



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: CA Technologies (a Broadcom company)

Website: www.CA.com

Name of Product: CA Automatic Workload Automation

Version: V12.2

Date: 5 December 2018 (Revised 4 November 2020)

CA AUTOMIC WORKLOAD AUTOMATION OVERVIEW

CA Automic Workload Automation V12.2 centrally manages and automates the execution of business processes end-to-end; across mainframe, cloud and hybrid environments. Each execution typically requires credentials to authenticate on the Server or Application.

Version: V12.2

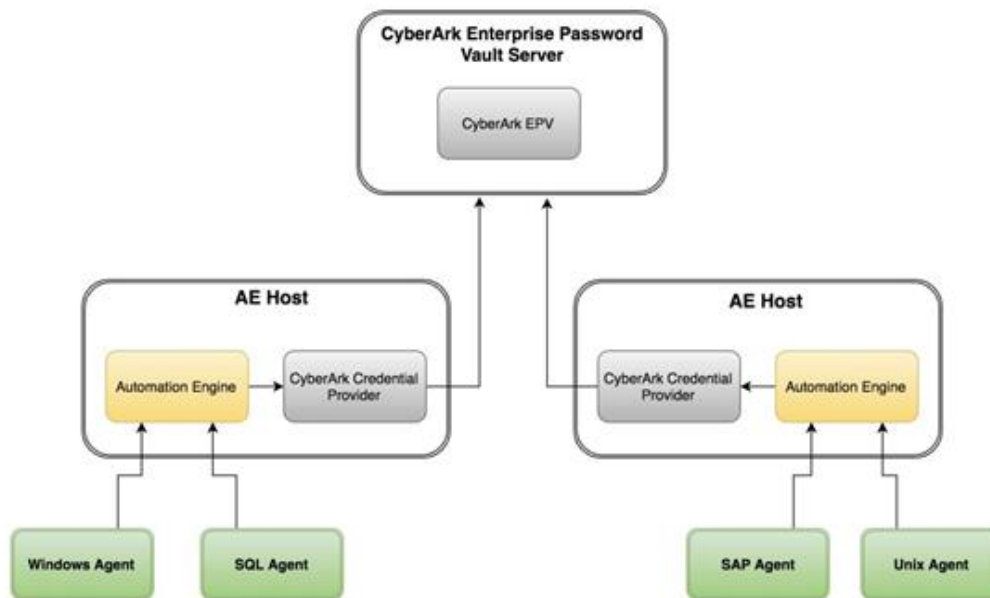
KEY BENEFITS

CA Automic Workload Automation automates your business processes, giving you the agility, speed, visibility, and scalability needed to respond to the constantly changing technology landscape.

- Gain the advantage of integration to Cyberark Password Vault
- Access Password Vault credentials directly at execution time
- Satisfy security compliance standards (not storing passwords in DB)
- Maintain enterprise credentials more easily with standard utilities
- Vault selection in Login object for phased implementation

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

CA Automic Workload Automation (Automation Engine) retrieves credentials from the Cyberark Enterprise Password Vault when Job execution occurs. The credentials are cached locally in the Cyberark Credential Provider to ensure there is no latency. This is important as customers can execute millions of jobs per day. The Agents are the End-points (Servers or Applications) where the work is executed.



SECRETS MANAGER INTEGRATION

The integration is provided in the Login Object where the vault can be referenced to retrieve the credentials for execution.

The Integration is in the Mid-Tier which uses the credentials to authenticate to the End-Point (Server or Application)

The Mid-Tier can be installed in a Single-server environment or in a High-Availability environment to ensure instant Failover in case of outages.

CREDENTIAL RETRIEVAL

The Credential Retrieval is triggered when a job requests a password from the Login Object and the Vault/Safe is set to CyberArk.

Access to the CyberArk Credentials is set per Login Object to enable a phased implementation. When fully implemented, the credential requests could peak at 5000+ per minute.

As a rule, each CyberArk account contains the credentials of exactly one CA Automatic Workload Automation agent. The exceptions are JMX agents which have special features and require three accounts for the same agent. In this case, the credentials must be set in the following format:

- Account 1: JMX_<username>_USERPASS
- Account 2: JMX_<username>_KEYSTOREPASS
- Account 3: JMX_<username>_TRUSTSTOREPASS

- Describe specific properties required for queries on various platforms
 - Unix
 - Windows
 - Other platforms

SECRETS MANAGER INSTALLATION

Secrets Manager Installation - <https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-CP/Latest/en/Content/CP%20and%20ASCP/installing-the-Credential-Provider.htm?tocpath=Installation%7CCredential%20Provider%7CInstall%20the%20Credential%20Provider%7C0>

The JavaPasswordSDK library is required for the integration with the Automic product. The Secrets Manager CP must be installed in order to retrieve the passwords via Secrets Manager.

Configuration in Server ini file to set the path where the Secrets Manager/Credential Provider is installed.

```
[JWP]
;
; libpath: Semicolon separated list of directories where to look for
optional external 3rd party libraries. Configure this with path to
CyberArk SDK library if you want to enable CyberArk integration.
;
libpath= C:\Program Files (x86)\CyberArk\ApplicationPasswordSdk;
```

SECRETS MANAGER CONFIGURATION

The following sections provide details on CA Automic Workload Automation 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.

Add Application

Name: AutomationEngine

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

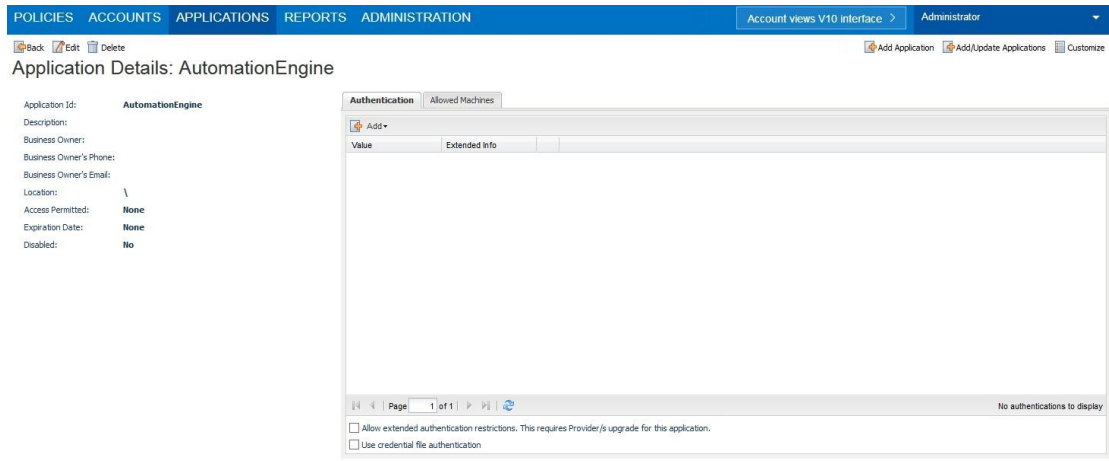
☐ Access Permitted: From: To:

☐ Expiration Date:

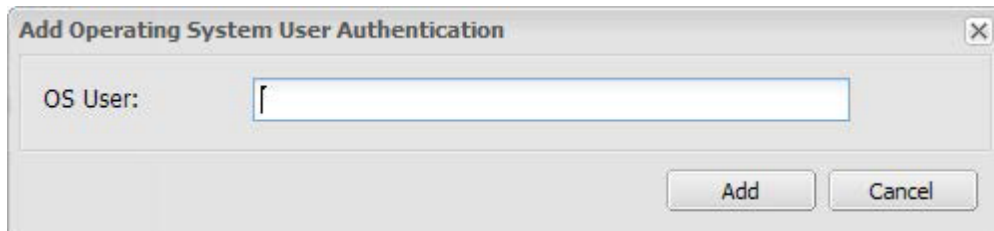
☐ Disabled

Add Cancel

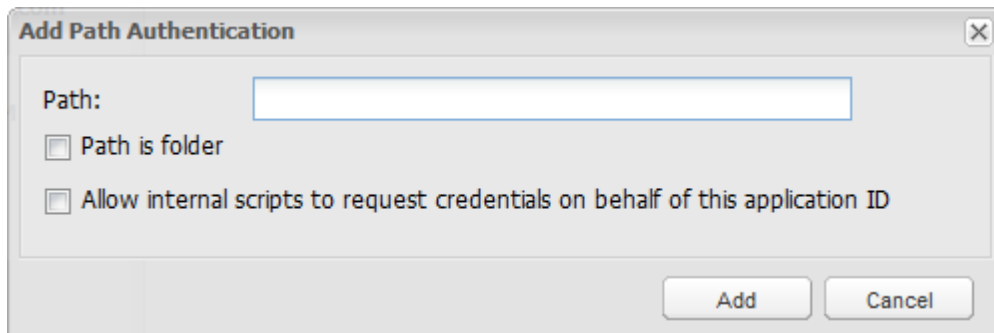
- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: AutomationEngine
 - In the **Description** box, specify a short description of the application that will help you identify it.
 - In 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.

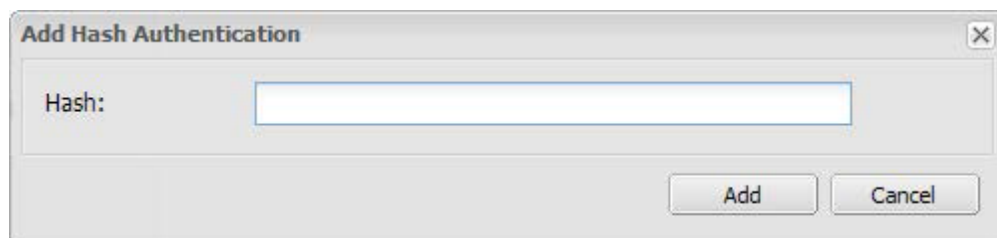


- ☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of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

A screenshot of the 'Add Hash Authentication' dialog box. It has a title bar with the text 'Add Hash Authentication' and a close button (X). Inside the dialog, there is a label 'Hash:' followed by a text input field. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- 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.

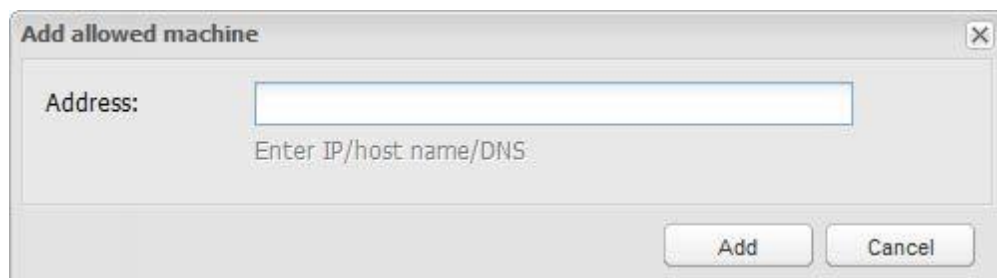
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2

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.

A screenshot of the 'Add allowed machine' dialog box. It has a title bar with the text 'Add allowed machine' and a close button (X). Inside the dialog, there is a label 'Address:' followed by a text input field. Below the input field, there is a placeholder 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.

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 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 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 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:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 AutomationEngine		

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

AutomationEngine 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**.

CA AUTOMIC WORKLOAD AUTOMATION INSTALLATION & INTEGRATION CONFIGURATION

Refer to [CA Automic Partner Vault Setup](#) for CA Automic Workload Automation installation.

Example for Windows account configuration:

Account Details

Edit Change Reconcile Verify Delete Move Send Link Refresh

Password

Show

Copy

RDP (non-ActiveX)

Connect

Copy Shortcut

Platform Name: **Windows Domain Account**
Device Type: **Operating System**
Safe: **AECredentials3**
Name: **Operating System-WinDomain-NB000829-NB000829oab**
Last verified: **N/A**
Last modified: **Administrator (6/12/2018 4:45:25 AM)**
Last used: **Administrator (6/12/2018 4:45:25 AM)**
Username: **NB000829\oab**
Address: **NB000829**

Application UI:

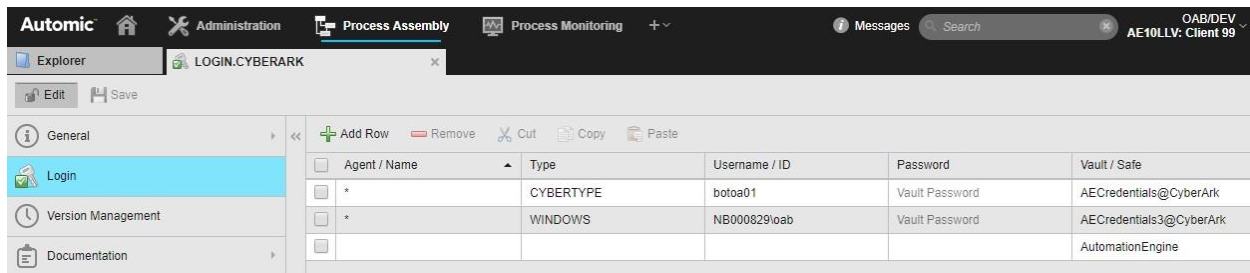
Configure CyberArk as an external password vault in the UC_EXTERNAL_VAULTS variable.

Key	Value 1	Value 2	Value 3	Value 4	Value 5
Cyberark	CYBERARK				

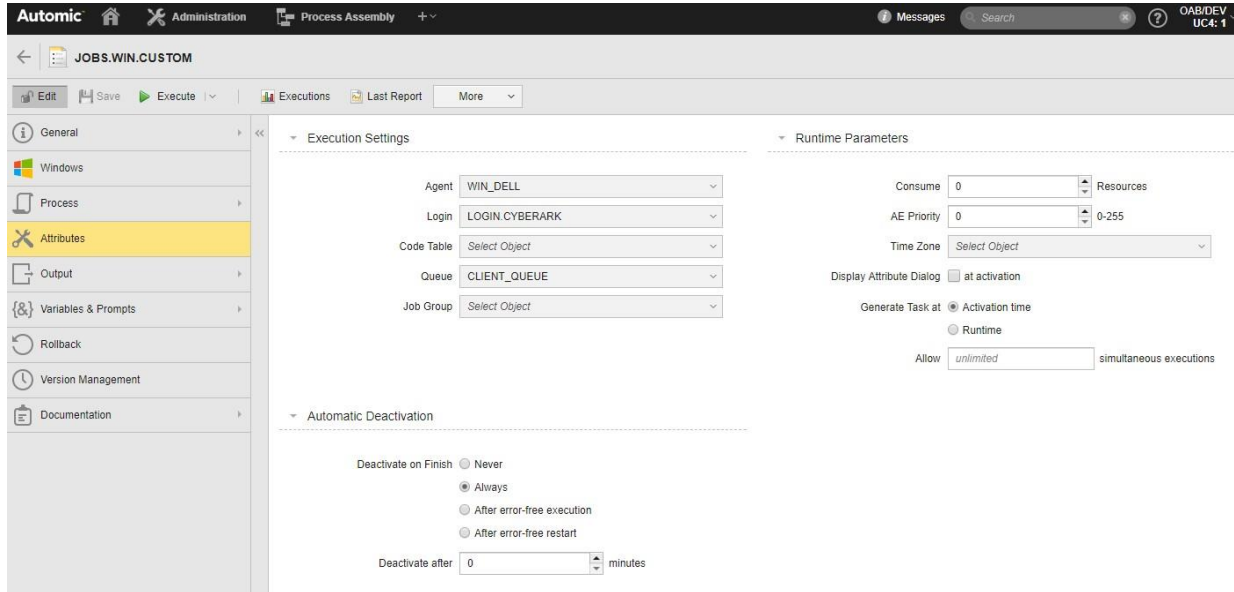
Create and configure the UC_EX_CYBERARK variable on the clients where the credentials should be retrieved from the external password vault.

Key	Value 1	Value 2	Value 3	Value 4	Value 5
ApplID	AutomationEngine				
Safe1	AECredentials				
safe2	AECredentials3				

Configure the LOGIN object which will be used by the job, to retrieve the password from the corresponding CyberArk safe for each agent.



Add the LOGIN object to the job that will run on the configured agent.



Common use case:

1. Local accounts (Windows/Unix)
 - a. The user will specify username, which will be matched to the account in the Vault
 - b. Safe name – optional but required if the username is not unique
 - c. Platform is not required as there is no 1:1 mapping to platforms in AE

PARTNER CONTACT INFO

Business Contact	Name	David Ainsworth
	Email	david.ainsworth@broadcom.com
	Tel	+44 (787) 644-0262
Technical Contact	Name	Oana Botez
	Email	oana.botez@broadcom.com
	Tel	
Support Contact	Name	
	Email	
	Tel	