



APPLICATION ACCESS MANAGER

(Agent Based Credential Provider CP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: Denodo Technologies Inc.

Website: <https://www.denodo.com>

Name of Product: Denodo Platform

Version: 8.0

Date: November 20th, 2020

PARTNER SOLUTION OVERVIEW

Data virtualization is a logical data layer that integrates all enterprise data siloed across the disparate systems, manages the unified data for centralized security and governance, and delivers it to business users in real time. *Data virtualization* is the modern approach to data integration. Unlike ETL solutions, which replicate data, data virtualization leaves the data in source systems, simply exposing an integrated view of all the data to data consumers.

Denodo is the leader in Data Virtualization.

How Data Virtualization Works

- **Connect** to any data source: Databases, data warehouses, cloud applications, big data repositories, and even Excel files.
- **Combine** any type of data: Structured, streaming, social, and flat files.
- **Consume** the data in any mode: Denodo provides several interfaces: JDBC, ODBC, REST and SOAP web services, a data catalog, etc. The Consume layer enables a single point of access and interaction with the underlying data sources, as well as abstracted data views in a standard delivery format. The Consume layer offers the broadest data delivery options to suit business user needs via JDBC, ODBC, ADO.NET, SOAP web services, RESTful web services (output as XML, JSON, HTML, or RSS), OData, exports to Microsoft Excel/SQL, and JMS message queues.

Data Virtualization Use Cases:

- BI and Analytics: Self-Service Analytics, Logical Data Warehouse, Enterprise Data Fabric.
- Customer Centricity / MDM: obtaining a complete view of the customer.
- Data Governance: GRC, GDPR, Data Privacy / Masking.
- Data Services: Data Marketplace, Data Services, data migration.
- Big Data: Logical Data Lake, Data Warehouse offloading, IoT Analytics.

Version: 8.0

Platform components:

- Virtual DataPort: the main component of the Denodo Platform. This is the component that includes the integration with CyberArk.
- The Denodo Platform has other components that are not relevant to this integration. For example, *Scheduler* to schedule the execution of queries, *Data Catalog*, etc.

KEY BENEFITS

Benefits of Denodo:

- **Zero replication:** unlike ETL, data virtualization does not need to “collect” the data into a separate repository in order to transform it to the destination format. It handles the transformation and aggregation on-the-fly.

- **Data abstraction:** Data virtualization hides the complexities of accessing data from the underlying data systems, their formats and structures.
- **Real-Time Data Delivery:** since data virtualization “connects” to the underlying data sources in real-time, it delivers up-to-the-minute data to the business users within their applications.
- Others, see the complete list at <https://www.denodo.com/en/data-virtualization/benefits>.

Benefits of integrating Denodo with CyberArk AAM:

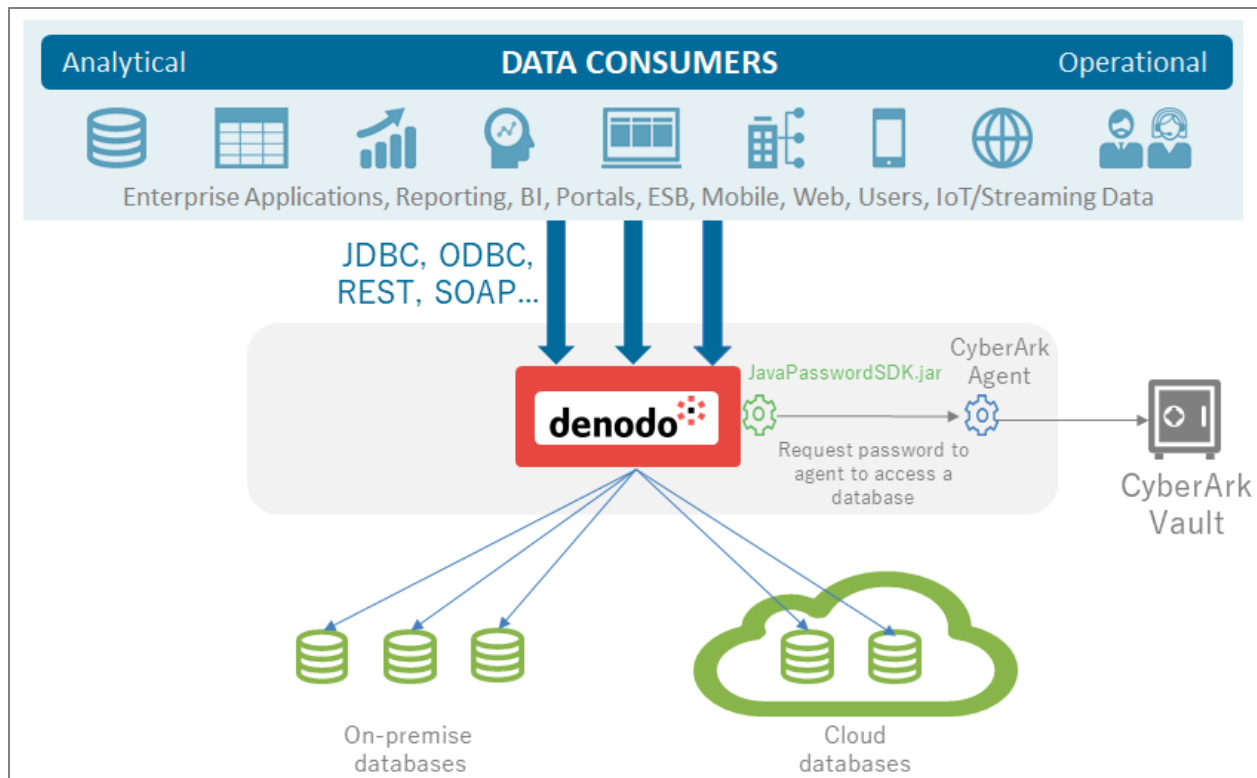
- With the CyberArk integration, the passwords are no longer stored in Denodo. When creating a connection to a database in Denodo, often users enter the credentials of a service account in that database (although Denodo also supports *single sign-on*; that is, passing the credentials of the user that connects to Denodo, to the underlying databases). The password is stored in Denodo. Even though Denodo stores the passwords of the data sources encrypted, it is more secure if it is stored in CyberArk’s password vault.
- With the CyberArk integration, if an administrator changes the password of a service account that Denodo uses, this change is immediately reflected in Denodo. Thanks to this, rotating the password of service accounts is much easier.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Denodo supports retrieving the credentials of a database in two ways:

1. From a CyberArk agent that runs on the same computer as the Denodo Platform. In this case, Denodo uses the library *JavaPasswordSDK.jar* to contact the local CyberArk agent, which in turn retrieves the password from the vault.
2. Or without an agent, by sending HTTPs requests to the service *AIMWebService*.

This document and the diagram below depict option #1.



Denodo and CyberArk are sold separately. Users have to obtain the appropriate license for each vendor. The integration with CyberArk is part of the Denodo Platform and is not sold separately nor there are additional charges for using it.

Denodo does not include the library “JavaPasswordSDK.jar”; the user will provide it.

AAM INTEGRATION

In Denodo, SQL developers create connections to databases (called *JDBC data sources*). Then, they will create *base views* in Denodo, which represent tables and views on those databases, and create views based on these *base views*, to combine data obtained from different sources, transform it, etc.

To create a JDBC data source, Denodo provides two main options regarding authentication to the database:

1. Connect to the database using the credentials of the user that connected to Denodo (i.e., *single sign-on*).
2. Connect to the database using a service account. With this feature, instead of entering the user and password of the service account, the user can enter the name of a CyberArk account. When Denodo needs to open a connection to this database, Denodo will retrieve the credentials from the CyberArk agent.

CREDENTIAL RETRIEVAL

When SQL developers configure a JDBC data source of Denodo, they can configure it to retrieve the credentials (i.e., user and password) from a CyberArk account instead of entering the credentials of a service account. In this scenario, this is what happens the first time the data source opens a connection to this database:

1. The data source uses the Java API provided by CyberArk to communicate with the CyberArk agent that runs in the same computer as the Denodo server. It uses this API to request the credentials (user and password) of the CyberArk account you entered in the data source.
2. Using the credentials provided by the agent, the data source opens the connection to the database.
3. The data source holds these credentials in-memory (never in disk) with the goal of speeding up the creation of further connections to this database.

The next time this data source opens a connection to this database, it will do this:

1. The data source will try to open the connection using the credentials stored in memory. That is, the credentials it previously obtained from the CyberArk agent.
2. If the connection fails, the data source will request the credentials to the agent and try to open the connection again.
3. If the connection fails again, the data source will return an error to the user.

The steps #1 and #2 happen automatically without the intervention of the user.

Additional considerations

- With the default configuration, the JDBC data sources of Denodo create a [pool of connection to the database](#). When you configure a data source to request the credentials to a CyberArk agent, the process of opening a new connection is the same regardless of if the pool is enabled or disabled.
- If you enabled the option *pass-through credentials* in the data source, the data source will use the credentials of the end user to execute queries and will use the credentials obtained from the CyberArk agent, to introspect the database. That is, to list the tables and views of the database when you click *Create base view*.
- If the Denodo server is restarted or the data source is recreated (e.g., you change the configuration and click *Save*), the credentials stored in memory for this data source are removed from memory and will be retrieved from the CyberArk agent again.
- You can also configure the data source to retrieve the credentials with the authentication option *Use Kerberos*. In this scenario, the data source will retrieve the credentials from the agent, and use these credentials to obtain a Kerberos ticket.

REQUIREMENTS

You need to install the update of Denodo *Denodo 8.0u01* in the Denodo server and the administration tool.

Copy the library *JavaPasswordSDK.jar* to the computer where Denodo is installed.

Denodo does not have any other specific requirements for the agent-based integration. An administrator of Denodo can enable the integration with CyberArk.

AAM INSTALLATION

Refer to the “Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.

AAM CONFIGURATION

The following sections provide details on the Denodo Platform configuration with CyberArk AAM.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.

Add Application

Name:

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location:

☐ Access Permitted: From: To:

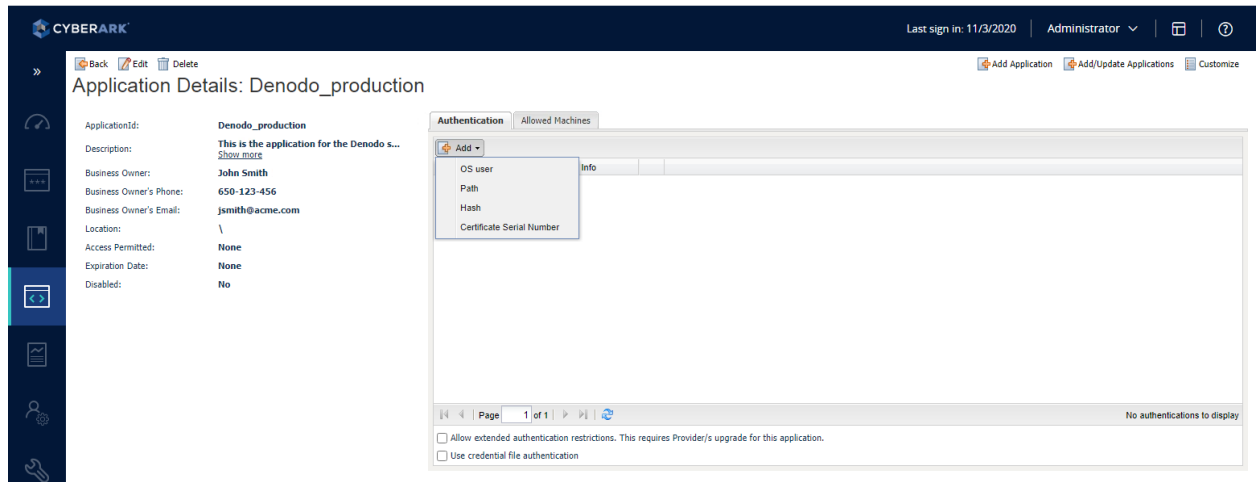
☐ Expiration Date:

☐ Disabled

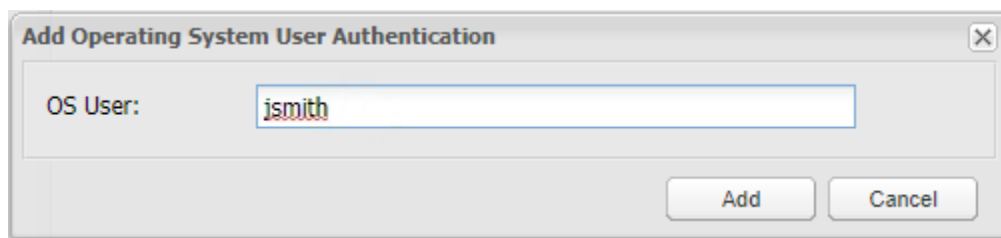
- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: *Denodo_<environment>*. For example: *Denodo_production*
 - In the **Description** box, specify a short description of the application that will help you identify it.

- In the **Business owner** section, specify contact information about the application's business owner.
- In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

- ☐ Click **Add**. The application is added and is displayed in the Application Details page.

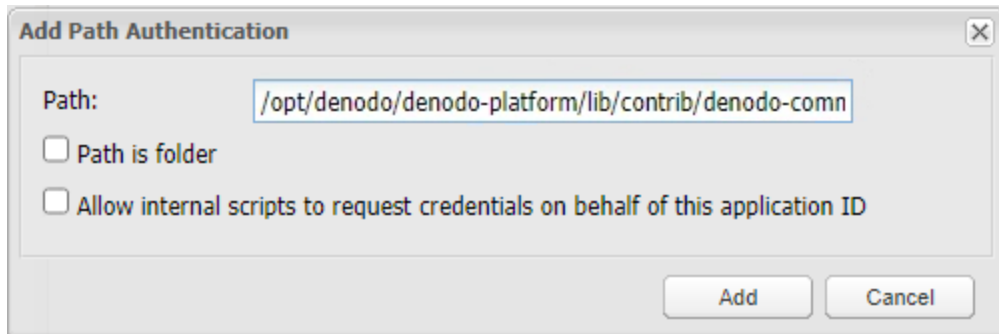


- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.



This is the account with which you start the Denodo server (i.e., Virtual DataPort).

- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.

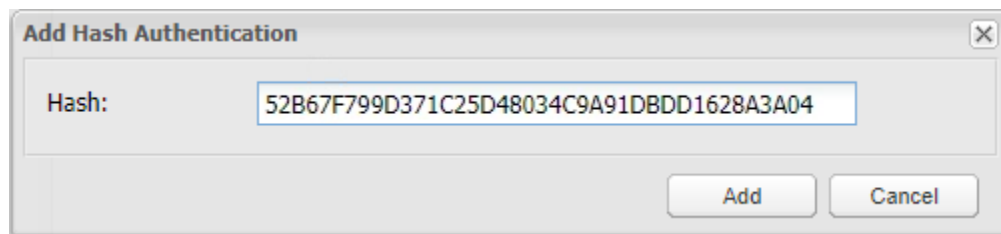


- ☐ In the **Path** box, enter `<DENODO_HOME>/lib/contrib/denodo-commons-vault.jar` (replace `<DENODO_HOME>` with the actual path to the Denodo installation). In this path, the path separator has to be same as in the computer where Denodo runs (i.e. “\” for Windows and “/” for Linux) or always “/”.

- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.

- ☐ Specify a hash:

- Run the `AIMGetAppInfo` utility to calculate the application’s unique hash. Provide the path `<DENODO_HOME>/lib/contrib/denodo-commons-vault.jar`.
Copy the hash value returned by the utility.
- In the PVWA, select **Hash**. The Add Hash window appears.



- In the Hash edit box, paste the application’s unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying ‘#’ after the hash value, followed by the comment.

For example, `52B67F799D371C25D48034C9A91DBDD1628A3A04`

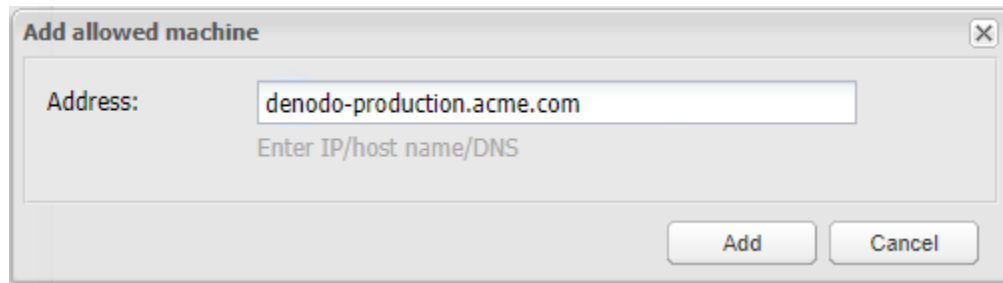
Note: The comment must not include a colon or a semicolon.

Note: this hash may change after installing an update of Denodo so, after installing an update, run the `AIMGetAppInfo` utility to check if the hash has changed. If it has changed, add the new hash and consider keeping the existing one if you have Denodo servers running different updates.

- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

- ☐ Specify the application’s Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords.

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.



The screenshot shows a standard Windows-style dialog box titled "Add allowed machine". It features a close button (X) in the top right corner. The main area contains a label "Address:" and a text input field with the value "denodo-production.acme.com". Below the input field, there is a hint text "Enter IP/host name/DNS". At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

Make sure the servers allowed include all mid-tier servers or all endpoints where the AAM Credential Providers were installed.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search:
Search In:

Selected Search: Vault
Display 4 result(s)

	Name	Business Email	Full Name
	Denodo-hash		
	Denodo-noauth		
	Denodo-cert		
	Denodo-path		

☐ Access

☒ Use accounts
☒ Retrieve accounts
☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☒ View Audit log
☒ View Safe Members

☐ Workflow

- ☐ Add the application (the APPID) as a Safe Member with the following authorizations:
- Retrieve accounts

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☐ View Safe Members

▲

▼

Add

Close

- ☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to the [documentation of the Denodo Platform](#) for more details about configuring the integration with CyberArk.

Follow these steps to enable the integration with CyberArk in Denodo:

1. Install the CyberArk agent on the same computer as the Denodo Platform.
2. Log in to Denodo from the Administration Tool, with an administrator account.

3. Click the menu **File > Extension management**.
4. In this dialog, click the tab **Libraries** and click **Import**.
5. In **Resource type**, select **jar** and click **Add**. Select the file *JavaPasswordSDK.jar* (usually located in `<CYBERARK_AGENT_HOME>/ApplicationPasswordSdk/JavaPasswordSDK.jar`)
6. Click **Ok** and **Ok** again to upload this library.
7. Restart Denodo Virtual DataPort.
8. Log in to Denodo from the Administration Tool again, with an administrator account.
9. On the menu **Administration**, click **Server configuration** and then, click the tab **Credentials vault**.
10. In this tab, select **Use external credentials vault** and then, set **Provider** to **CyberArk (agent mode)**.
11. In **Application Id**, enter the application name with which you registered Denodo in CyberArk. For example, *denodo_production*.
12. Click **Ok** to save the changes.

The screenshot shows the 'Server Configuration' dialog box with the 'Credentials vault' tab selected. On the left is a sidebar with various configuration categories. The main area shows the 'Use external credentials vault' checkbox checked. Below it is explanatory text about integrating with an external vault. The 'Provider' dropdown is set to 'CyberArk (agent mode)' and the 'Application Id' text field contains 'denodo_production'. At the bottom right are 'Ok' and 'Cancel' buttons.

Configuration Category	Value
Cache	
Concurrent requests	
Credentials vault	☒ Use external credentials vault Enable the integration with an external credentials vault to retrieve the credentials for JDBC data sources. After this, enable this support on the JDBC data sources you want to use it. Provider: CyberArk (agent mode) Application Id: denodo_production
Default I18n	
HTTP proxy	
Identifiers charset	
Memory usage	
ODBC data sources	
Privileges	
Queries optimization	
REST web services	
Server authentication	
Server connectivity	
Stored procedures	
Threads pool	

You have now configured the communication with the CyberArk agent. After this, the developers can configure any JDBC data source to retrieve the user and password from the agent instead of entering a service account. To do this, they have to follow these steps:

1. Open the JDBC data source.

2. In this dialog, select **Obtain credentials from password vault**.
3. Enter the **Account name** that contains the credentials for this database. To speed up the retrieval of the credentials, also enter the "safe name". E.g., *ora_db\prod_18g*.
4. Click **Save**.

The screenshot shows a configuration window titled '* new_datasource'. It has a top bar with 'Configuration', 'Create base view', 'VQL', and 'Save' buttons. Below this are tabs for 'Connection', 'Read & Write', and 'Metadata'. The 'Connection' tab is selected. The form contains the following fields and options:

- Name: ds_jdbc_oracle_acct
- Database adapter: Oracle 18c
- Driver class path: 18c
- Driver class: oracle.jdbc.OracleDriver
- Database URI: jdbc:oracle:thin:@oracle-prod.acme.com
- Transaction isolation: Database default
- Authentication: Use login and password
- ☒ Obtain credentials from password vault
- Account name: ora_db\prod_18g
- ☐ Use Oracle Proxy Authentication with current user session
- ☐ Use other type of authentication to create base views

At the bottom, there are links for 'Initial SQL sentences', 'Connection Pool configuration', and 'Driver properties', and a 'Test connection' button.

PARTNER CONTACT INFO

Business Contact	Name	Ron Yu
	Email	ryu@denodo.com
	Tel	N/A
Technical Contact	Name	Carlos Santos Canelles
	Email	csantos@denodo.com
	Tel	N/A

Support Contact	Name	Support Team
	Email	support@denodo.com . When a customer or a partner runs into a bug/problem with Denodo, they open support case on our Support Site. In your case, due to the nature of the integration, it is unlikely you have to do this. https://support.denodo.com/
	Tel	The Support Team has a phone number for each region; find it at https://support.denodo.com/ .