



NetIQ® Identity Manager Driver for SAP HANA Implementation Guide

May 2024

Legal Notice

Copyright 2009 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>).

About this Book and the Library

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

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

For more information about the library for Identity Manager, see the following resources:

- ♦ [Identity Manager documentation website \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/)
- ♦ [Identity Manager drivers documentation website \(https://www.netiq.com/documentation/identity-manager-49-drivers/\)](https://www.netiq.com/documentation/identity-manager-49-drivers/)

Contents

About this Book and the Library	3
1 Understanding the SAP HANA Driver	7
Driver Concepts	7
How the Driver Works	7
Support for Standard Driver Features	8
Local Platforms	8
Remote Platforms	9
Supported Operations	9
Support for Password Synchronization	9
Supported Pagination techniques	9
2 Installing and Configuring the SAP HANA Driver	11
SAP HANA Driver Packages	11
Checklist for Installing and Configuring the Driver	12
Installing the Driver Files	12
Installing the Driver Files as a Root User	12
Installing the Driver Files as a Non-Root User	13
Configuring Remote Loader for the Driver Instance	13
Creating the Driver Object	14
Importing the Current Driver Packages	14
Installing and Configuring the Driver Object	14
Configuring Entitlements	17
Fetching Entitlements from SAP HANA Cloud Database	17
Deploying the Driver Object	18
Starting the Driver	19
Activating the Driver	19
3 Attributes Mapping & Filtering	21
User Attributes	21
User Group Attributes	21
Role Attributes	22
Attribute Filter Settings	22
User Attributes Filter Settings	22
User Group Filter Settings	23
Role Filter Settings	23
4 Securing Communication	25
5 Update User with Minimum Rights	27
Create a System User	27
Grant Roles	27

A	Driver Properties	29
	Driver Configuration	29
	Driver Module	29
	Driver Object Password	30
	Authentication	30
	Startup Option	30
	Driver Parameters	31
	Global Configuration Values	31
B	Trace Level	35
C	IDV Schema Extension	37
D	IDV Proposed Structure	39

1 Understanding the SAP HANA Driver

The Identity Manager Driver for SAP HANA (High-performance Analytic Application) synchronizes data between Identity Vault and SAP HANA database. SAP HANA is a single suite that combines the HANA Database, Data Modeling, HANA Administration, and Data Provisioning. The driver supports the Subscriber and Publisher channels, uses filters to control objects and attributes, and uses policies to control data.

SAP HANA Cloud provides a single place to access, store, and process all enterprise data in real time. SAP HANA Cloud is a single database as a service (DBaaS) foundation. It is a cloud-native platform that reduces the complexity of multi-cloud or hybrid system landscapes. SAP HANA Cloud provides all of the advanced SAP HANA technologies for multi-model data processing in-memory. The SAP HANA Cloud allows you to consume the SAP HANA database from applications running on SAP Business Technology Platform, as well as from applications running on premise or other cloud services using the standard SAP HANA clients. The SAP HANA Cloud provides simplified data access to connect all your information without the need to have all data loaded into a single storage solution.

Every SAP HANA Cloud, SAP HANA database instance is equivalent to a single tenant database. For multiple databases, create multiple SAP HANA database instances. Using SAP HANA Cloud Central or the command-line interface, you can create and manage SAP HANA Cloud instances in your sub-account.

This section provides the following information on the SAP HANA driver:

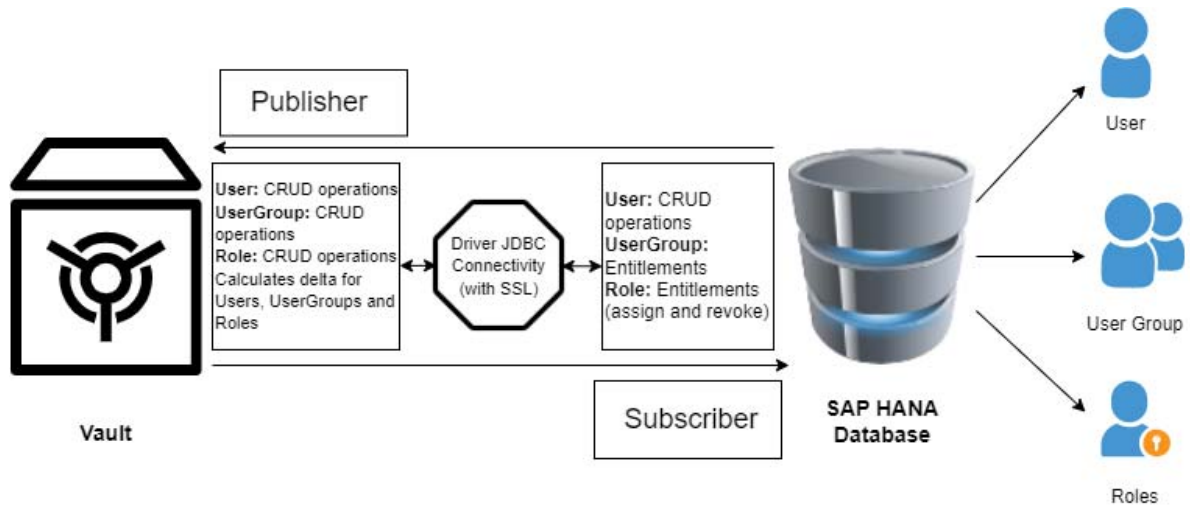
- ♦ [“Driver Concepts” on page 7](#)
- ♦ [“Support for Standard Driver Features” on page 8](#)

Driver Concepts

How the Driver Works

The following diagram illustrates the bi-directional relationship between Identity Manager and the connected application.

Figure 1-1 SAP HANA Driver Architecture



The SAP HANA driver supports User, User Group and Roles. It uses JDBC and SSL connection to create and configure for secured communication. Subscriber channel supports all the CRUD (create, read, update, and delete) operations for Users. User Group and Roles operations are supported using Entitlements.

Publisher Channel supports all the CRUD operations for Users, User Groups and Roles.

Since SAP HANA does not provide any delta changes, we use our own generic delta computation module. Also we build a wrapper to calculate these delta changes. SAP HANA supports offset pagination as well.

Support for Standard Driver Features

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

- ♦ [“Local Platforms” on page 8](#)
- ♦ [“Remote Platforms” on page 9](#)
- ♦ [“Supported Operations” on page 9](#)
- ♦ [“Support for Password Synchronization” on page 9](#)
- ♦ [“Supported Pagination techniques:” on page 9](#)

Local Platforms

A local installation is an installation of the driver on the Metadirectory server. You can install the SAP HANA driver on the operating systems supported for the Metadirectory server.

For information about the operating systems supported for the Metadirectory server, see [Considerations for Installing Drivers with the Identity Manager Engine](#) in the [NetIQ Identity Manager Overview and Planning Guide](#).

Remote Platforms

The SAP HANA driver can use the Remote Loader service to run on a server other than the Metadirectory server. You can install the SAP HANA driver on the operating systems supported for the Remote Loader.

For information about the supported operating systems, see [NetIQ Identity Manager Setup Guide for Linux](#).

Supported Operations

The SAP HANA driver supports the following operations on the Publisher and Subscriber channel:

- ♦ Publisher Channel
 - ♦ Users: Publisher Channel supports add, modify, delete and query operations for users.
 - ♦ User Group: Publisher Channel supports add, modify, delete and query operations for users groups.
 - ♦ Roles Operations: Publisher Channel supports add, modify, delete and query operations for roles.
- ♦ Subscriber Channel
 - ♦ Users: Subscriber Channel supports add, modify, delete, migrate and query operations for users.
 - ♦ User Group: Subscriber Channel supports query operations, adding and removing members using Entitlements.
 - ♦ Roles Operations: Subscriber Channel supports query operations, assigning and revoking operations using Entitlements.

Support for Password Synchronization

The SAP HANA driver supports password synchronization only in subscriber channel. The password set for the user must meet the password policy criteria defined in SAP HANA. For more information see, [Password Policy Configuration Options \(https://help.sap.com/docs/SAP_HANA_PLATFORM/b3ee5778bc2e4a089d3299b82ec762a7/61662e3032ad4f8dbdb5063a21a7d706.html\)](https://help.sap.com/docs/SAP_HANA_PLATFORM/b3ee5778bc2e4a089d3299b82ec762a7/61662e3032ad4f8dbdb5063a21a7d706.html)

Supported Pagination techniques:

SAP HANA driver follows pagination technique that uses an Offset Pagination. It updates paging parameter with page size.

2 Installing and Configuring the SAP HANA Driver

This section contains information about installing and configuring the SAP HANA driver.

The installation and configuration process for the driver varies depending on whether you want to install the driver with the Identity Manager server or with the Remote Loader. After installing the driver, you must manually activate it. For more information, see [“Activating the Driver” on page 19](#).

The following sections provide instructions to create the driver:

- ♦ [“SAP HANA Driver Packages” on page 11](#)
- ♦ [“Checklist for Installing and Configuring the Driver” on page 12](#)
- ♦ [“Installing the Driver Files” on page 12](#)
- ♦ [“Creating the Driver Object” on page 14](#)
- ♦ [“Configuring Entitlements” on page 17](#)
- ♦ [“Deploying the Driver Object” on page 18](#)
- ♦ [“Starting the Driver” on page 19](#)
- ♦ [“Activating the Driver” on page 19](#)

SAP HANA Driver Packages

The following packages are available for this driver:

Name	Package Name	Description
SAP HANA Base Configuration	SAPHANABASE	This package contains the base configuration. It is a mandatory package.
SAP HANA Default Configuration	SAPHANADFG	These packages contain the default configuration information for the SAP HANA. Always leave this package selected.
SAP HANA Driver Entitlements Package Configuration	SAPHANAENT	This package is used for synchronizing entitlements.
SAP HANA Driver Group and Role Synchronization	SAPHANAGNR	This package is used for synchronizing roles and groups.
SAP HANA Driver Password Synchronization	SAPHANAPSYNC	This package is used for password synchronizing

Checklist for Installing and Configuring the Driver

Use the following checklist to ensure that you complete all of the tasks required to set up.

- ♦ Ensure that your environment meets the requirements for installing and configuring the SAP HANA driver. For more information, see [Chapter 1, “Understanding the SAP HANA Driver,” on page 7](#).
- ♦ Install the driver files on the Identity Manager engine or on a Remote Loader server. For more information, see [“Installing the Driver Files” on page 12](#).
- ♦ Ensure that you have the appropriate packages installed and imported for the driver. For more information, see [“Importing the Current Driver Packages” on page 14](#).
- ♦ Deploy the driver to the Identity Vault. For more information, see [“Deploying the Driver Object” on page 18](#).
- ♦ Start the driver. For more information, see [“Starting the Driver” on page 19](#).

Installing the Driver Files

The SAP HANA driver is a Java-based driver and can be run on the Identity Manager engine or on a Remote Loader server. It works only with Java Remote Loader.

- ♦ [“Installing the Driver Files as a Root User” on page 12](#)
- ♦ [“Installing the Driver Files as a Non-Root User” on page 13](#)
- ♦ [“Configuring Remote Loader for the Driver Instance” on page 13](#)

Installing the Driver Files as a Root User

You must install the driver files manually. The SAP HANA driver files are installed on the Identity Manager server at the same time as the Identity Manager engine. The installation program extends the Identity Vault’s schema and installs the driver shim and the driver configuration file, but does not create the driver in the Identity Vault or upgrade an existing driver’s configuration. For information about creating the driver, see [“Creating the Driver Object” on page 14](#).

To install the dependent jar files, perform the following actions on your platform as applicable:

- 1 Login as root on the server where you want apply the driver jar file.
- 2 Navigate to the extracted IDM_SAPHanaDriver_1.0.0.zip directory and perform one of the following actions for your platform:
 - ♦ For Linux:
Install the new netiq-DXMLSAPHana-1.0.0.0000-1.noarch.rpm in your driver installation directory by running the following command in a terminal window. If you are installing the binary, run the below command:


```
rpm -ivh (binaries-path)/netiq-DXMLSAPHana-1.0.0.0000-1.noarch.rpm
```
 - ♦ For Windows:
Copy the saphanashim.jar file to your driver installation folder. For example,
<InstallLocation_Drive>\NetIQ\IdentityManager\NDS (local installation) or
<InstallLocation_Drive>\Novell\RemoteLoader\64bit (remote installation).

NOTE: It is mandatory,

- ♦ **For Windows:** Identity Manager engine must contain the ngdbc-2.16.11.jar (available in [Maven Repository \(https://repo1.maven.org/maven2/com/sap/cloud/db/jdbc/ngdbc/2.16.11/\)](https://repo1.maven.org/maven2/com/sap/cloud/db/jdbc/ngdbc/2.16.11/)) in <InstallLocation_Drive>\NetIQ\IdentityManager\NDS\lib and Windows RL path <InstallLocation_Driver>\NetIQ\IDM\RemoteLoader\64bit\lib
 - ♦ **For Linux:** Identity Manager engine must contain the ngdbc-2.16.11.jar (available in [Maven Repository \(https://repo1.maven.org/maven2/com/sap/cloud/db/jdbc/ngdbc/2.16.11/\)](https://repo1.maven.org/maven2/com/sap/cloud/db/jdbc/ngdbc/2.16.11/)) in /opt/novell/eDirectory/lib/dirxml/classes.
-

Installing the Driver Files as a Non-Root User

1. Verify that the /rpm directory exists and contains the _db.* file.
2. The _db.* file is created during a non-root installation of the Identity Manager engine. The absence of this file indicates that the Identity Manager is not installed properly. In such a case, reinstall the Identity Manager to correctly place the file in the mentioned directory.
3. To set the root directory to the location of non-root in Identity Manager, enter the following command in the command prompt:

ROOTDIR=<non-root eDirectory location>

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

4. For example, to install the SAP HANA driver rpm, use this command:

```
rpm --dbpath $ROOTDIR/rpm -ivh --relocate=/usr=$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/netiq-DXMLSAPHana-
1.0.0.0000-1.noarch.rpm
```

NOTE: In the above command /opt/novell/eDirectory is the location where non-root Identity Manager is installed, and /home/user/ is the home directory of the non-root user.

You must configure the driver to use an SSL connection between the Remote Loader and the Identity Manager server. For more information, see [Creating a Secure Connection to the Identity Manager Engine](#) in the *NetIQ Identity Manager Driver Administration Guide*.

For more information on configuring the Remote Loader, see “[Configuring Remote Loader for the Driver Instance](#)” on page 13.

Configuring Remote Loader for the Driver Instance

For more information about specifying values for these parameters, see [Configuring the Remote Loader and Drivers](#) in the *NetIQ Identity Manager Driver Administration Guide*.

Below is an example of a Linux configuration file with some sample values.

```
-description "SAP HANA Driver"
-commandport 8000
-connection "port=8090"
-trace 3
-tracefile "/opt/netiq/SAP HANAdriver.log" (or
"C:\novell\remoteload\64bit\SAP HANADriver-Trace.log" on Windows)
-tracefilemax 100M
-class "com.netiq.dirxml.driver.saphana.SAPHanaDriverShim"
```

Once the driver instance is running, you can use the command line on Linux or Remote Loader Console on Windows to instruct the Remote Loader to perform a function. For example, turn the trace on or off on Windows or stop the driver instance.

Creating the Driver Object

To create a SAP HANA driver object you must install the driver packages and then modify 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 the driver.

- ♦ [“Importing the Current Driver Packages” on page 14](#)
- ♦ [“Installing and Configuring the Driver Object” on page 14](#)

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.

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

- 1 Open Designer.
- 2 In the Outline view, right-click the Package Catalog.
- 3 Click **Import Package**.
- 4 Browse to the location where you downloaded the SAP HANA packages.
- 5 Select the required packages for SAP HANA. Alternately, you can click **Select All** to import all of the packages displayed. For the available SAP HANA packages, see [“SAP HANA Driver Packages” on page 11](#).
- 6 Click **OK** to import the selected packages, then click **OK** in the successfully imported packages message.
- 7 After the current packages are imported, continue with [“Installing and Configuring the Driver Object” on page 14](#).

Installing and Configuring the Driver Object

- 1 In **Designer**, open your project.
- 2 From the **Palette**, drag-and-drop the SAP HANA driver to the desired driver set in the **Modeler**.
The SAP HANA driver is under the **Enterprise** category in the Palette.

- 3 Select the required packages that you want to install for the SAP HANA driver, then click **Next**.
For more information, see “[SAP HANA Driver Packages](#)” on page 11.
- 4 Click **OK** on the **Package Dependencies** screen.
- 5 Fill the **Driver Name** field, then click **Next**.
- 6 In the **Driver Parameters** page, the following sections and fields are displayed. Enter the values in the corresponding fields as shown below and click **Next**.
 - ♦ **Driver Options:** The **Driver Options** field defaults to **Show Authentication Parameters**.
 - ♦ **SAP HANA Driver Database Configuration:** Select the authentication type as required. The available options are:
 - ♦ **Username:** This option requires the user name of the SAP HANA database to establish connection.
 - ♦ **Password:** Specify the database password.
 - ♦ **SQL Endpoint:** Specify the destination SAP HANA SQL Endpoint details to establish the connection.
For example:
 - ♦ <server>:<port>. Ex: myServer:30015
 - ♦ <endpoint>:<port>. Ex: 1234568-abcd-12ab-34cd-1234abcd.hana.hanacloud.ondemand.com:443
 - ♦ **Use SSL Connection:** By default this value is set to **False**. You can switch it to **True** if SSL Connection is required. If it is set to **True**, provide **Truststore Path** and **Truststore Password**. If **Truststore Path** and **Truststore Password** are not provided, the driver looks for the certificate in the default Java keystore. For more information on secured connection, see (<https://help.sap.com/docs/hana-cloud/sap-hana-cloud-getting-started-guide/connect-to-sap-hana-database-in-sap-hana-cloud-via-jdbc>).
 - ♦ **Cache Parameters:** It reads the default cache path or user defined path. Specify the **Cache Directory Path** to store the temporary files.
 - ♦ **Advanced Parameters:** By default the value is set to **Hide**. When it is set to **Show**, under **Paging Parameters** specify the number of pages to be processed at a time by the driver in **Page Size**.
- 7 Fill in the **Subscriber Options** as shown below and click **OK**.
 - ♦ **Assign User to a default UserGroup:** By default the value is set to **Yes** to assign the user to default user group. Else the user is not assigned to any user group.
 - ♦ **Default usergroup name:** This field is enabled if **Assign User to a default UserGroup** value is set to **Yes**. By default, DEFAULT is the UserGroup name and is editable.
- 8 Fill in the **Publisher Options** as shown below and click **Next**.
 - ♦ **Publisher Options:**
 - ♦ **Enable Publisher Channel:** **Yes**
 - ♦ **Users:** Specify the values in the fields as shown below:
 - ♦ **Migrate Users on Driver Startup:** These parameters are valid only at driver startup. Driver will continue with regular polling after the task at startup is completed. If driver shuts down unexpectedly during migration, just restart the

driver and migration will continue. If it's is set to **True**, migration is initiated for users, on driver startup. When it's set to **False**, regular polling for users is initiated.

- ♦ **Poll Users:** It polls the users from SAP HANA application during migration. By default this value is set to **True**.
- ♦ **Exclude Users:** This field excludes the system generated users while polling. You can add/delete/ edit the user prefixes. All the Users with UserName starting with any of the strings listed will not be migrated or polled.
- ♦ **User Groups:**
 - ♦ **Migrate User Groups on Driver Startup:** These parameters are valid only at driver startup. Driver will continue with regular polling after the task at startup is completed. If driver shuts down unexpectedly during migration, just restart the driver and migration will continue. If it's is set to **True**, migration is initiated for user groups on driver startup. When it's set to **False**, regular polling for user groups is initiated.
 - ♦ **Poll User Groups:** It polls the user groups from SAP HANA application during migration. By default this value is set to **False**.
 - ♦ **Exclude User Groups:** This field excludes the system generated users groups while polling. You can add/delete/ edit the user group prefixes. All the user groups starting with any of the strings listed will not be migrated or polled.
- ♦ **Roles:**
 - ♦ **Migrate Roles on Driver Startup:** These parameters are valid only at driver startup. Driver will continue with regular polling after the task at startup is completed. If driver shuts down unexpectedly during migration, just restart the driver and migration will continue. If it's is set to **True**, migration is initiated for roles on driver startup. When it's set to **False**, regular polling for roles is initiated.
 - ♦ **Poll Roles:** It polls the roles from SAP HANA application during migration. By default this value is set to **False**.
 - ♦ **Exclude Roles:** This field excludes the system generated roles while polling. You can add/delete/ edit the role prefixes. All the roles with the name starting with any of the strings listed will not be migrated or polled.
- ♦ **Polling Interval:** It is the number of minutes between the polling cycles.
- ♦ **Heartbeat Interval:** This option is used to configure the driver shim to send a periodic status message on the Publisher channel, when there is no Publisher traffic for a specified number of minutes. By default, this is set to 10 minutes.

9 Fill in the following fields for the Remote Loader information, then click **Next**:

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 for Linux* or [Configuring the Remote Loader and Drivers](#) in the *NetIQ Identity Manager Setup Guide for Windows*.

If you select **No**, skip to Step 8. 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.

KMO: Specify the Key Name (for example, kmo=remotecert) of the Key Material Object (KMO) containing the keys and certificate to be used for SSL.

If you used spaces in the certificate name, you need to enclose the KMO object nickname in single quotation marks.

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 Identity Manager server. It must be the same password that is specified as the Driver Object Password on the Remote Loader.

- 10 Click **Next**. Review the summary of tasks that will be completed to create the driver, then click **Finish**.
- 11 After you have installed the driver, you can change the configuration for your environment. or more information, see [“Creating the Driver Object” on page 14](#).

Configuring Entitlements

In Designer, after creating the driver object, double click the connector line and navigate to **GCVs > Entitlement** tab. Specify the following parameters to configure entitlements:

- ♦ **Enable User Account Entitlement:** Select the value as **true** to enable the entitlements feature for User Accounts.
- ♦ **Enable User Group Entitlement:** Select the value as **true** to enable the entitlements feature for User Groups.
- ♦ **Enable Role Entitlement:** Select the value as **true** to enable the entitlements feature for Roles.

NOTE: After configuring the SAP HANA driver for entitlements, you can deploy the driver. Post deployment, perform the procedures as explained in the following sections.

Fetching Entitlements from SAP HANA Cloud Database

You must ensure to perform a “CodeMap refresh” to fetch all the users, user groups and assignable roles from SAP HANA. The code map refresh, helps to facilitate the grant or revoke permissions through Identity Manager. For the procedure to refresh the code map, see [Entitlement Query Settings](#) section in the [NetIQ Identity Manager - Administrator’s Guide to the Identity Applications](#). SAP HANA driver is supported by following entitlements.

- ♦ Users: Assigning Permissions to users.
- ♦ User Group: Adding and removing members to the user group is supported using entitlements.
- ♦ Roles operations: Assigning and revoking privileges to roles is supported using entitlements.

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 5; otherwise, specify the following information:
 - ♦ **Host:** Specify the IP address or DNS name of the server hosting the Identity Vault.
 - ♦ **Username:** Specify the DN of the user object used to authenticate to the Identity Vault.
 - ♦ **Password:** Specify the user's password.
- 4 Click **OK**.
- 5 Read through the deployment summary, then click **Deploy**.
- 6 Read the successful message, then click **OK**.
- 7 Click **Define Security Equivalence** to assign rights to the driver and all required jobs.

The driver and all required jobs require the 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.
 - 8b Click **OK**.
 - 8c Repeat Step 8a and Step 8b for each object you want to exclude.
 - 8d Click **OK**.
- 9 Click **OK**.

Starting the Driver

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

To start the driver:

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

The driver cannot initialize completely unless it successfully connects to the Remote Loader and loads the SAP HANA driver shim.

Activating the Driver

To activate the SAP HANA driver, activate the Metadirectory engine, then activate the driver by using the separate SAP HANA activation key. If you created the driver in a driver set that has not been activated, you must activate the Metadirectory engine and the driver within 90 days. Otherwise, the driver stops working.

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

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

To use the driver, you must reactivate it.

For more information on activation, see [Activating Identity Manager](#) in the *NetIQ Identity Manager Overview and Planning Guide*.

3 Attributes Mapping & Filtering

This chapter provides information about mapping of various attributes available for the SAP HANA driver:

- ♦ [“User Attributes” on page 21](#)
- ♦ [“User Group Attributes” on page 21](#)
- ♦ [“Role Attributes” on page 22](#)
- ♦ [“Attribute Filter Settings” on page 22](#)

User Attributes

The below table lists user attributes.

Table 3-1 Mapping of User Attributes

SAP HANA Attribute Name	NDS-Name	Description
USER_NAME	CN	Name of the user.
COMMENTS	Description	Description of the user.
USERGROUP_NAME	Group Membership	Group to which the user belongs to.
USER_MODE	employeeType	Employee type to which the user belongs to.
USER_DEACTIVATED	Login Disabled	Specifies if the user is disabled or deactivated from login activities.
EMAIL ADDRESS	Internet EMail Address	E-mail address of the user.

User Group Attributes

The below table lists User Group attributes.

Table 3-2 Mapping of User Group Attributes

SAP HANA Attribute Name	NDS-name	Description
USERGROUP_NAME	CN	Name of the user.
COMMENTS	sapHanaComments	Description of the user group object.

Role Attributes

The below table lists Role attributes.

Table 3-3 Mapping of Role Attributes

SAP HANA Attribute Name	NDS-name	Description
ROLE_NAME	CN	Role description
COMMENTS	sapHanaComments	Description of the role.
ROLE_MODE	sapHanaRoleMode	Mode of the specified role.
ROLE_SCHEMA_NAME	sapHanaRoleSchemaName	Schema name to which the role belongs to.
ROLE_GROUP_NAME	sapHanaRoleGroupName	Group name to which the role belongs to.

Attribute Filter Settings

This section provides information about the Identity Vault Filter settings in the driver. The SAP HANA will be the authoritative source for all the above attributes except user ID and Email address which are generated in the Identity Manager.

- ♦ [“User Attributes Filter Settings” on page 22](#)
- ♦ [“User Group Filter Settings” on page 23](#)
- ♦ [“Role Filter Settings” on page 23](#)

User Attributes Filter Settings

The following table provides information about the Users Attributes Filter settings:

Table 3-4 User Attributes Filter Settings

Attribute Name	Merge Authority	Publisher	Subscriber
nspmDistributionPassword	default	ignore	notify
CN	default	sync	sync
Description	default	sync	sync
DirXML-Associations	default	ignore	notify
Group Membership	default	sync	sync
employeeType	default	sync	sync
Login Disabled	default	sync	sync
Internet EMail Address	default	sync	sync
DirXML-EntitlementRef	default	ignore	notify

User Group Filter Settings

The following table provides information about the User Group Filter settings:

Table 3-5 User Group Filter Settings

Attribute Name	Merge Authority	Publisher	Subscriber
CN	default	sync	ignore
sapHanaComments	default	sync	ignore
DirXML-Associations	default	ignore	notify

Role Filter Settings

The following table provides information about the Role settings:

Table 3-6 Role Filter Settings

Attribute Name	Merge Authority	Publisher	Subscriber
CN	default	sync	ignore
DirXML-Associations	default	ignore	notify
sapHanaComments	default	sync	ignore
sapHanaRoleMode	default	sync	ignore
sapHanaRoleSchemaName	default	sync	ignore
sapHanaRoleGroupName	default	sync	ignore

4 Securing Communication

SAP HANA provides secure communication using TLS/SSL. You can configure the driver to take advantage of this increased security.

The communication between the Identity vault and SAP HANA is established through the Subscriber and Publisher channels. To establish a secure communication between them, you need a trust store containing a certificate issued by the certificate authority that signed the server's certificate.

It is recommended to import the chain of CA certificates from issuer's trusted URL. SAP HANA instance uses certificates from a trusted CA. For example, if SAP HANA is using the certificates from Digicert (trusted CA), you must verify the authenticity of the certificates from the Digicert's website before downloading and importing them into the Java Keystore.

For testing purposes, you can download the certificates from the browser directly but this is not recommended. In case you want to view and download the certificates from browser, perform the following steps:

- 1 Enter the SAP HANA login URL in your browser (for example Chrome), and click **Enter**.

NOTE: Different browsers have different procedures to view the certificates. Steps 1 to 6 considers Chrome browser as an example.

- 2 Click the lock icon near the browser, and select **Certificate (Valid)**. The certificate is displayed.
- 3 Click **Certification Path**. The Certification Path displays the hierarchical structure of the structure of all the certificates.
- 4 Select the root certificate (the top most parent certificate), and click **View Certificate**. The root certificate is displayed.
- 5 To save the certificate to your system, click **Details > Copy to File > Next > Next**.
- 6 Enter a filename for the certificate and save it to a location as required.
- 7 Import the saved SAP HANA tenant root CA certificate into your trust store or create a new trust store by entering the following command at the 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
```

- 8 Configure the driver to use the trust store you created in Step 1:
 - 8a Log into the Identity Console. Click **Identity Manager > Identity Manager Overview**.
 - 8b Locate the driver set containing the SAP HANA driver, when click the driver's icon to display the Identity Manager Driver Overview page.

- 8c** On the Identity Manager Driver Overview page, click the driver's icon again, then scroll to **Driver Options**.
- 8d** In the **Keystore File** setting, specify the trust store password and the path to the trust store you created in Step 1.
- 9** Click **Apply**, then click **OK**.

5 Update User with Minimum Rights

This section provides the information about assigning minimum rights required for a user management in the publisher channel.

Create a System User

Follow the below steps to create a system user.

- 1 Go to **User Management** and click  to **Create User** or to **Create Restricted User**.
- 2 Under **General Information**, specify the **User Name**, **User Group**, **Email**, validity of the user (in **Valid From** and **Valid Up To** fields). Select Yes or No for **Creation of Objects in Own Schema**, **PUBLIC Role**, and **Disable ODBC/JDBC Access**.
- 3 Under **Authorization Mode** tab, select the **Authorization Mode**.
- 4 Under **Authentication Mechanism**, specify the password parameters for the user.

Grant Roles

Follow below steps to assign the roles to the system user.

- 1 Under **User Management**, select a user that has been created already.
- 2 This display the User details in a view mode. Click **Assign Roles**.
- 3 **Role Assignment for User** (the selected user) page appears.
- 4 Check the role to which the selected user has to be assigned. Toggle to  if the role assigned is **Grantable to Others**. Else toggle to .
- 5 Click **Save**.

Assign Privileges

User can be assigned with the following types of privileges.

System Privileges

Go to **Privilege Management** and under **System Privileges** tab, assign system privileges to the selected user.

Object Privileges

Go to **Privilege Management** and under **Object Privileges** tab, assign system privileges to the selected user.

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the SAP HANA driver. These are the only unique properties for drivers. 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 Identity Console. If a field is different in Designer, it is marked with a Designer icon.

Refer to the following sections for more information:

- ♦ [“Driver Configuration” on page 29](#)
- ♦ [“Global Configuration Values” on page 31](#)

Driver Configuration

In Identity Console:

- 1 Login to Identity Console, select **IDM Administration** under Identity Manager if not defaulted already.
- 2 The Identity Manager Overview page appears.
- 3 Click **Driver Sets** tab, the configured drivers appear.

NOTE: 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.

- 4 Click the driver tile. By default **Connection Parameters** tab appears. To configure the selected driver, goto **Configuration** tab and click **Driver Parameters** under **Driver Settings**, **Subscriber Settings** and **Publisher Settings**.
- 5 Define the driver parameters as required.

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:

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 is: `com.netiq.dirxml.driver.saphana.SAPHanaDriverShim`

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

- ♦ **Remote Loader Client Configuration for Documentation:** Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

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.

Authentication

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

Authentication ID: This option is not used with the SAP HANA driver.

Authentication Context: This option is not used with the SAP HANA 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 it is set to zero, the file size is unlimited. Click **Unlimited** to set the file size to unlimited in Designer.

Application Password: This option is not used with the SAP HANA driver.

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.

Startup Option

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 Identity Console.

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.

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 divided into the following categories:

- ♦ Driver Options
- ♦ Subscriber Options
- ♦ Publisher Options

To configure the above options, see [Step 6](#) in the section “[Creating the Driver Object](#)” on page 14.

Global Configuration Values

Global Configuration Values (GCVs) can be used by the driver to control its functionality. GCVs are defined in the driver or in the driver set. Driver set GCVs can be used by all drivers residing in the driver set.

The SAP HANA driver includes predefined GCVs. You can also add your own GCVs as required for the additional policy implementation in the driver. For information on most of the GCVs, see “[Creating the Driver Object](#)” on page 14.

However, the following GCV’s should be configured after installing the driver:

- ♦ **Common Password Setting:**
 - ♦ ***Set default password if not available:*** Set this value to **True** if the default password is not available for the server.
- ♦ **SAP HANA Group and Role:**
 - ♦ **Group - Publisher Settings**
 - ♦ *Group Placement Container* - Specify the tree path where the data has to sync for group placement container.
 - ♦ **Role - Publisher Settings**
 - ♦ *Role Placement Container* - Specify the tree path where the publisher settings data has to sync for roles.
- ♦ **Entitlements:**
 - ♦ **Entitlements Configuration:**
 - ♦ *Enable User Account Entitlements:* Set this value to **True** if you need to enable the user account entitlements, else set to **False**.

- ♦ *Enable User Group Entitlement:* Set this value to **True** if you need to enable the user group entitlements, else set to **False**.
- ♦ *Enable Role Entitlement:* Set this value to **True** if you need to enable the role entitlements, else set to **False**.
- ♦ **Advanced Settings:**
 - ♦ *Advanced Settings:* By default this value is **Hide**. Set this value to **Show** if you need to define advanced setting parameters for Data Collection or Role Mapping or Resource Mapping or Entitlement Extensions. When Advanced Settings is set true below listed GCV values are displayed.
 - ♦ **Data Collection**
 - ♦ **Enable Data Collection:** When this value is set to **Yes**, the below listed GCV values are displayed. Else set it to **No**.
 - ♦ *Allow Data Collection from User Account:* Set this value to **Yes** if data collection is required from user accounts. Else set it to **No**.
 - ♦ *Allow Data Collection from User Groups:* Set this value to **Yes** if data collection is required from user groups. Else set it to **No**.
 - ♦ *Allow Data Collection from Role:* Set this value to **Yes** if data collection is required from roles. Else set it to **No**.
 - ♦ **Role Mapping:** When this value is set to **Yes**, the below listed GCV values are displayed. Else set it to **No**.
 - ♦ *Allow mapping of User Account:* Set this value to **Yes** if role mapping is required for user accounts. Else set it to **No**.
 - ♦ *Allow mapping of User Groups:* Set this value to **Yes** if role mapping is required for user groups. Else set it to **No**.
 - ♦ *Allow mapping of Role:* Set this value to **Yes** if mapping is required for roles. Else set it to **No**.
 - ♦ **Entitlement Extensions:**
 - ♦ *User Account Extensions:* Specify the assignment extensions for user accounts.
 - ♦ *User Groups Extensions:* Specify the assignment extensions for user groups.
 - ♦ *Role Extensions:* Specify the assignment extensions for roles.

♦ Password Synchronization

Password Management

- ♦ *Application accepts password from Identity Manager: (Managed from the Password Sync page)* - By default the value is set to **True**. The SAP HANA application accepts the password from Identity Manager.
- ♦ *Reset user's external system password to the Identity Manager Password on failure: (Managed from the Password Sync page)* - By default the value is set to **True**. If there is any failure during password synchronization, the Identity Manager password is synced to the external system (SAP HANA) user.
- ♦ *Notify the User Password Synchronization failure via e-mail: (Managed from the Password Sync page)* - By default the value is set to **True**. This enables in notifying the user through an e-mail, if there is any failure in synchronizing the password.

For more information on GCVs, see [When and How to Use Global Configuration Values in *NetIQ Identity Manager Driver Administration Guide*](#).

B Trace Level

The driver supports the following trace levels:

Table B-1 *Supported Trace Levels*

Level	Description
0	Provides error/warning/exception
1	Previous level and success messages.
2	Previous level and input/output trace
3	Previous level and policy processing/SOAP calls
4 & 5	More debug messages

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

C IDV Schema Extension

As part of solution, we need to extend the schema of eDirectory so that the SAP HANA driver can create these additional objects in the IDV. The proposed schema extension in sch formats are available for download. The following classes are added in IDV.

- ♦ The schema file should only be extended with the ndssch utility. Using any other method for importing the schema file fails for certain attributes. A sample syntax for importing the schema file has been provided below:

For Windows:

Syntax: /opt/novell/eDirectory/bin/ndssch -h IP:PORT -t WIN-TREE-NAME
admin-FDN SchemaFilePath/schemaFile.sch -p password

Example: /opt/novell/eDirectory/bin/ndssch -h WINDOWS_IP:524 -t WIN_TREE
admin.sa.system /home/sapHana-schema.sch -p password

For Linux:

Syntax: ndssch -t LINUX-TREE-NAME admin-FDN SchemaFilePath/schemaFile.sch

Example: ndssch -t TREE-NAME admin.sa.system /home/sapHana-schema.sch

- ♦ Effective Class for UserGroup: sapHanaUserGroup
- ♦ Effective Class for Role: sapHanaRole

D IDV Proposed Structure

As part of solution, it is proposed to have a different container for different objects in IDV. The proposed structure is as follow:

