructions in "[Installing Remote Loader](#)" in the *NetIQ Identity Manager Setup Guide*.

3 Creating a New Driver Object

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

- ♦ [Section 3.1, “Creating the Driver Object in Designer,” on page 15](#)
- ♦ [Section 3.2, “Creating an Administrative User Account for the Driver,” on page 20](#)
- ♦ [Section 3.3, “Activating the Driver,” on page 20](#)
- ♦ [Section 3.4, “Adding Packages to an Existing Driver,” on page 21](#)

3.1 Creating the Driver Object in Designer

The following sections provide steps for using Designer to create and configure a new SAP Portal driver.

- ♦ [Section 3.1.1, “Importing the Current Driver Packages,” on page 15](#)
- ♦ [Section 3.1.2, “Installing the Driver Packages,” on page 16](#)
- ♦ [Section 3.1.3, “Using Designer to Adjust the Driver Settings,” on page 19](#)
- ♦ [Section 3.1.4, “Using Designer to Deploy the Driver Object,” on page 19](#)
- ♦ [Section 3.1.5, “Using Designer to Start the Driver,” on page 20](#)

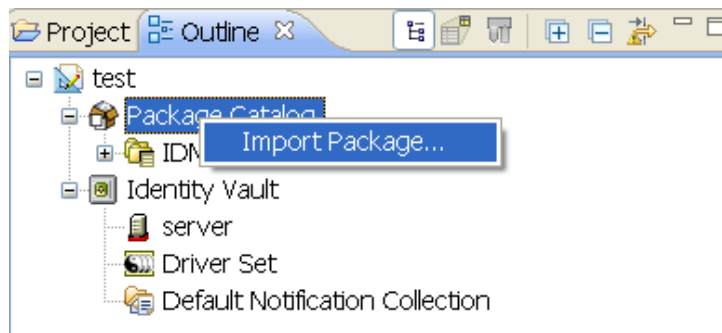
NOTE: You should not create driver objects by using the new Identity Manager 4.0 and later configuration files through iManager. This method of creating driver objects is no longer supported. To create drivers, you now need to use the new package management features provided in Designer.

3.1.1 Importing the Current Driver Packages

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

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

- 1 Open Designer.
- 2 In the toolbar, click **Help** > **Check for Package Updates**.
- 3 Click **OK** to update the packages
or
Click **OK** if the packages are up-to-date.
- 4 In the Outline view, right-click the Package Catalog.
- 5 Click **Import Package**.



- 6 Select any SAP Portal 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 message indicating that the package imported.
- 8 After the current packages are imported, continue with [Section 3.1.2, “Installing the Driver Packages,”](#) on page 16.

3.1.2 Installing the Driver Packages

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 Portal Base**, then click **Next**.
- 4 Select the optional features to install for the SAP Portal driver. All options are selected by default. The options are:

Entitlements: These packages contain the policies and entitlements required to enable the driver for account creation and management with entitlements.

Process File Logging: These packages contain the policies for creating a daily, rolling log file of SAP Business Operations.

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 [Administrator Guide to NetIQ Identity Reporting](#).

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

Account Tracking feature was introduced with NetIQ Compliance Management Platform. The Compliance Management Platform helps you mitigate risk, simplify business governance, and ensures compliance throughout the enterprise. The platform enables you to provision users based on how you do business, secure both Web and Client applications by granting access to users based upon provisioning policy, and monitor and validate user and system activity in real time with automated, policy-based corrective actions for non-compliant activities. For more information, see [NetIQ Compliance Management Platform product page](#).

- 5 After selecting the packages that you want, click **Next**.
- 6 (Conditional) If there are package dependencies for the packages you selected to install, you must install these dependencies to install the selected packages. Click **OK** to install the package dependencies.
- 7 (Conditional) Fill in the following fields on the Common Settings page, then click **Next**:

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

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

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

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

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.
- 8 On the Driver Information page, specify a name for the driver, then click **Next**.
- 9 Fill in the following fields to configure the driver, then click **Next**:

URL of the remote SPML Provisioning Service Point: Specify the URL of the remote SAP Portal SPML Provisioning Service Point.

For example: `http://my.sap.com:50000/spml/spmlservice`

Authentication ID: Specify the authentication ID for the remote SAP Portal SPML Provisioning Service Point. For more information, see [Section 3.2, "Creating an Administrative User Account for the Driver," on page 20](#).

Authentication Password: Specify the password for the Authentication ID, then reenter the password for verification.
- 10 Fill in the following fields for Remote Loader information:

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

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

Host Name: Specify the IP address or DNS name of the server where the Remote Loader is installed and running.

Port: Specify the port number for this driver. Each driver connects to the Remote Loader on a separate port. The default value is 8090.

Remote Loader Password: Specify a password to control access to the Remote Loader. It must be the same password that is specified as the Remote Loader password on the Remote Loader.

Driver Password: Specify a password for the driver to authenticate to the Metadirectory server. It must be the same password that is specified as the driver object password on the Remote Loader.
- 11 (Conditional) Fill in the following fields on the Process Logging page to create the daily, rolling log file of SAP Business Operations, then click **Next**:

Show Process Logging Options: Select **show** to display the options to configure the rolling log file of SAP Business Operations.

Enable process logging: Select **true** to enable process logging, then fill in the following fields:

- ♦ **Daily log file:** Select **true** to create the daily log file with the format of `<YYYYmmDD>-<driver-name>-<drv.proclog.logfile>`.
- ♦ **Log file name:** Specify the process log filename.
- ♦ **Log file directory:** Specify the directory where the log file is created.

- 12 (Conditional) Fill in the following fields on the Managed System Information page, then click **Next**:

This page is displayed only if you selected to install the Data Collection and Account Tracking packages.

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

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

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

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

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

- 13 (Conditional) Fill in the following fields to define the classification of the SAP Portal System, then click **Next**:

This page is displayed only if you selected to install the Data Collection and Account Tracking packages.

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

- ♦ Mission-Critical
- ♦ Vital
- ♦ Not-Critical
- ♦ Other

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

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

- ♦ Development
- ♦ Test
- ♦ Staging
- ♦ Production
- ♦ Other

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

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


- 15 If this basic driver configuration fits your needs, continue with [Section 3.1.4, "Using Designer to Deploy the Driver Object,"](#) on page 19.

or

If you need to customize the driver settings, continue with [Section 3.1.3, "Using Designer to Adjust the Driver Settings,"](#) on page 19.


3.1.3 Using Designer to Adjust the Driver Settings

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

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select **Properties**.
This opens the properties page for the driver. Use the information in [Appendix A, "Driver Properties," on page 39](#) to adjust the configuration.
- 3 After you have customized the driver for your environment, you must deploy the driver to the Identity Vault. Proceed to [Section 3.1.4, "Using Designer to Deploy the Driver Object," on page 19](#).

3.1.4 Using Designer to Deploy 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 5](#); otherwise, specify the following information to authenticate:
Host: Specify the IP address or DNS name of the server hosting the Identity Vault.
Username: Specify the DN of the user object used to authenticate to the Identity Vault.
Password: Specify the user's password.

- 4 Click **OK**.
- 5 Read through the deployment summary, then click **Deploy**.
- 6 Read the message indicating the success, then click **OK**.
- 7 Click **Define Security Equivalence** to assign rights to the driver.

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

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


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

- 8 Click **Exclude Administrative Roles** to exclude users that should not be synchronized.
You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.
 - 8a Click **Add**, then browse to and select the user object you want to exclude, then click **OK**.
 - 8b Repeat [Step 8a](#) for each object you want to exclude.
 - 8c Click **OK**.
- 9 Click **OK**.
- 10 Continue with [Section 3.1.5, "Using Designer to Start the Driver," on page 20](#).

3.1.5 Using Designer to Start the Driver

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

To start the driver after the driver is deployed:

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

For information about management tasks with the driver, see [Chapter 8, “Managing the Driver,”](#) on [page 35](#).

3.2 Creating an Administrative User Account for the Driver

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

To create an administrative user for the driver:

- 1 Log into the SAP Portal as the Administrator.
- 2 Search for the Administrator user account in Identity Management.
- 3 Select the Administrator user account.
- 4 Click **Copy to New User** to create a user with the same rights as the Administrator.
- 5 Specify the **Logon ID** for the administrative user.
- 6 Specify a password for this user in the **Define Initial Password** field.
- 7 Click **Save** to save the new user.
- 8 Log out of the portal.
- 9 Log back into the portal as the new administrative user.
This prompts the user to set a permanent password.
- 10 Specify this user in the [“Authentication ID:” on page 41](#), then update the password in the [“Authentication Password:” on page 42](#) on the Subscriber settings of the driver.

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

3.3 Activating the Driver

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

- ♦ Identity Manager driver for SAP HR

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

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 Portal 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 will be 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](#).

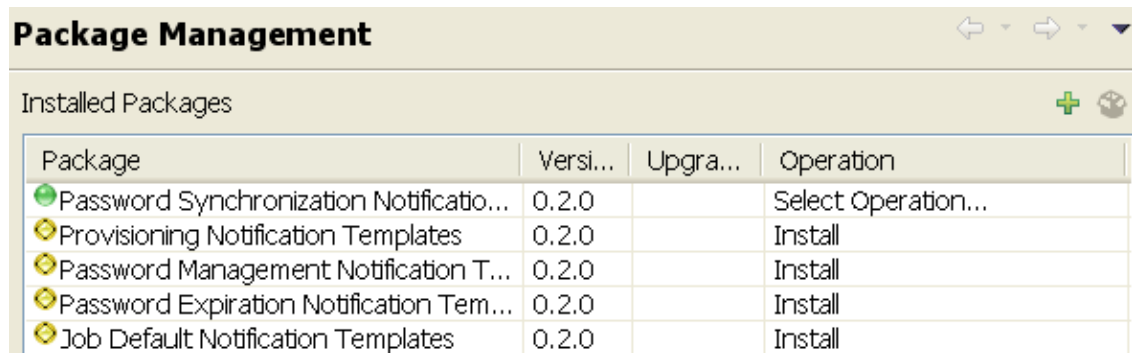
3.4 Adding Packages to an Existing Driver

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.

Package Management			
Installed Packages			
Package	Versi...	Upgra...	Operation
Job Default Notification Templates	0.2.0		Select Operation...
Password Expiration Notification Tem...	0.2.0		Select Operation...
Password Management Notification T...	0.2.0		Select Operation...
Password Synchronization Notificatio...	0.2.0		Select Operation...
Provisioning Notification Templates	0.2.0		Select Operation...

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

4 Upgrading an Existing Driver

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

- ♦ [Section 4.1, “What’s New in Version 4.0.1.0,” on page 23](#)
- ♦ [Section 4.2, “Upgrading the Driver,” on page 23](#)

4.1 What’s New in Version 4.0.1.0

Version 4.0.1.0 of the driver does not include any new features.

4.2 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 4.2.1, “Upgrading the Installed Packages,” on page 23](#)
- ♦ [Section 4.2.2, “Applying the Driver Patch,” on page 24](#)

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

4.2.1 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*.

4.2.2 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 Portal 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, `IDM45_SAPPortal_4010.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 command in a command prompt:

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

For example, `rpm -Uvh <IDM45_SAPPortal_4010.zip>/linux/novell-DXMLsappt.rpm`

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

For example, copy `SAPPortalShim.jar` file from `<Extracted IDM45_SAPPortal_4010.zip>\windows` to `<IdentityManager installation>\RemoteLoader\64bit\lib` folder.

- 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, run the following script in a command prompt:

```
*****
#!/bin/sh
#set -x
#© 2017 NetIQ Corporation and its affiliates. All Rights Reserved
clear
echo "=====
echo " Installing packages... "
echo "=====
if [ "$1" == "" ] ; then
    exit
fi
pkgfile=$1
ROOTDIR="/local/home/bshidm/base/bshappl/edir"
RPMDB=$ROOTDIR/rpm
if [ ! -d "$RPMDB" ] ; then
    mkdir $RPMDB
fi
# create rpm database if it doesn't exist
if [ ! -f $RPMDB/__db.000 ]
then
# mkdir -p $RPMDB
rpm --dbpath "$RPMDB" --initdb
fi
RPM_FLAGS="--dbpath $RPMDB -Uvh --relocate=/etc=$ROOTDIR/etc --relocate=/
opt=$ROOTDIR/opt --relocate=/opt/novell/eDirectory/lib64=$ROOTDIR/opt/novell/
eDirectory/lib64 --relocate=/var=$ROOTDIR/var --badreloc --nodeps --
replacefiles --force"
rpm $RPM_FLAGS $pkgfile
```

5 Implementing the Preconfigured Entitlements

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

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

- ◆ [Section 5.1, “Entitlement Agents,” on page 27](#)
- ◆ [Section 5.2, “User Account Entitlement,” on page 28](#)
- ◆ [Section 5.3, “Portal Role Entitlement,” on page 28](#)
- ◆ [Section 5.4, “Portal Group Entitlement,” on page 29](#)

5.1 Entitlement Agents

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

- ◆ **Role-Based Entitlements (RBE):** Manages entitlements based on the events that occur in the Identity Vault. This agent is used for simple automation. For example, when a user is added to the HR system, the user is automatically granted accounts in other systems. This requires an Entitlements driver created with policies that define the desired action. For instructions, see the “[Implementation Checklist](#)” in the *NetIQ Identity Manager Entitlements Service Driver Implementation Guide*.
- ◆ **Workflow:** Manages entitlements through provisioning workflows. This agent is used when approvals are required. For example, when a user is added to the HR system, the manager must approve the accounts for the user. This requires a workflow that contains the desired actions. For instructions, see “[Configuring and Managing Provisioning Workflows](#)” in the *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications*.
- ◆ **Roles Based Provisioning Module (RBPM):** Manages entitlements based on roles that are assigned to users. For example, when a user is added to the Accounting role, the user automatically receives all accounts associated with the Accounting role. This requires that the Roles Based Provisioning Module be installed and configured for roles. For installation instructions, see the “[System Requirements for the Identity Applications](#)” in the *NetIQ Identity Manager Setup Guide*.

5.2 User Account Entitlement

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

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

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

To enable this entitlement:

- 1 Verify that an entitlement agent that contains your list of criteria to grant or revoke a user's access to resources in SAP exists. For more information, see [Section 5.1, "Entitlement Agents," on page 27](#).
- 2 If you have an existing driver, continue with [Step 3](#); otherwise, during the creation of a driver, select **True** for the **Use User Account Entitlement** option.
This sets the entitlement GCVs to True.
- 3 Access the GCVs page for the driver.
- 4 Select **show** for the **Show entitlements configuration** option.
- 5 Enable the user account entitlement by selecting **true**.
- 6 Select what to do when the user account entitlement is revoked by indicating whether you want the account disabled, deleted, or nothing done to the account.
- 7 Click **OK** to save the changes.

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

5.3 Portal Role Entitlement

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

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

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

To manually enable this entitlement:

- 1 Verify that an entitlement agent that contains your list of criteria to grant or revoke Portal role assignments in SAP exists. For more information, see [Section 5.1, “Entitlement Agents,” on page 27](#).
- 2 If you have an existing driver continue with [Step 3](#); otherwise, during the creation of a driver, select **True** for the **Use Portal Role Entitlement** option.
This sets the entitlement GCVs to True.
- 3 Access the GCVs page for the driver.
- 4 Select **True** for the **User Portal Role Entitlement** option.
- 5 Click **OK** to save the changes.

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

5.4 Portal Group Entitlement

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

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

To manually enable this entitlement:

- 1 Verify that an entitlement agent that contains your list of criteria to grant or revoke Portal group assignments in SAP exists. For more information, see [Section 5.1, “Entitlement Agents,” on page 27](#).
- 2 If you have an existing driver, continue with [Step 3](#); otherwise, during the creation of a driver, select **True** for the **Use Portal Group Entitlement** option.
This sets the entitlement GCVs to True.
- 3 Access the GCVs page on the driver.
- 4 Select **True** for the **User Portal Group Entitlement** option.
- 5 Click **OK** to save the changes.

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

6 Configuring the SAP System

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

- ♦ Verify that the [SPML](#) listener on the SAP Web Application server is available and working. For more information, see the [SAP Netweaver Documentation Web page \(http://help.sap.com/content/documentation/netweaver/index.htm\)](http://help.sap.com/content/documentation/netweaver/index.htm).
- ♦ Create an administrative user for the driver to use instead of using the SAP Administrator account. For more information, see [Section 3.2, "Creating an Administrative User Account for the Driver,"](#) on page 20.

7 Security Best Practices

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

For additional information about securing your Identity Manager system, see the [NetIQ Identity Manager Security Guide](#).

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

To create a secure connection:

- 1 Create a server certificate in iManager:
 - 1a In the **Roles and Tasks** view, click **NetIQ Certificate Server > Create Server Certificate**.
 - 1b Browse to and select the server object where the SAP Portal driver is installed.
 - 1c Specify a certificate nickname.
 - 1d Select **Standard** as the creation method, then click **Next**.
 - 1e Click **Finish**, then click **Close**.
- 2 Export this self-signed certificate from the certificate authority in eDirectory.
 - 2a In the **Roles and Tasks** view, click **Directory Administration > Modify Object**.
 - 2b Select your tree's certificate authority object, then click **OK**.

It is usually found in the Security container and is named something like *TREENAME CA.Security*.
 - 2c Click **Certificate > Self Signed Certificate**.
 - 2d Click **Export**.
 - 2e When you are asked if you want to export the private key with the certificate, click **No**, then click **Next**.
 - 2f Depending on the client to be accessing the Web service, select either **File in binary DER format** or **File in Base64 format** for the certificate, then click **Next**.

If the client uses a Java-based keystore or trust store, then you can choose either format.
 - 2g Click **Save the exported certificate to a file**.
 - 2h Click **Save** and browse to a known location on your computer.
 - 2i Click **Save**, then click **Close**.
- 3 Import the self-signed certificate into the client's trust store:
 - 3a Use the keytool executable that is included with any Java JDK.

For more information on keytool, see [Keytool - Key and Certificate Management Tool \(http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html\)](http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html).
 - 3b Import the certificate into your trust store or create a new trust store by entering the following command at a command prompt:

```
keytool -import -file name_of_cert_file -trustcacerts -noprompt  
-keystore filename -storepass password
```

For example:

```
keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore  
dirxml.keystore -storepass novell
```

- 4 Configure the Subscriber channel to use the trust store you created in [Step 3](#):
 - 4a In iManager, in the **Roles and Tasks** view, click **Identity Manager > Identity Manager Overview**.
 - 4b Locate the driver set containing the SAP Portal driver, then click the driver's icon to display the Identity Manager Driver Overview page.
 - 4c On the Identity Manager Driver Overview page, click the driver's icon again, then scroll to **Subscriber Settings**.
 - 4d In the **Keystore File** setting, specify the path to the trust store you created in [Step 3 on page 33](#).
- 5 Click **Apply**, then click **OK**.

8 Managing the Driver

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

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

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

9 Troubleshooting the Driver

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

- ♦ [Section 9.1, “Authenticating to the SPML Service,” on page 37](#)
- ♦ [Section 9.2, “Troubleshooting Driver Processes,” on page 37](#)
- ♦ [Section 9.3, “Error LOGONID_TOO_LONG,” on page 37](#)
- ♦ [Section 9.4, “Error PASSWORD_TOO_SHORT or ALPHANUM_REQUIRED_FOR_PSWD,” on page 37](#)
- ♦ [Section 9.5, “Error Occurs when Uninstalling the Driver,” on page 38](#)

9.1 Authenticating to the SPML Service

If the driver is not connecting to the [UME](#), authenticate to the [SPML](#) service to verify if it is available and communicating.

9.2 Troubleshooting Driver Processes

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

9.3 Error LOGONID_TOO_LONG

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

9.4 Error PASSWORD_TOO_SHORT or ALPHANUM_REQUIRED_FOR_PSWD

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

9.5 Error Occurs when Uninstalling the Driver

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

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

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

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

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

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

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

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

For information about uninstalling the driver, see [“Uninstalling the Identity Manager Engine”](#) in the *NetIQ Identity Manager Setup Guide*.

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the SAP Portal driver. These are the only unique properties for this driver. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to “[Driver Properties](#)” in the *NetIQ Identity Manager Driver Administration Guide* for information about the common properties.


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

The information is presented from the viewpoint of Designer.


- ♦ [Section A.1, “Driver Configuration,”](#) on page 39
- ♦ [Section A.2, “Global Configuration Values,”](#) on page 43

A.1 Driver Configuration

In Designer:

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

In iManager:

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

By default, the properties page opens with the **Driver Configuration** tab displayed.

The Driver Configuration options are divided into the following sections:

- ♦ [Section A.1.1, “Driver Module,”](#) on page 40
- ♦ [Section A.1.2, “Driver Object Password,”](#) on page 40
- ♦ [Section A.1.3, “Authentication,”](#) on page 40
- ♦ [Section A.1.4, “Startup Options,”](#) on page 41
- ♦ [Section A.1.5, “Driver Parameters,”](#) on page 41

- ♦ [Section A.1.6, “ECMAScript,” on page 43](#)
- ♦ [Section A.1.7, “Global Configurations,” on page 43](#)

A.1.1 Driver Module

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

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

The name of the Java class is: `com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim`

Native: This option is not used with the SAP Portal driver.

Connect to Remote Loader: Used when the driver is connecting remotely to the connected system. Designer includes two suboptions:

- ♦ **Driver Object Password:** Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.
- ♦ **Include in documentation:** Includes information on the Remote Loader client configuration when Designer generates documentation for the SAP Portal driver.

A.1.2 Driver Object Password

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

A.1.3 Authentication

The authentication options store the information required to authenticate to the connected system.

Authentication ID: This field is not used for the SAP Portal driver. The authentication field is in the Subscriber settings documented in the [URL of remote SPML Provisioning Service Point](#).

Authentication Context: This field is not used for the SAP Portal driver.

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

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

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

Cache limit (KB): Specify the maximum event cache file size (in KB). If this option is set to zero, the file size is unlimited. Click **Unlimited** to set the file size to unlimited in Designer.

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

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

A.1.4 Startup Options

The Startup options allow 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 option is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

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

The parameters are presented by category:

Driver Settings

XML element handling specific for Identity Manager (<nds>, <input>, <output>): Enables the Identity Manager engine to handle XML elements.

- ♦ **Remove/add elements:** Enables the driver shim to remove and add the required XML elements of <nds>, <input>, and <output>. These required elements are removed from the XML documents sent to the application and the elements are added to the XML documents received from the application before presenting the document to the Identity Manager engine.
- ♦ **Pass elements through:** Turns off XML element handling.

Custom Java Extensions: Enables custom Java extensions to extend the driver shim's functionality. Select **Show** to enable the custom Java extensions. Select **Hide** if you don't have any custom Java extensions.

Subscriber Settings

Portal Authentication Information: Fill in the following fields for the SAP Portal authentication information:

- ♦ **URL of remote SPML Provisioning Service Point:** Specify the URL for the remote [SPML Provisioning Service Point \(PSP\)](#). A PSP is a software component that listens for, processes, and returns the results for well-formed [SPML](#) requests.

For example: `http://my.sap.com:50000/spml/spmlservice`

- ♦ **Authentication ID:** Specify the authentication ID for the remote [SPML Provisioning Service Point](#).

- ♦ **Authentication Password:** Specify the password for the authentication ID.

Show Advanced Options: Select **Show** to display the advanced configuration options for the SAP Portal driver.

Truststore file: When the remote server is configured to provide server authentication, this is the path and the name of the keystore file which contains trusted certificates.

For example: `c:\security\trustore`

Leave this field blank when server authentication is not used.

Set mutual authentication parameters: Select **Show** if you want to set mutual authentication information.

- ♦ **Keystore file:** Specify the path and name of the keystore file, if the remote server is configured to provide mutual authentication. For example: `c:\security\keystore`. Leave this field blank when mutual authentication is not used.
- ♦ **Keystore password:** Specify the keystore file password, if the remote server is configured to provide mutual authentication. Leave this field blank when mutual authentication is not used.

Proxy host and port: When a proxy host and port are used, specify the host address and the host port. Choose an unused port number on your server. Otherwise, leave this field blank.

For example: `192.10.1.3:8180`

Handle HTTP session cookies: Some HTTP applications set cookies and expect them to be present on future requests. Select **Handle Cookies** if you want the driver to keep track of session cookies. Cookies are only kept until the driver is stopped.

Process empty subscriber documents: Select whether or not the Subscriber channel should send empty documents to the target application. Documents could be empty if policies or style sheets strip the XML without vetoing the command. Select **Ignore** to block empty documents from being sent to the target application.

HTTP errors to retry: List the HTTP error codes that should return a retry status. Must be a list of integers separated by spaces.

Customize HTTP Request-Header Fields: Select **Show** if you want to set mutual authentication information. Use the following fields to define the custom HTTP request-header:

- ♦ **Authorization:** Select **Use** to add the Authentication ID and the password from the Authentication section into this request-header field.
 - ♦ **Key:** Specify Authorization as the keyword for the HTTP request-header field.
 - ♦ **Value:** Specify the value to associate with the keyword in an HTTP request-header field.
- ♦ **Context Type:** Select **Use** to add the media type to the HTTP request-header field to comply with RFC 2376.
 - ♦ **Key:** Specify Content-Type to set an HTTP request-header field.
 - ♦ **Value:** Specify `text/xml; charset=utf-8` as the value of the keyword in the HTTP request-header field.
- ♦ **SOAPAction:** Select **Use** to enable the SOAPAction HTTP request header field to indicate the intent of the SOAP HTTP request.
 - ♦ **Key:** Specify SOAPAction to set an HTTP request-header field.
 - ♦ **Value:** Specify `#batchRequest` as the value of the HTTP request-header.

Optional Request-Header: When required, specify an additional request-header that is unique to your situation.

Publisher Options

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

A.1.6 ECMAScript

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

A.1.7 Global Configurations


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

A.2 Global Configuration Values

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

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

To access the driver's GCVs in iManager:

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

To access the driver's GCVs in Designer:

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

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

The Global Configuration Values are divided into categories:

- ◆ [Section A.2.1, “Entitlements,” on page 44](#)
- ◆ [Section A.2.2, “Account Tracking,” on page 46](#)
- ◆ [Section A.2.3, “Process Logging,” on page 46](#)
- ◆ [Section A.2.4, “Managed System Information,” on page 47](#)
- ◆ [Section A.2.5, “SAP Portal Driver,” on page 48](#)

A.2.1 Entitlements

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

- ◆ [“Entitlements Options” on page 44](#)
- ◆ [“Data Collection” on page 45](#)
- ◆ [“Role Mapping” on page 45](#)
- ◆ [“Resource Mapping” on page 45](#)
- ◆ [“Parameter Format” on page 45](#)
- ◆ [“Entitlement Extensions” on page 46](#)

Entitlements Options

Entitlements act like an ON/OFF switch to control account access. For more information about entitlements, see the [NetIQ Identity Manager Entitlements Guide](#).

Show entitlements configuration: Select **show** to display the configuration options for the entitlements.

Use User Account Entitlement: Entitlements act like an on/off switch to control access. When the driver is enabled for entitlements, accounts are created and removed or disabled only when the account entitlement is granted to or revoked from users.

Select **True** to enable the user account entitlement. You must have an entitlement agent configured in your environment.

Action when account entitlement revoked: Specifies which action is taken in the SAP system when a User Account Entitlement is revoked. The options are to disable the account or to delete the account.

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

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

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

Data Collection

Data collection enables the Identity Report Module to gather information to generate reports. For more information, see the [Administrator Guide to NetIQ Identity Reporting](#).

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

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

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

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

Role Mapping

The Identity Manager Catalog Administrator allows you to map business roles with IT roles. For more information, see the [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#).

Enable role mapping: If **Yes**, this driver is visible to Catalog Administrator.

Allow mapping of user accounts: If **Yes**, allows mapping of user accounts in Catalog Administrator. An account is required before a role, profile, or license can be granted through Catalog Administrator.

Allow mapping of groups: If **Yes**, allows mapping of groups in Catalog Administrator.

Allow mapping of roles: If **Yes**, allows mapping of roles in Catalog Administrator.

Resource Mapping

The Roles Based Provisioning Module allows you to map resources to users. For more information, see the [NetIQ Identity Manager - User's Guide to the Identity Applications](#).

Enables resource mapping: If **Yes**, this driver is visible to the Roles Based Provisioning Module.

Allow mapping of user accounts: If **Yes**, allows mapping of user accounts in the Roles Based Provisioning Module. An account is required before a role, profile, or license can be granted.

Allow mapping of groups: If **Yes**, allow mapping of groups in the Roles Based Provisioning Module.

Allow mapping of roles: If **Yes**, allows mapping of roles in the Roles Based Provisioning Module.

Parameter Format

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

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

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

Entitlement Extensions

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

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

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

A.2.2 Account Tracking

Account tracking is part of the Identity Reporting Module. For more information, see the [Administrator Guide to NetIQ Identity Reporting](#).

Show Account Tracking Configuration: Select **show** to display the account tracking settings. If you changes these settings from the default, you risk disabling the account tracking feature.

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

Realm: Specifies the name of the realm, security domain, or namespace in which the account name is unique.

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

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

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

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

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

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

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

A.2.3 Process Logging

These GCVS enable the policies for creating a daily, rolling log file of SAP Business Operations.

Show Process Logging Options: Select **show** to display the options to configure a rolling log file of the SAP Business Operations.

Enable process logging: If **true**, it enables process logging, then fill in the following fields:

- ♦ **Daily log file:** Select **true** to creating the daily log file with the format of `<YYYYmmDD>-<driver-name>-<drv.proclg.logfile>`.
- ♦ **Log file name:** Specify the process log file name.
- ♦ **Log file directory:** Specify the directory where the log file is created.

A.2.4 Managed System Information

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

- ◆ [“General Information” on page 47](#)
- ◆ [“System Owner” on page 47](#)
- ◆ [“System Classification” on page 47](#)
- ◆ [“Connection and Miscellaneous Information” on page 48](#)

General Information

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

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

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

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

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

System Owner

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

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

System Classification

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

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

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

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

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

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

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 that are necessary for reporting to work. If you make any changes, reporting stops working.

A.2.5 SAP Portal Driver

At this time, there are no defined GCVs specified for the SAP Portal driver.

B Trace Levels

The driver supports the following trace levels:

Table B-1 Supported Trace Levels

Level	Description
0	No debugging
1–3	Identity Manager messages. Higher trace levels provide more detail
4	Previous level plus Remote Loader, driver, driver shim, and driver connection messages, driver parameters, driver security, driver schema, request and response XML.

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

