



Secrets Manager

(Agentless Central Credential Provider CCP)

Secrets Manager INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Privitar

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

Name of Product: Data Privacy Platform

Version: 4.0.1

Date: 30 November 2020

PARTNER SOLUTION OVERVIEW

Privitar Data Privacy Platform (PDPP) is a data privacy solution for managing data privacy policies to allow organisations to use sensitive data safely.

Integration with CyberArk will provide users an alternative to manage the secrets used in the configuration of the platform.

Version: 4.0.1

Platform components:

- Policy Manager
- Job Processor
- Event Broker (optional)

KEY BENEFITS

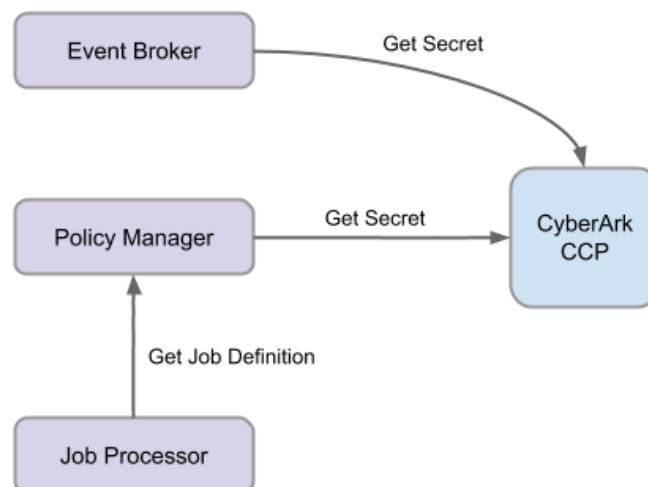
Benefits of Privitar Data Privacy Platform:

- Centralised management of data privacy policies
- Comprehensive set of privacy preserving techniques

Benefits of integrating Privitar Data Privacy Platform with CyberArk SECRETS MANAGER:

- Another way for users to manage credentials used by the platform

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Secrets Manager INTEGRATION

Policy Manager is responsible for managing privacy policies and providing them to Job Processors that apply those policies.

Event Broker is an analytics and diagnostics tool for the platform. The installation of this tool is optional.

In a typical installation, there will be 2 integration endpoints:

- one for the Policy Manager to retrieve credentials from an SECRETS MANAGER CCP
- one for Event Broker to retrieve credentials from an SECRETS MANAGER CCP

CREDENTIAL RETRIEVAL

There are four flows in which credential retrieval may occur:

- On start up of Policy Manager to fetch any credentials required by the application
- On start up of Event Broker to fetch any credentials required by the application
- When a Policy Manager user enters a new CyberArk CCP query for their team-specific Job processing credentials. Credential retrieval is performed to validate the query.
- When Policy Manager handles a request to retrieve a Job definition from a Job Processor to apply a privacy policy. Typical usage is below 100 requests per hour.

REQUIREMENTS

- The instance on which Policy Manager is deployed requires connectivity to a CyberArk CCP that has access to credentials specified in the Policy Manager configuration and Token Vault credentials for each PDPP Team.
- The instance on which Event Broker is deployed requires connectivity to a CyberArk CCP that has access to the credentials specified in the Event Broker configuration.

Secrets Manager INSTALLATION

Refer to the “Credential Provider Implementation Guide” for CyberArk Agentless installation and configuration.

Secrets Manager CONFIGURATION

The following sections provide details on Policy Manager configuration with CyberArk SECRETS MANAGER.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

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

Log in as a 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: PRIVITAR_POLICY_MANAGER

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☒ Access Permitted: From: To:

☒ Expiration Date:

☐ Disabled

Add Cancel

Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. This value must match the property **agrotera.cyberark.application_id** configured in the application properties file for that component. The recommended Application ID for this integration is **PRIVITAR_POLICY_MANAGER**.
- 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.

CYBERARK Last sign in: 11/11/2020 | Administrator

Back Edit Delete Add Application Add/Update Applications Customize

Application Details: PRIVITAR_POLICY_MANAGER

ApplicationId: PRIVITAR_POLICY_MANAGER

Description:

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: **None**

Expiration Date: **None**

Disabled: **No**

Authentication Allowed Machines

Add

Value	Extended Info
No authentications to display	

Page 1 of 1

☐ Allow extended authentication restrictions. This requires Provider/s upgrade for this application.

☐ Use credential file authentication

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.

Specify the Certificate Serial Number.

Add Certificate Serial Number Authentication

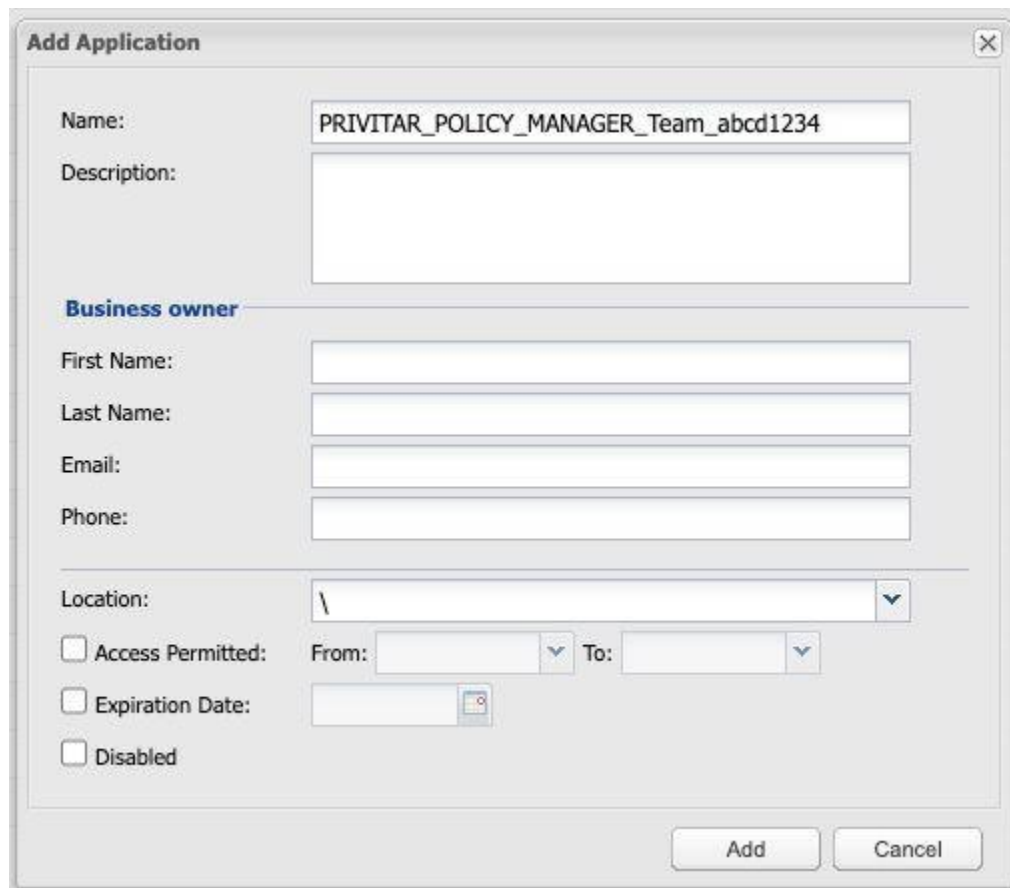
SN:

Add Cancel

DEFINING THE TEAM APPID AND AUTHENTICATION DETAILS

To define an application for a Team that requires access to their own set of secrets, create it manually through the CyberArk Password Vault Web Access (PVWA) interface:

Log in as a 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 for the team. This name must be defined using the format given by the Privitar application property **agrotera.cyberark.application_id.team_format**.
By default, the format is specified as **{globalAppId}_Team_{teamId}**.
For example if the **globalAppId** given by **agrotera.cyberark.application_id** is to PRIVITAR_POLICY_MANAGER and **teamId** is abcd1234, then the name to add here is **PRIVITAR_POLICY_MANAGER_Team_abcd1234**.
For more information about Teams and teamId, see PDPP User Guide.
- 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.

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 set up the access to both the application and CyberArk Application Password Providers serving the Application.

Add the provider user (where the Central Credential Provider is installed) 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 1 result(s)

Name	Business Email	Full Name
 PRIVITAR_POLICY_MANAGER		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☒ View Safe Members

☐ Workflow

Add the application (e.g. **PRIVITAR_POLICY_MANAGER** for Policy Manager or **PRIVITAR_POLICY_MANAGER_Team_abcd1234** for a team-specific application) as a Safe Member with the following authorizations:

- Retrieve accounts

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

	Name	Business Email	Full Name
	PRIVITAR_POLICY_MANAGER		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

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

The Privitar platform is typically deployed as part of a customer privacy implementation project with Privitar Professional Services. Privitar platform components will be used to deliver an Enterprise Privacy Service capable of addressing privacy protection use cases across the customer's enterprise.

An implementation project takes customers through the following set of delivery phases:

- Requirements gathering including functional, non-functional and service-oriented (including CyberArk if required).
- Design and documentation of a full Privitar service solution.
- Implementation phasing and planning.
- Installation of Privitar components and configuration and integration with enterprise infrastructure.
- Functional and non-functional platform testing.
- Service definition and enablement.
- Training and knowledge transfer.

Privitar Professional Services enables customers - using a combination of training and documentation - to install and configure subsequent platform deployments/upgrades.

Please contact them for more information about Partner Product installation.

To configure CyberArk CCP as the external secrets provider for a Privitar component, the parameters are specified in the **application.properties** file for that component.

To enable CyberArk CCP:

- **agrotera.secret_provider** must be set to **CYBERARK_CCP**

The following properties should also be specified:

- **agrotera.cyberark.provider_url** (*required*) - CyberArk Central Credential Provider web service URL e.g. **https://<host name>:<port>/AIMWebService**
- **agrotera.cyberark.application_id** (*required*) - The global Application ID which identifies the Privitar component created in CyberArk. Please note that Application IDs containing '+' or '&' are not supported.
- **agrotera.cyberark.application_id.team_format** (*optional*) - The format to be used when defining a specific Team in Privitar to make requests to CyberArk. The default is **{globalAppId}_{teamId}**. The supported placeholders are:
 - {globalAppId} - this will substitute in the global Application ID
 - {teamId} - this will substitute in the Team Id of the Team making the request for retrieving team-specific credentials
- **agrotera.cyberark.certificate.authority** (*optional*) - Path to the trusted certificate
- **agrotera.cyberark.certificate.path** (*optional*) - Path to the client certificate
- **agrotera.cyberark.certificate.secret** (*optional*) - Password for the client certificate, please note that this is required if **agrotera.cyberark.certificate.path** is specified

DESCRIPTOR FORMAT

Use the following format for the descriptor:

Safe=<safe name>;Folder=<folder name>;Object=<object name>##<attribute> , where:

- safe name - optional but recommended for increasing performance
- folder name - optional, defaults to Root
- object name - specifies the name of the password object to retrieve
- attribute - optional, defaults to Content. The name of the value to be retrieved, e.g. "Content" returns the password and "UserName" returns the optional username value.

Examples:

- This example specifies an Object without specifying the folder:
Safe=Privitar;Object=PM-config-db##UserName
- This example does not specify the attribute which means "Content" will be retrieved:
Safe=Privitar;Folder=Test-Env;Object=PM-config-db

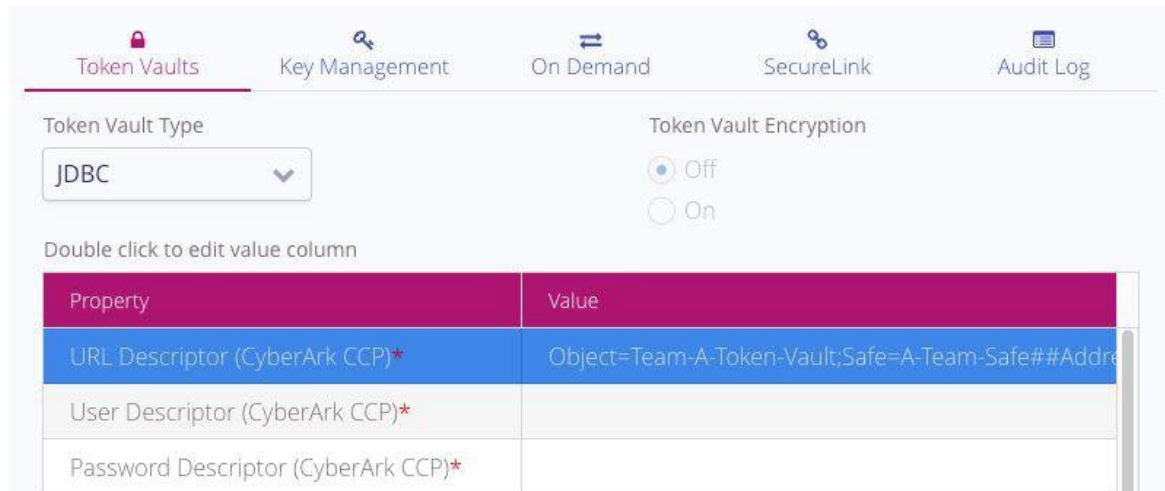
USE CASE: APPLICATION CONFIGURATION CREDENTIALS RETRIEVAL

Properties in **application.properties** file (excluding `agrotera.secret_provider` and `agrotera.cyberark.*`) can be configured to retrieve the value from CyberArk by adding the suffix **.secret_descriptor** to an existing property. e.g.

agrotera.database_user.secret_descriptor=Safe=Privitar;Object=PM-config-db##UserName

USE CASE: TEAM-SPECIFIC CREDENTIALS RETRIEVAL

Users can configure their team's Environments to fetch JDBC Token Vault credentials from the CyberArk Central Credentials Provider. This can be achieved using the PDPP UI (shown below) or the PDPP v3 APIs.



Token Vaults Key Management On Demand SecureLink Audit Log

Token Vault Type:

Token Vault Encryption: ☒ Off ☐ On

Double click to edit value column

Property	Value
URL Descriptor (CyberArk CCP)*	Object=Team-A-Token-Vault;Safe=A-Team-Safe##Address
User Descriptor (CyberArk CCP)*	
Password Descriptor (CyberArk CCP)*	

PARTNER CONTACT INFO

Business Contact	Name	Shawn James
	Email	shawn.james@privitar.com
	Tel	+1 510-928-5530
Technical Contact	Name	Mandy Choi
	Email	mandy.choi@privitar.com
	Tel	+44 203-282-7136
Support Contact	Name	https://privitar.zendesk.com/hc
	Email	support@privitar.com
	Tel	+44 203- 929- 3801 (available during business hours)