



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: AutomationEdge Inc.

Website: www.automationedge.com

Name of Product: AutomationEdge

Version: 5.2.0

Date: 7 September 2018 (Revised 27 October 2020)

AUTOMATIONEDGE OVERVIEW

AutomationEdge is an IT automation and Robotic Process Automation (RPA) solution provider. AutomationEdge helps organizations automate their mundane, repetitive rule-based tasks across verticals.

In its short stint, AutomationEdge has already delivered its innovative solution to large multinationals globally like American Express, Capita, Coty, ICICI Lombard, HDFC Life, Smart Dubai Government,

Mashreq Bank, and Genpact to name a few. It is a unified platform that helps in automated resolution of IT tickets like password reset user creation as well as automates various business processes in front, middle, and back office. AutomationEdge is also listed in the Salesforce AppExchange.

Version: 4.1.0.0

AutomationEdge runs on Windows, Linux and Mac-OS.

KEY BENEFITS

AutomationEdge is an Intelligent Robotic Process Automation product which comes bundled with key essential technologies for automation of front office, middle office, back office, and IT operations. AutomationEdge provides chatbots, intelligent automation bots, and AI and machine learning capabilities that help clients reduce costs, improve response time, increase business, and achieve compliance. AutomationEdge provides ready Bots and development environment to build new Bots.

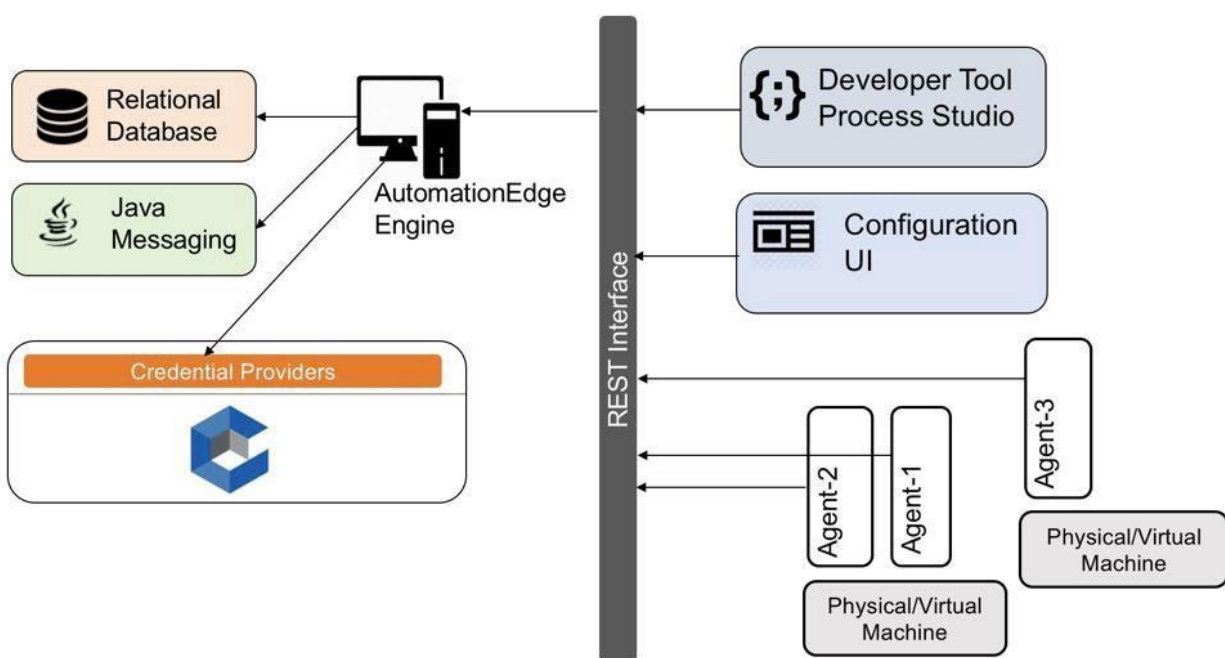
Part of any automation involves talking to different software systems. In order to do so, bots need to authenticate with these systems for which they need to provide valid credentials and hence, credentials need to be securely stored somewhere. CyberArk PAS solution offers many capabilities including:

- Storing, leasing, and revocation of secrets
- Managing encryption and decryption of secrets
- Rolling over keys used for encryption
- Auditing all operations done on secrets

With this integration, AutomationEdge will fetch credentials from CyberArk security vault when they are needed for execution of business processes.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

The diagram below is the high-level architecture diagram of AutomationEdge.

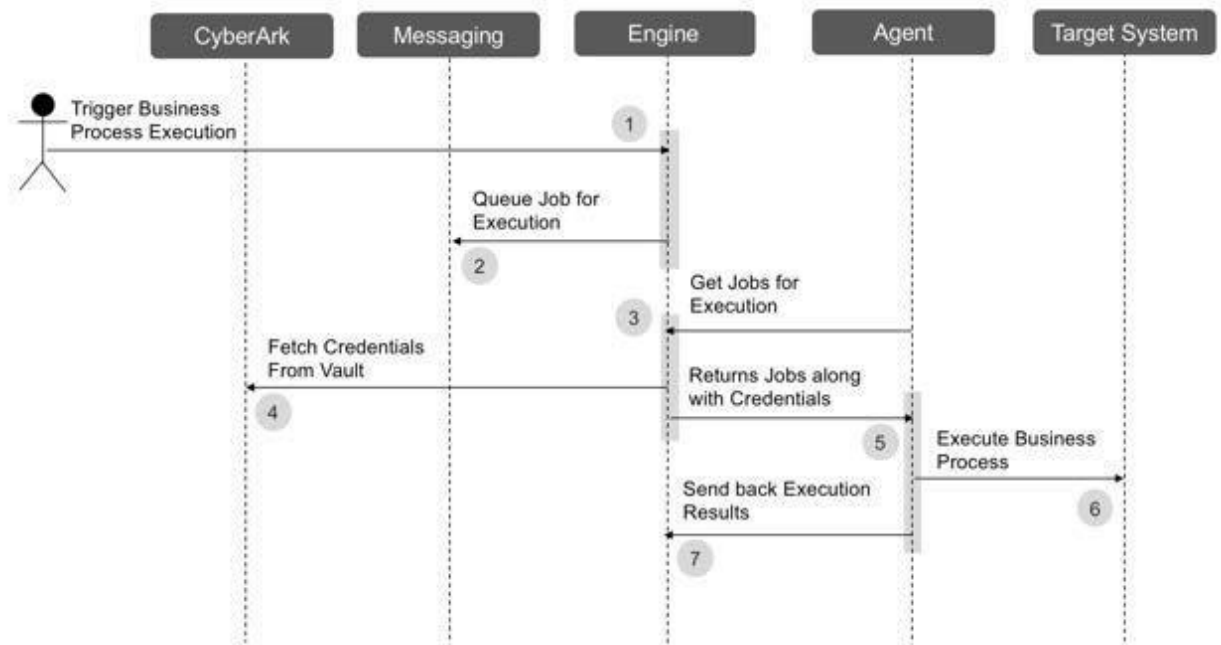


SECRETS MANAGER INTEGRATION

AutomationEdge Engine is the orchestrator of all business process executions with AutomationEdge Agents or Bots carrying out executions. Credentials needed for automations can reside within AutomationEdge database itself (called as Native credentials) or they can reside inside a security vault like CyberArk. AutomationEdge engine has a component called 'Credential provider' which manages communication with security vaults, and it is the ONLY component within AutomationEdge which talks to security vaults. AutomationEdge Engine can be deployed in HA (high availability) mode which would mean more than one AutomationEdge Engine can potentially talk to the security vault.

CREDENTIAL RETRIEVAL

The diagram below shows how execution of a business process happens inside AutomationEdge and where security vaults like CyberArk fit in.



- A business process execution is triggered in AutomationEdge, either through a REST API or a scheduler of the configuration UI. The business process might one or more credential objects as input parameters.
- The engine queues up the execution requests.
- When an Agent asks for 'Jobs', the engine first finds a matching business process and hands it over to the Agent. However, before handing it over to the Agent, it also fetches credential values from security vault.
- The agent carries out the execution of the business process, utilizing the provided credentials and returning the execution response to the Engine.

The number of times a credential object would be used (and, in turn, the number of times the vault would be accessed) depends on number and frequency of business processes.

SECRETS MANAGER INSTALLATION

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

AutomationEdge has notion of Vault Master, which is a list of all security vault solutions it supports. In order to use CyberArk with AutomationEdge, you need to create a ‘Vault connection’ object (by selecting CyberArk as Vault Master Type) and provide connection URL and username (CyberArk ApplicationID) and password. Once this is done, you can use this connection object while creating credentials in AutomationEdge as explained in subsequent sections.

SECRETS MANAGER CONFIGURATION

The following sections provide details on AutomationEdge 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:

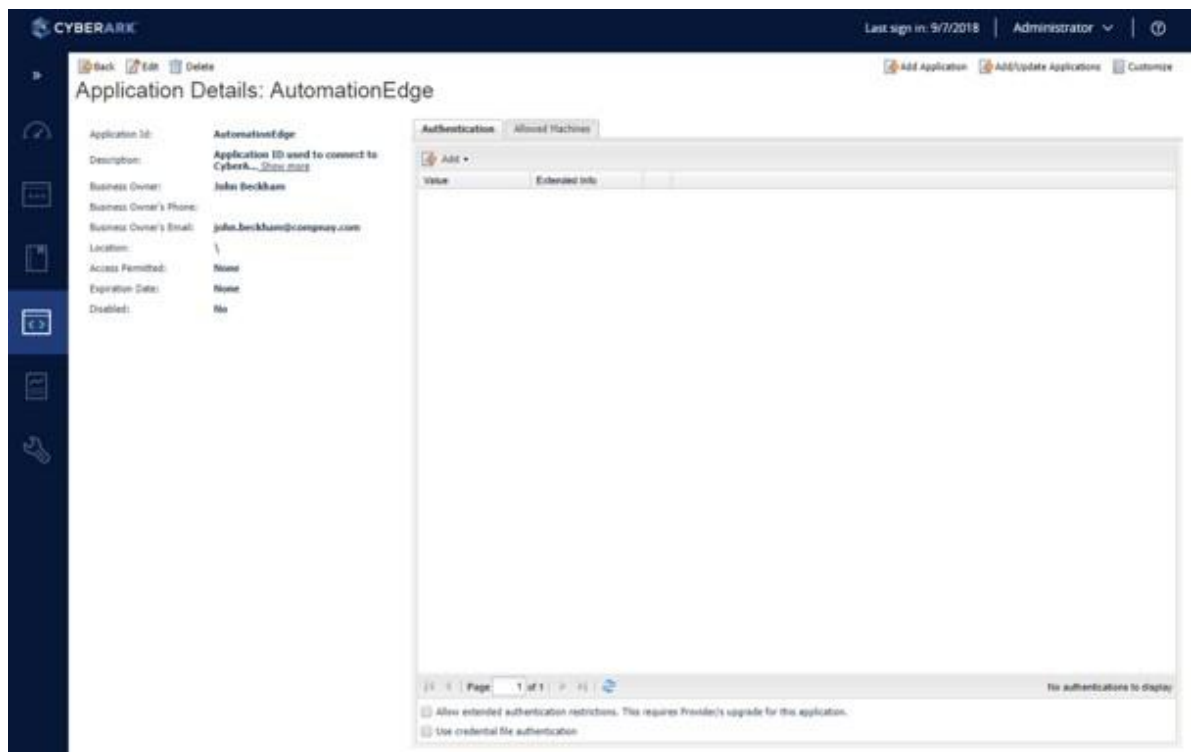
- Name:** AutomationEdge
- Description:** Application ID used to connect to CyberArk through AutomationEdge
- Business owner:**
 - First Name:** John
 - Last Name:** Beckham
 - Email:** john.beckham@company.com
 - Phone:** (empty)
- Location:** (empty dropdown menu)
- Access Permitted:** From: (empty dropdown) To: (empty dropdown)
- Expiration Date:** (empty date field)
- Disabled:** (unchecked checkbox)

At the bottom right, there are 'Add' and 'Cancel' buttons.

☐ Specify the following information:

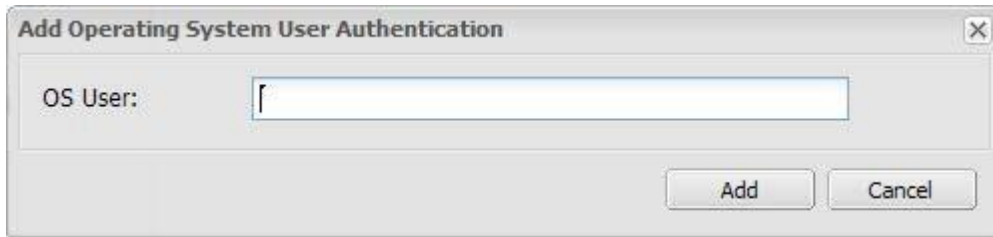
- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: AutomationEdge
- In the **Description** box, specify a short description of the application that will help you identify it.
- In the **Business owner** section, specify contact 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.

A dialog box titled "Add Operating System User Authentication" with a close button (X) in the top right corner. It contains a label "OS User:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

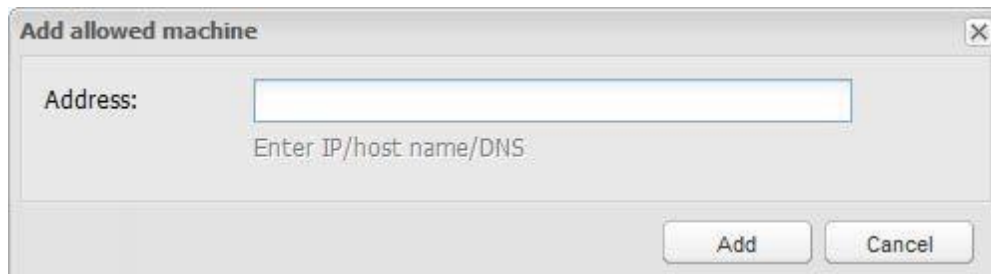
- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.

- ☐ Specify the Certificate Serial Number.

A dialog box titled "Add Certificate Serial Number Authentication" with a close button (X) in the top right corner. It contains a label "SN:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

- ☐ Specify the application's Allowed Machines. This information enables Secrets Manager to make sure that only applications that run from specified machines can access their passwords. [SEP]

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

A dialog box titled "Add allowed machine" with a close button (X) in the top right corner. It contains a label "Address:" followed by a text input field. Below the input field is a hint text "Enter IP/host name/DNS". At the bottom right, 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.

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

8

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 AutomationEdge	john.beckham@c...	John Beckham

☐ Access
☒ Use accounts
☒ Retrieve accounts
☒ List accounts
☐ Account Management
☐ Safe Management
☐ Monitor
☐ View Audit log
☐ View Safe Members

AutomationEdge has been added.

- ☐ 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**.

AUTOMATIONEDGE INSTALLATION & INTEGRATION CONFIGURATION

Refer to the AutomationEdge installation document for AutomationEdge installation.

Below are the steps to create integration with CyberArk.

1. Log in to AutomationEdge configuration UI as Tenant administrator and go to the **Security Vault** tab. Under that, you will find the **Connections** subtab.
2. Create a new CyberArk connection by providing connection the URL, ApplicationID, and password

3. Navigate to the **Credentials** subtab under **Workflows** tab and create a new Credential object of type CyberArk, as demonstrated below:



4. In the ensuing dialog, provide the credential name and description as shown in the image below.
 - a. AutomationEdge uniquely identifies an Account in CyberArk by its three attributes. "safe", "folder" and "object". Specify values of these in form of a JSON as shown below under "Vault Reference JSON".
 - b. Choose Vault connection object created in Step 1.
 - c. Once done, specify attributes of that account object which map to attributes of AutomationEdge credential object attributes (username, password, option1, option2, enc1 and enc2). Typically attributes in CyberArk account object of type secret would get mapped to either password or encrypted 1 or encrypted 2). Except for Credential Providers, AutomationEdge deals only with AutomationEdge credential objects. Credential providers take care of mapping vault object attributes to credential attributes before being presented to the Agent.

Create New Credential (CyberArk)

Credential Name: *

Cred1

Description (Maximum 50 Characters):

Credential to connect to database

Vault Reference JSON *

```
{
  "safe": "test",
  "folder": "root",
  "object": "cyberark_object"
}
```

Vault Connection *

CyberArk

Account Field Mapping

Username:

UserName

Password:

Content

Parameter 1:

Parameter 2:

Encrypted Parameter 1:

Encrypted Parameter 2:

Create

Cancel

PARTNER CONTACT INFO

Business Contact	Name	Edward Markowitz
	Email	edward.markowitz@automationedge.com
	Tel	(631) 523-3188
Technical Contact	Name	Yogesh Ketkar
	Email	yogesh.ketkar@automationedge.com
	Tel	+91 (982) 260-6619
Support Contact	Name	Abhijit Kelkar
	Email	abhijit.kelkar@automationedge.com

	Tel	+91 (960) 791-8783
--	-----	--------------------