



Secrets MANAGER INTEGRATION (CCP)

Secrets Manager Integration - Technical documentation

Name of Company – UiPath SRL

Website – www.uipath.com

Name of Product – UiPath Orchestrator

Version – 2020.4

Date – May 2020

SOLUTION OVERVIEW

UiPath Orchestrator is a web application that enables you to orchestrate your UiPath Robots in executing repetitive business processes.

Orchestrator lets you manage the creation, monitoring, and deployment of resources in your environment.

It acts as an integration point with third-party solutions and applications.

Its power comes from its capability of managing your entire Robot fleet.

You are able to run debugging in Studio with all types of Robots.

Orchestrator Main Capabilities

- **Provisioning** - creates and maintains the connection between Robots and web application
- **Deployment** - assures the correct delivery of the package versions to the assigned Robots for execution
- **Configuration** - maintains and delivers Robot environments and processes configuration
- **Queues** - ensures automatic workload distribution across Robots
- **Monitoring** - keeps track of Robot identification data and maintains user permissions
- **Logging** - stores and indexes the logs to an SQL database and/or Elasticsearch (depending on your architecture and configuration)
- **Inter-connectivity** - acts as the centralized point of communication for 3rd party solutions or applications

The latest version of our Platform is 2020.4 and includes CyberArk CP, CyberArk CCP, CyberArk PSM, CyberArk CPM integration

KEY BENEFITS

Auditable Execution Trace. Highly auditable compliance is supported by robot log files, aggregated at the server level, which record end-to-end activity data, easily queried and reported using Elastic Search.

Web Based Control Panel. Server level, web-based management consoles are used for robot deployment, monitoring and operational reporting.

Release Management. Robust release management enables multiple versions of a published process on the server. The process reviewer can release a stable process version to robot groups for execution.

Process Monitoring. Active robots send a constant “heartbeat” to the server as a sign of operational health. Process performance is monitored, and alerts can be raised in case of failures.

Remote Control. Back Office Robots are remotely deployed, monitored, and retired from the control center.

Centralized Scheduling. Deployment and scheduling of processes to robot groups is centralized and handled by the control center.

Asset Manager. Assets are variables that are stored on server and can be changed. They can be defined per robot.

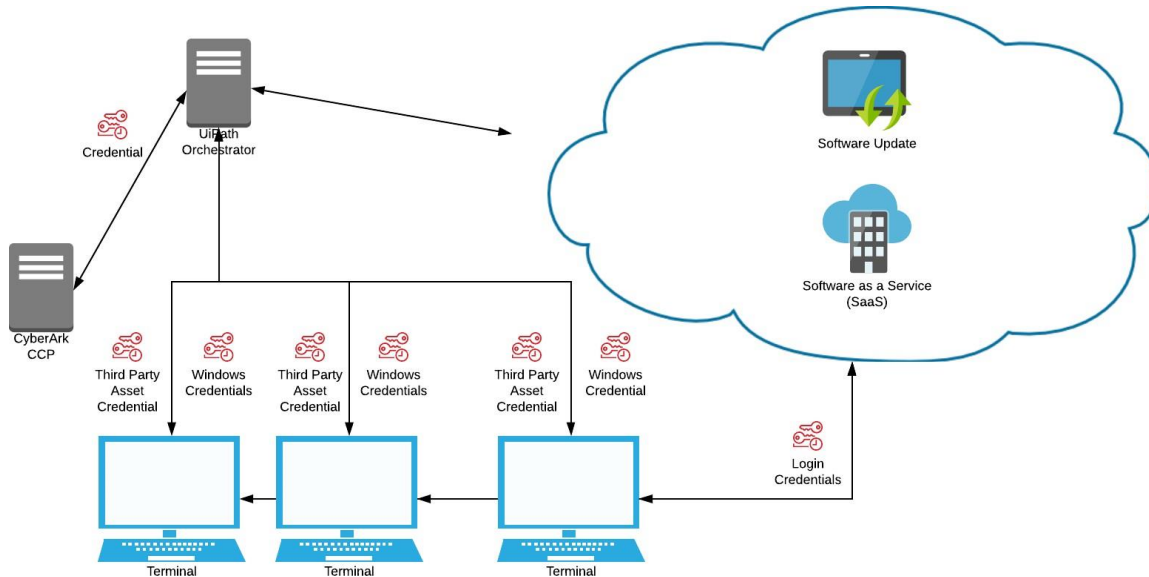
Transaction Queue. The built-in transaction queue system stores work items on the server and makes them available to robot groups.

Enhanced Exception Handling. Robots are instructed to retry a failed transaction before sending an exception message to the server.

Web Based Control Center. A server-level management tool that consolidates and displays key robot/process metrics - while also providing utilities for: transaction queues, robot scheduling, deployment, reassignment, and retirement.

Having an integration with CyberArk will allow our customers to store Windows Login Credentials and Third-party software credentials (aka Credential Assets) securely. UiPath Robots will be able to retrieve through the Orchestrator, the credentials that they will be using for performing automations in a secure manner.

INTEGRATION DIAGRAM & DESCRIPTION



I. Describe Partner Product and depict where Secrets Manager integration lies.

- UiPath Orchestrator manages the entire fleet of Robots deployed in a customer environment.
- CyberArk Central Credential Provider can be installed on any machine that can communicate with the UiPath Orchestrator is installed.
- CyberArk CCP connector is an agentless integration that does not need to be installed on the same machine where Orchestrator is also installed, as opposed to the CyberArk CP integration.

II. Describe how the credential retrieval plays a role within the Partner product. Describe the flow in detail.

- When connecting the UiPath Robot to the Orchestrator, it is required to provide the Robot with the Windows login details (username and password) with specific rights on that machine. These credentials will be used by the UiPath Robot to open the Windows session in which it will perform the triggered job/automation from Orchestrator.
- During the triggered job/automation, the Robot needs to retrieve third party software credentials, stored as Assets in the Orchestrator. These Credential Assets, can also be stored in the CyberArk vault, and retrieved via the same procedure.
- To enable storing and managing them from a third-party enterprise-grade credential store, we created an integration between UiPath Orchestrator and CyberArk CCP.
- Credentials are retrieved automatically when multiple entities (UiPath Robots) are connecting to our UiPath Orchestrator and requesting credentials to execute automations.

- Credentials are retrieved whenever our UiPath Robot entities require the login credentials for a specific account.
- Describe specific properties required for queries on various platforms:
 - 1 query that checks for the account existence and the password based on account name.
 - 1 query that retrieves the password based on account name.

CYBERARK CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the Application, here are the instructions to define it manually via CyberArk's PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed 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. The 'Name' field contains 'Orchestrator'. The 'Description' field contains 'RPA Server UiPath Orchestrator'. Under the 'Business owner' section, there are empty fields for 'First Name', 'Last Name', 'Email', and 'Phone'. The 'Location' dropdown is set to '\'. The 'Access Permitted' checkbox is unchecked, with 'From' and 'To' dropdowns. The 'Expiration Date' checkbox is unchecked, with a date picker icon. The 'Disabled' checkbox is unchecked. At the bottom right are 'Add' and 'Cancel' buttons.

2. Specify the following information:

- In the Name edit box, specify the **Orchestrator**.
- In the Description, 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 lowest section, 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.

3. Click **Add**; the application is added and is displayed in the Application Details page.

- **Allowing extended authentication restrictions.** This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.

4. Under the application details click add, select certificate serial number and fill it in. This will allow authentication with the certificate.

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 (Step 1). 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 (Step 2).

1. 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 the UiPath Robots to correctly identify the Privileged accounts and be able to retrieve the passwords, the accounts must be provisioned in the Password Safe using one of the following naming conventions for the ObjectName of the account:

- domainName-username – for domain users.
- machineName-username – for local users.

For credentials assets, the asset name or asset external name must be the exact same name in CyberArk (custom name) as in the Orchestrator. If the external name is present it will be used, if not the name will be used to identify the CyberArk entity.

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

2. 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.

i. 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

- ii. Add the application (the APPID) 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
Orchestrator		

☐ Access

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

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

Orchestrator has been added.

- iii. If your environment is configured for dual control:
- In Privileged Account Security solutions , when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- iv. 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 Account Security Implementation Guide**.

ORCHESTRATOR INSTALLATION & INTEGRATION CONFIGURATION

To enable the integration between UiPath Orchestrator and CyberArk CCP you would need to do the following:

Certificates configuration:

1. Import the Root CA for the client certificate that you want to use in the *Trusted Root Certificate Authorities* in the Local Machine store.
2. Import the client certificate in the Local Machine store making sure that the key is marked as exportable and extended properties are included.

✕

←  Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☒ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☐ Protect private key using virtualized-based security(Non-exportable)

☒ Include all extended properties.

Next Cancel

Web Config and Orchestrator configuration:

1. Copy the CyberArkCCP plugin assembly (dll) in the UiPath's Orchestrator *plugins* folder.
2. Navigate to Orchestrator's web.config file and open it with a text editor, such as Notepad++.
3. Configure the parameter
`<add key="Plugins.SecureStores" value="<CyberArkCCP Dll name>.dll"/>`
3. Save the file.
4. In the UiPath Orchestrator, go to the credential store page.
5. Select the CyberArkCCP plugin and fill in the information as seen in the following image:

Add Credential Store

Type *

CyberArkCCP



Name *

CCP URL *

CyberArkCCP Certificate thumbprint *

Application ID *

CyberArkCCP Safe *

CyberArkCCP Folder

CANCEL

CREATE

PARTNER CONTACT INFO

Business Contact	Name	Bogdan Nedelcov
	Email	bogdan.nedelcov@uipath.com
	Tel	
Technical Contact	Name	Ion Dinica
	Email	ion.dinica@uipath.com
	Tel	
Support Contact	Name	Ion Dinica
	Email	ion.dinica@uipath.com
	Tel	