

SECRETS MANAGER INTEGRATION

(Agentless Central Credential Provider CCP)

Name of Company: Smart Robotic Process Automation

Website: <http://smartrpa.com>

Name of Product: SmartRPA Catalyst

Version: 6.6.0

Date: 2021-10-18

PARTNER SOLUTION OVERVIEW

Many organizations are having difficulties in getting to a point where they can scale their RPA solution. SmartRPA Catalyst prepare these organizations for scale. Further, SmartRPA Catalyst addresses the challenges that organizations who are scaling will undoubtedly meet, in the form of exponentially increasing operational complexity. SmartRPA Catalyst is providing a solid foundation for the pillars of scalable RPA automation:

1. Standardization, modularity & reusability
2. Simplifying scheduling & execution
3. Granular monitoring & reporting on tasks
4. Seamless human / robot interaction
5. Strong data security & governance

SmartRPA Catalyst ensures the lowest possible TCO and highest ROI for the RPA venture.

PageVersion: 6.6.0

Platform components:

- All-in-one SmartRPA Catalyst web application

KEY BENEFITS

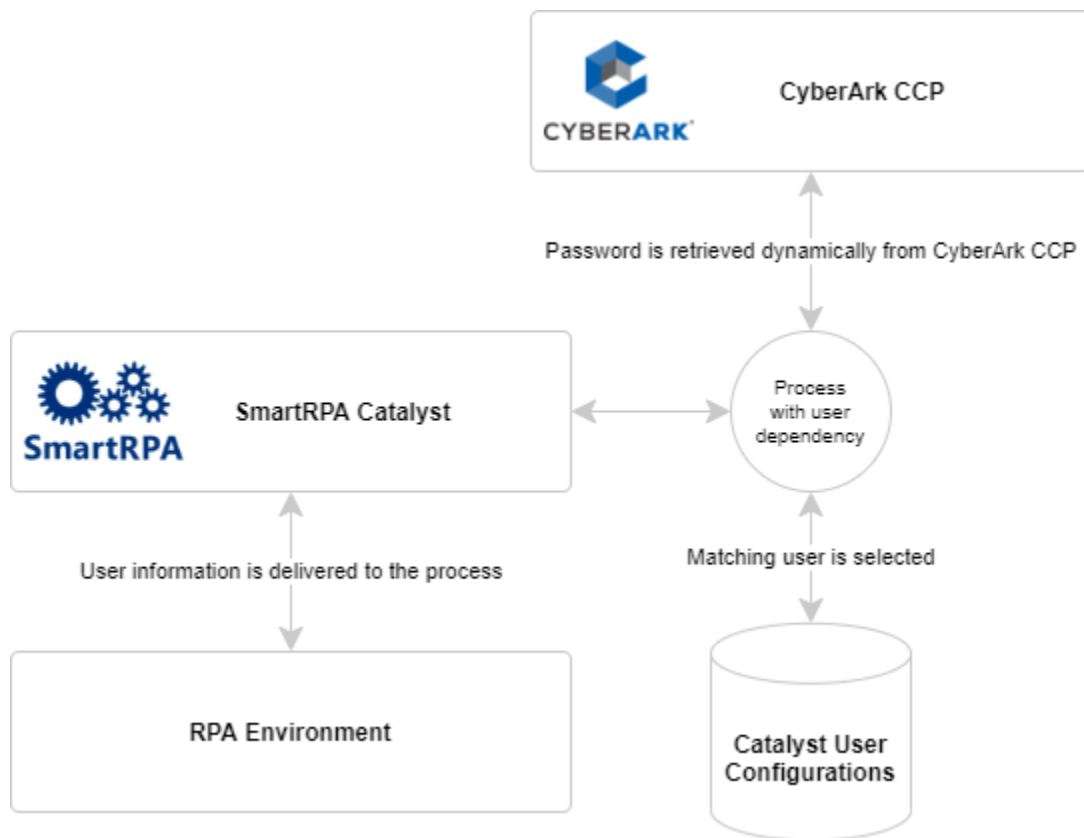
Benefits of SmartRPA Catalyst:

- Increased automation of existing RPA Platform
- Robust and integrated process framework
- Security audit trail with desktop integration
- Self-service access for users and business units

Benefits of integrating SmartRPA Catalyst with CyberArk Secrets Manager:

- Seamlessly utilize an existing CyberArk Secrets Manager setup
- Configured users in SmartRPA Catalyst are not affected by password rotation policies

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Secrets Manager INTEGRATION

SmartRPA Catalyst's CyberArk CCP integration is built-in and does not need to be installed separately. The Catalyst setup does not need to be changed to accommodate the integration and works out of the box whether it is run in high availability (multiple instances), or just one instance.

CyberArk CCP can be configured as a credential store for a user. With such a configuration, instead of retrieving the user's credentials from Catalyst's built-in credential store, the password will instead be retrieved from the CyberArk vault. As a result, the user's credentials are not stored on the Catalyst, and instead delivered directly to the process in which the credentials are required.

CREDENTIAL RETRIEVAL

In most cases, when automating a system credentials are required to access it. Naïve solutions embed credentials directly in the RPA process, but this approach exposes credentials to anyone with even read access to the project. For this reason, a better solution is for the process to dynamically obtain the required credentials, so that their storage is not directly tied to the deployment of the process.

In SmartRPA Catalyst, each execution will advance a task to the next state, often advancing multiple tasks in one execution. Due to the nature of the automated programs, this usually means that one execution will retrieve the required credentials once and use them to log in to a system once per execution.

REQUIREMENTS

SmartRPA Catalyst supports integration with CyberArk CCP out of the box. Therefore, the requirements are simply as follows:

- Existing Secrets Manager CCP Agentless installation
- Existing SmartRPA Catalyst installation

Secrets Manager INSTALLATION

Refer to [CyberArk Agentless installation and configuration](#).

Secrets Manager CONFIGURATION

The following sections provide details on SmartRPA Catalyst 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.

The screenshot shows the 'Add Application' dialog box with the following fields and values:

- Name:** SmartRPA-Catalyst
- Description:** Agentless integration with SmartRPA Catalyst
- Business owner:**
 - First Name:** John
 - Last Name:** Smith
 - Email:** example@smarttpa.com
 - Phone:** +1-202-555-0124
- Location:** \
- Access Permitted:** From: [] To: []
- Expiration Date:** []
- Disabled:** []

Buttons: Add, Cancel

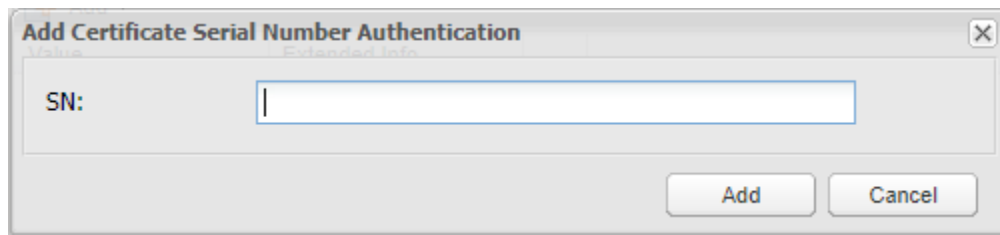
- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: SmartRPA-Catalyst

- 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.
- ☐ Specify the Certificate Serial Number.



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 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:

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

- ☐ 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

In SmartRPA Catalyst, ensure you have the MODIFY_RESOURCES permission for the selected entity, and navigate to the CyberArk CCP page.

Dev

Catalyst
6.2_dev_build

Dashboard

Alerts

Execution

Queues

Resources

Entity

Access Roles

Your Current Roles

Calendars and Work Plans

Management Console Credentials

Kofax Login Robot Configurations

Blue Prism Connections

UiPath Orchestrators

CyberArk CCP

RDP Configurations

Configuration Entries

API Tokens

Settings

Global

Other

CyberArk Central Credential Provider

Configure a connection to CyberArk Central Credential Provider to serve as a credential store for user resources in Catalyst.

Base URL*

The URL at which the CyberArk Central Credential Provider is hosted (for example: https://example.com:1234/AIMWebService).

Folder

The folder in which Catalyst can find the credentials of users corresponding to those configured on Catalyst.

Application Id*

The id of the configured application for Catalyst in CyberArk CCP.

Safe*

The safe to which Catalyst has access to in CyberArk CCP.

Key

The password protected key store file (usually .p12, PKCS#12), used when authenticating with CyberArk CCP

Key Password

The password with which the key is encrypted.

Fill out the relevant connection information for CyberArk CCP, including uploading the key file containing the certificate needed for Client Certificate authentication.

Once configured, CyberArk CCP can be specified as the credential store for any user:

Dev SmartRPA Catalyst 6.2_dev_build

Users

This shows de

1 - 1 of 1 ite

Username

TestUser

Edit User

Note: some properties of users cannot be edited, such as whether to return credentials or how the password is encrypted. To change the actual password, please use the 'Change Password' action from the user context menu.

Username*

TestUser

Password

Credential Store

CyberArk CCP

Built-in

CyberArk CCP

☐ **Return Credentials**

If checked, the user credentials will be returned with the lease. Otherwise, only the leasing token, used to generate a session and logging in to desktops, is returned.

Pool Membership

Not a member of any pools.

Choose a pool to add membership

Notes

Cancel Save

This, of course, assumes there exists a user named “TestUser” in the CyberArk vault.

PARTNER CONTACT INFO

Business Contact	Name	Flemming Weber
	Email	fw@smarttpa.com
	Tel	+45 2329 2545

Technical Contact	Name	Mads Kahler
	Email	mk@smarttpa.com
	Tel	+45 5136 8483
Support Contact	For support inquiries, create a support ticket at: https://support.smarttpa.com	