CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Informatica Inc.

Website: www.informatica.com

Name of Product: Secure@Source

Version: v2.5

Date: 18 April 2016 (Revised 25 November 2020)

SECURE@SOURCE OVERVIEW

Informatica Secure@Source provides insights into sensitive data risks. Secure@Source automates the process of collecting all information around sensitive data, analyzing it, monitoring it, and providing a 360-degree view of risk. This enables security and IT teams to rapidly apply the right policies and controls to the most critical data. Secure@Source replaces costly, time-consuming manual efforts with automated discovery, identification, detection, scoring, and analysis of sensitive data risks.

Version: v2.5

KEY BENEFITS

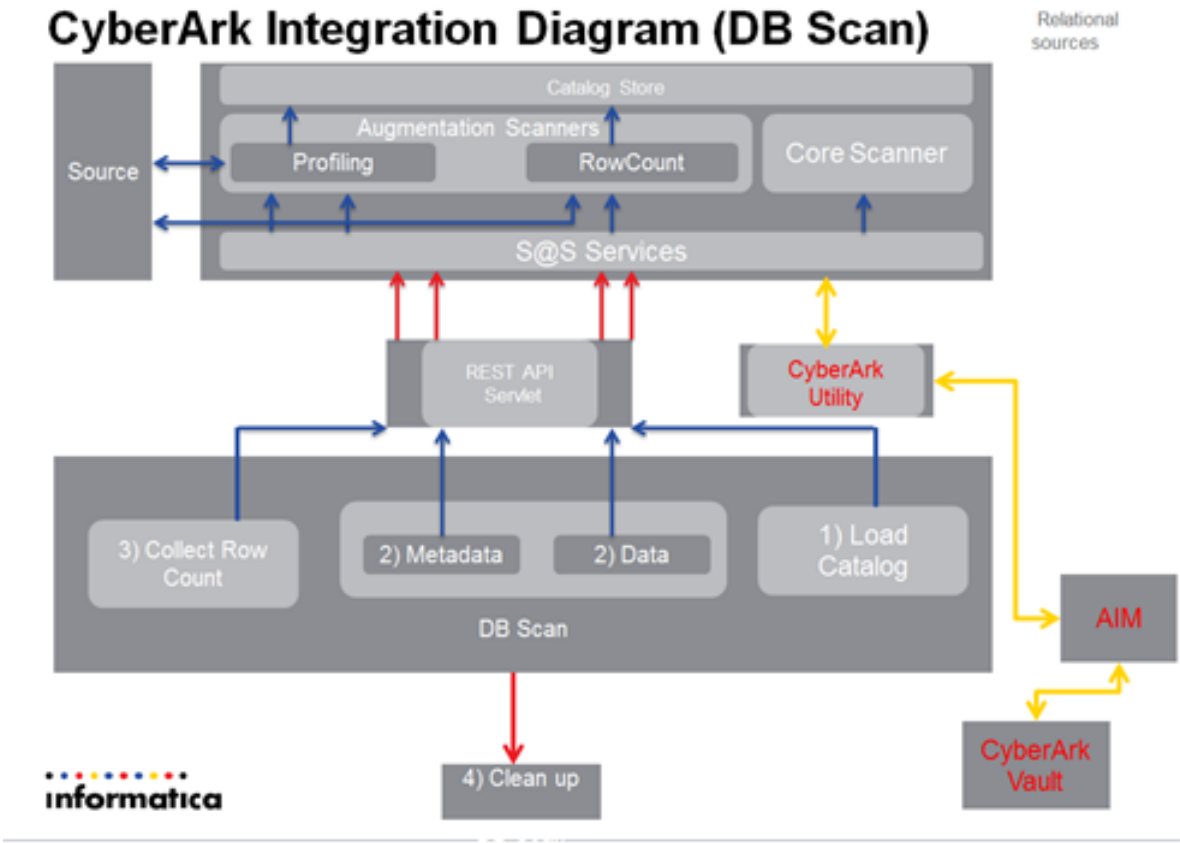
Secure@Source is a Data Security Intelligence solution that provides:

- Comprehensive visibility to data risks
- A quantified method to measure, track risks, and prioritize security investments
- Timely detection of threats on sensitive data

Integration with CyberArk simplifies management of and reduces security risks associated with credentials of high value data repositories. Integrating Secure@Source with Secrets Manager allows credentials to be requested on-demand rather than requiring manual population and local, secondary storage.

Integration with Secure@Source improves visibility of risks associated with sensitive data, enabling easy prioritization of investments for remediation or additional security controls. Gaps in coverage of high-risk systems and users can be targeted for CyberArk access or monitoring policies.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

A Secure@Source DB scan can contain up to three tasks. Each task will require password retrieval from CyberArk if the Db scanned is managed by CyberArk.

CREDENTIAL RETRIEVAL

A CyberArk password retrieval is executed:

- Every time a new Java Database Connectivity (JDBC) connection needs to be established within S@S (for example, a row count task).
- Every time a REST API request is sent to Logical Data Model (LDM) for Loading Catalog & for triggering profiling scanner. Whether a job is newly kicked off or resumed from error, pause, or stop operation, password retrieval will occur before invoking LDM REST API, in case the password has changed since the last retrieval operation.

Constant password retrieval is required as Secure@Source does not store an account password which is managed by CyberArk in our repository.

The required properties for a successful query are as follows:

- Host – An attempt will occur using alternative host name (FQN vs non-FQN) or IP depending on what was originally provided upon failure to find a unique result. This is retrieved from the DNS cache (if available).

- Port
- Username
- Database name (SID, Service name, or database name)
- CyberArk Safe to search
- Data store name (Object Name) (Only used if the first five attributes are yielding an exception indicating too many results found)

REQUIREMENTS

Users are recommended to enable Secrets Manager cache as it will increase performance when retrieving passwords from the local cache. It is highly recommended to select a cache refresh interval which is less than five minutes. Otherwise, this could lead to inaccurate password cache.

SECRETS MANAGER INSTALLATION

Secrets Manager Installation - link

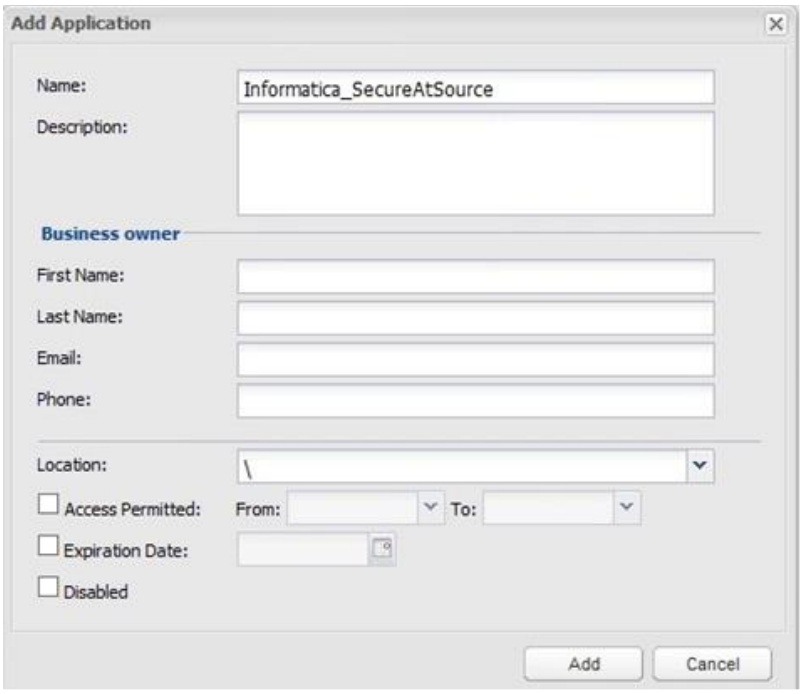
SECRETS MANAGER CONFIGURATION

The following sections provide details on Secure@Source configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

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

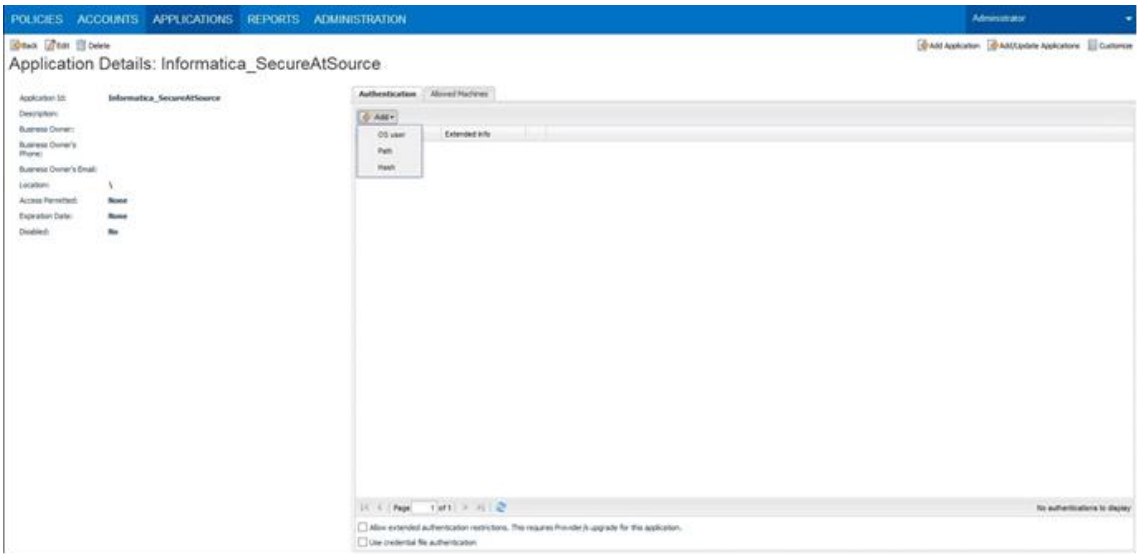
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



☐ Specify the following information:

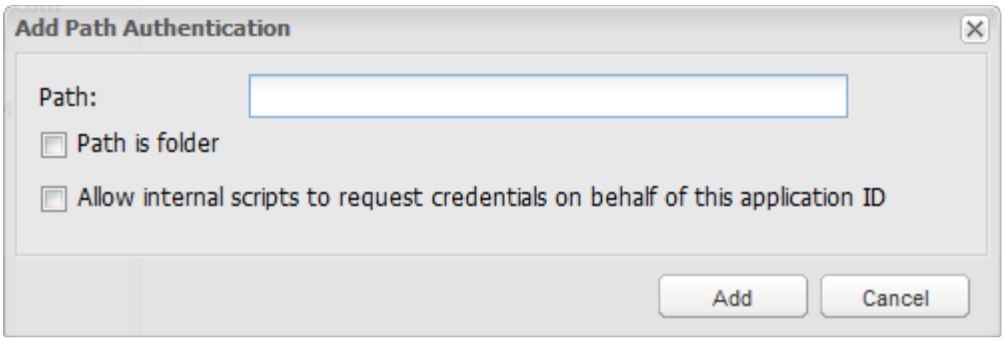
- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Informatica_SecureAtSource
- In the **Description** box, specify a short description of the application that will help you identify it.
- In the **Business owner** section, 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. Partner should suggest the authentication details to secure the access by the partner's application.
- ☐ 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.

- ☐ 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, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.

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

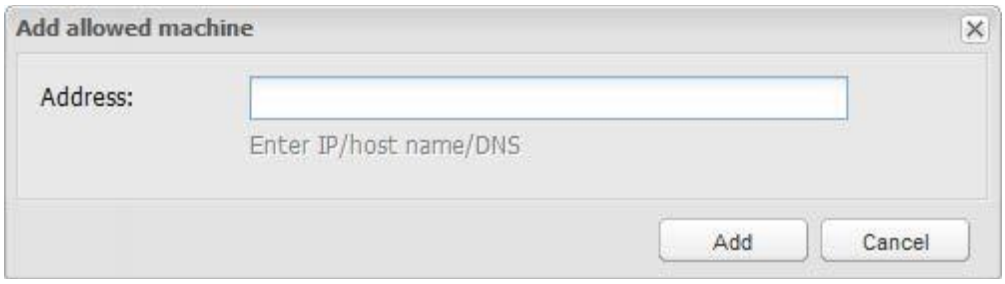
☐ Specify a hash:

- Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is 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, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 **#app2**
  Note: The comment must not include a colon or a semicolon.
- 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.



- 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 Secrets Manager 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 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.**

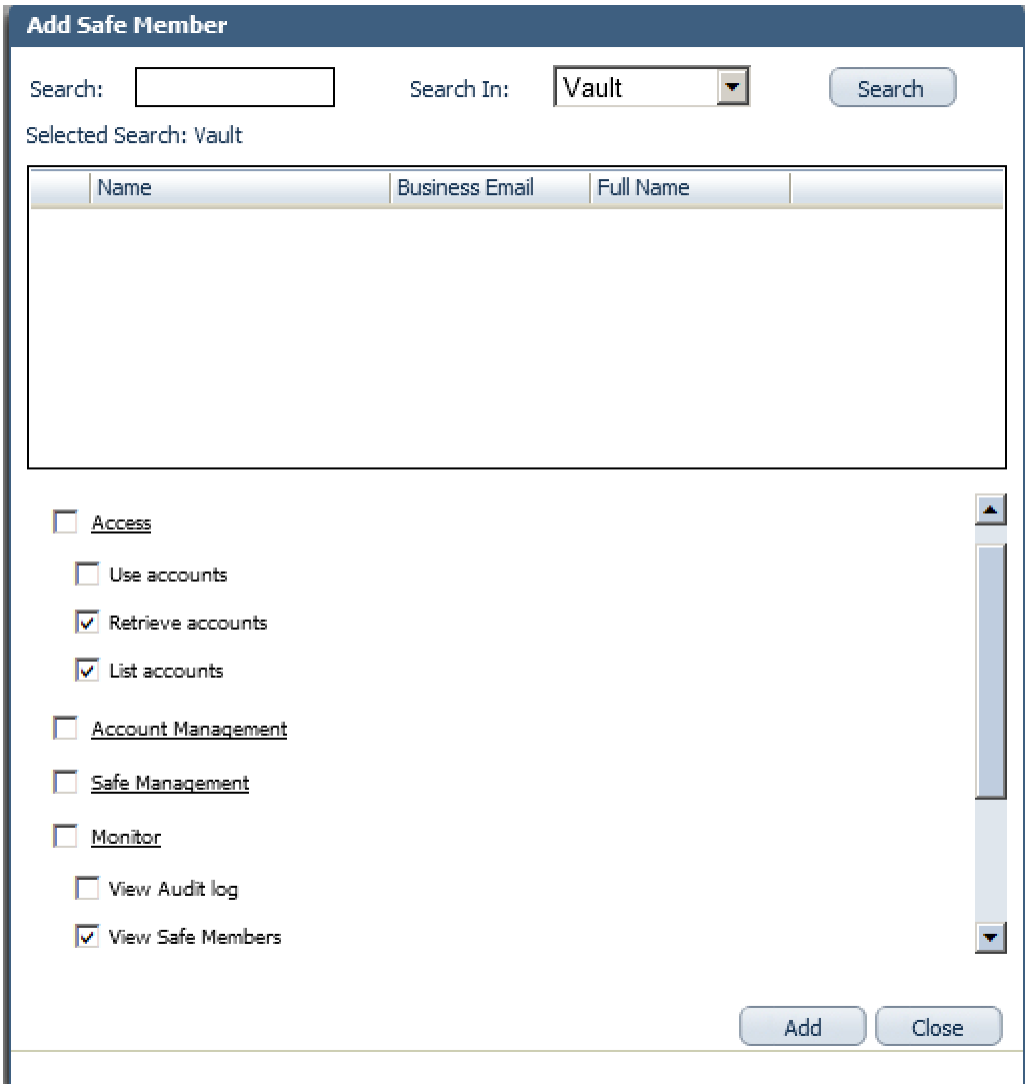
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

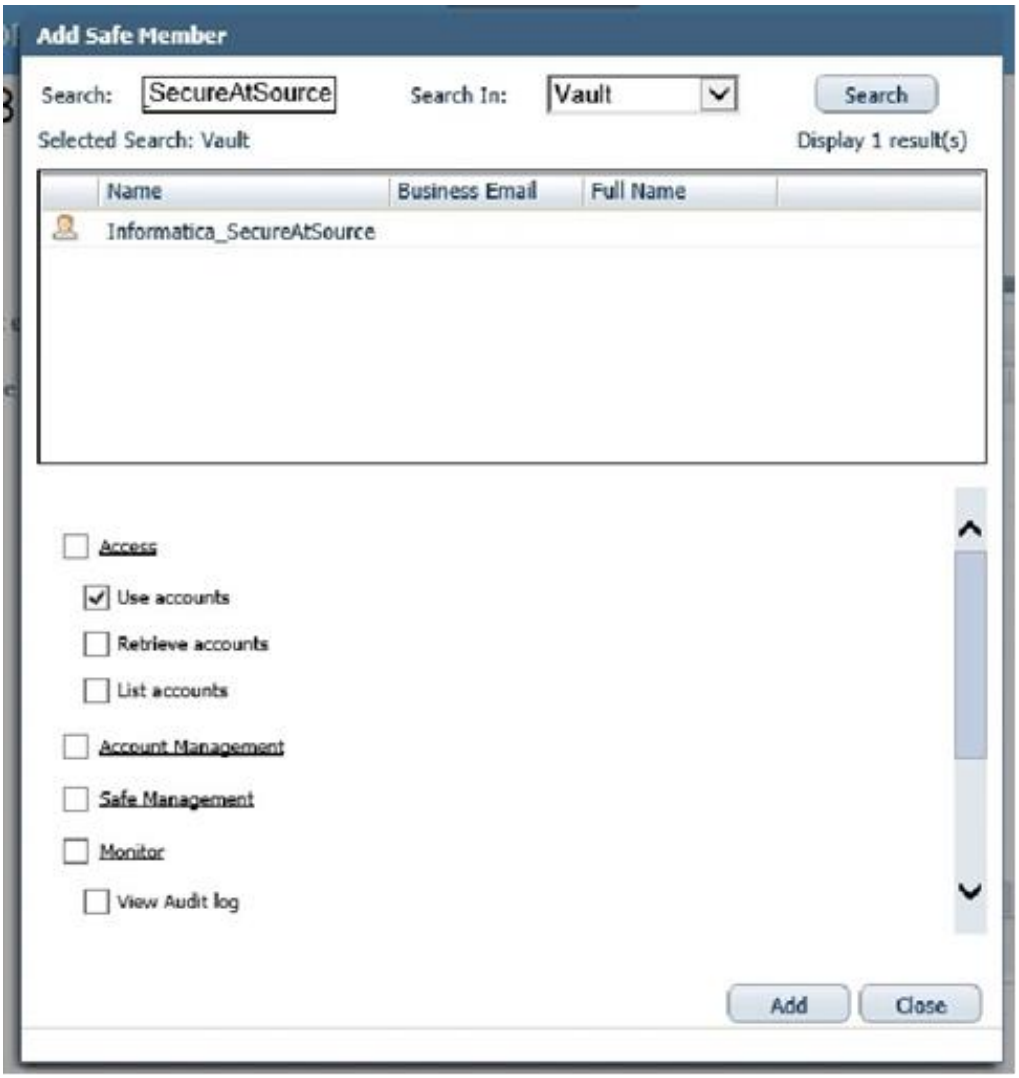
- List accounts
- Retrieve accounts
- View Safe Members

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 the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts



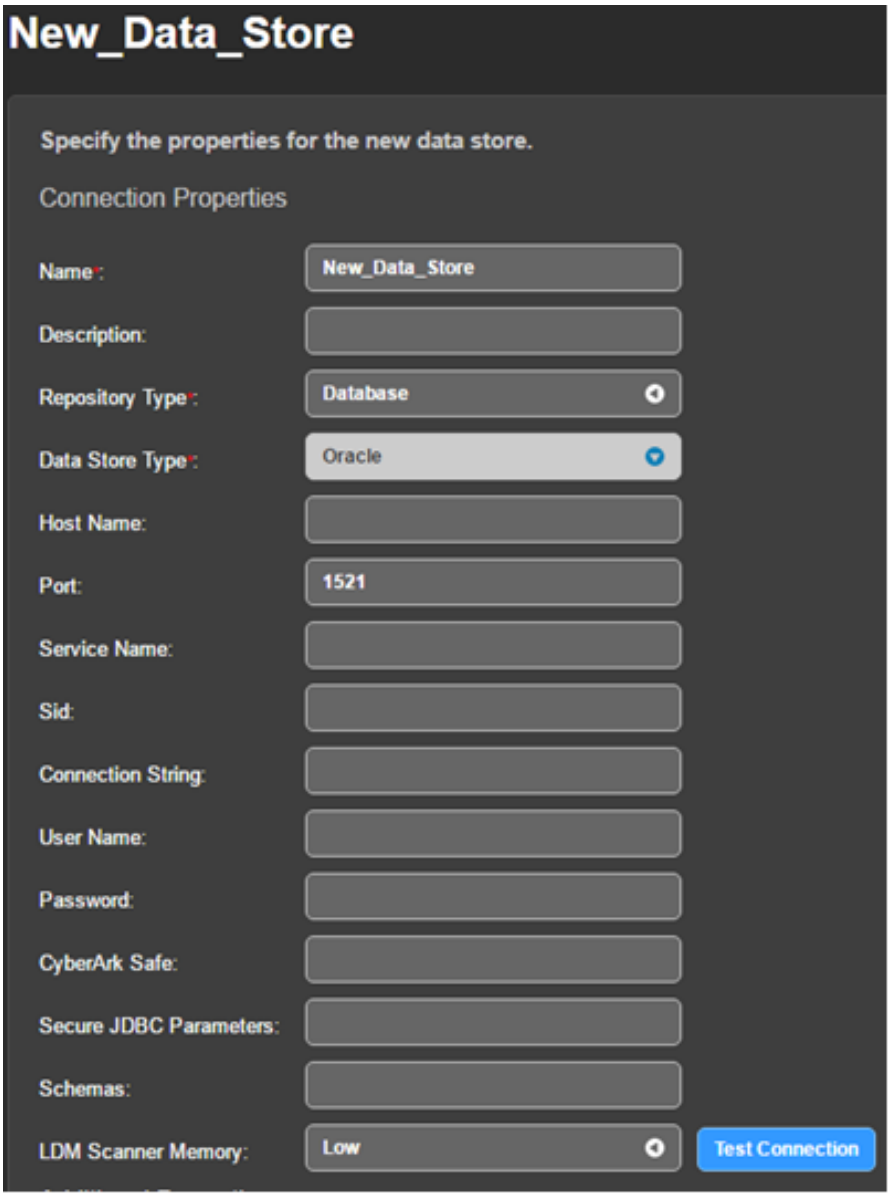
☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

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

SECURE@SOURCE INSTALLATION & INTEGRATION CONFIGURATION

List specific steps to configuring Partner Product to work with Secrets Manager, including:

1. Any special configurations within or outside the product
2. How to specify credentials for scanning, that are stored in the Vault (instead of providing usernames and passwords) – include screenshots and description of steps



Common use cases:

1. Windows domain credentials or other standard credentials
    a. The user will specify: username, address, platform
    b. Safe name – optional but recommended for increasing performance

2. Local accounts (windows/Unix)
    a. The user will specify: username & platform
    b. Safe name – optional but recommended for increasing performance
    c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned

3. Non-standard credentials (can't be unique with username+address+Platform)
    a. The user will specify: Safe and object name (folder is usually root by default)

PARTNER CONTACT INFO

Business Contact	Name	Christophe Hassaine
	Email	chassaine@informatica.com
	Tel	(650) 385-5337
Technical Contact	Name	Gary Paterson
	Email	gpatterson@informatica.com
	Tel	(650) 385-5638
Support Contact	Name	Senthil Kumaran Palanisamy
	Email	senthil@informatica.com
	Tel	(650) 385-5190