SECRETS MANAGER CREDENTIAL PROVIDER

CENTRAL CREDENTIAL PROVICER INTEGRATION TECHNICAL DOCUMENTATION

Rocket Software, Inc

www.rocketsoftware.com

ASG-Enterprise Orchestrator

4.3.0

June 2022

ASG-ENTERPRISE ORCHESTRATOR SOLUTION OVERVIEW

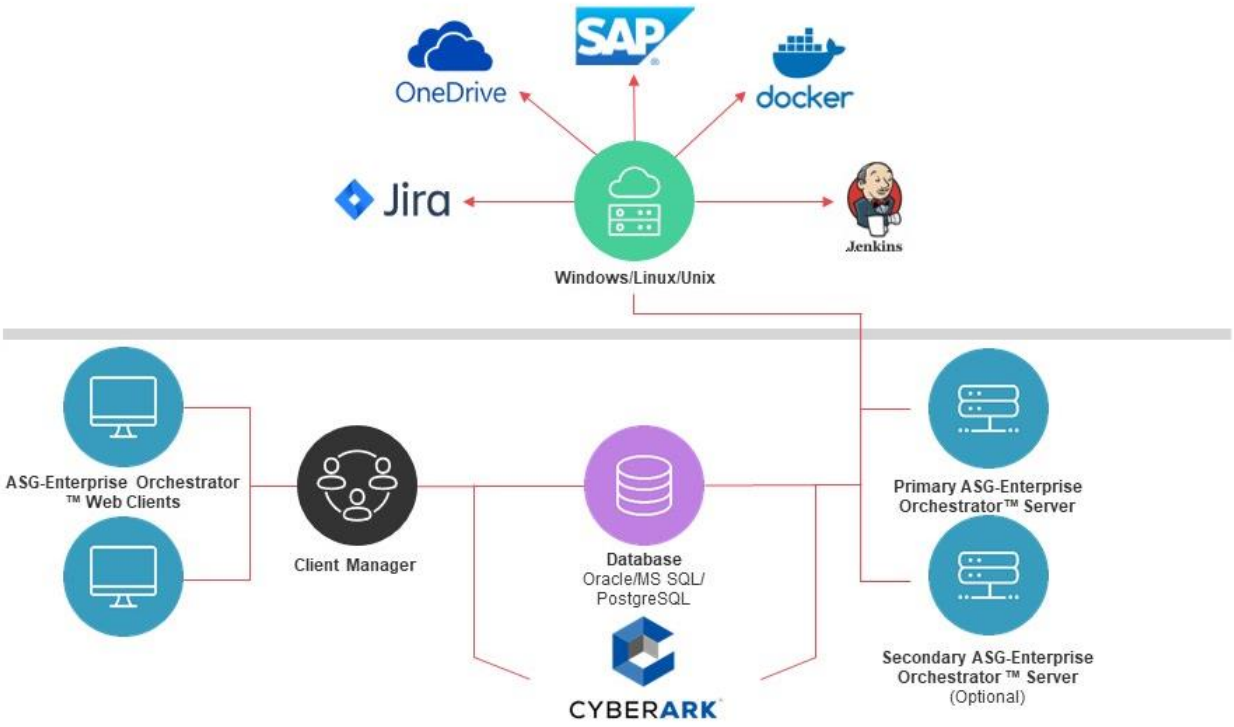
ASG-Enterprise Orchestrator enables IT teams to visualize, automate, and coordinate end-to-end development and operations tasks needed to deliver solutions across operating systems, platforms, and business applications. It unifies an organization's DevOps strategy with the tools and applications already in place to maximize existing investments. Adding ASG-Enterprise Orchestrator provides the connectivity and visibility IT leaders need to manage all end-to-end processes from a single console.

KEY BENEFITS

The automation of digital business value streams enables IT leaders to optimize process flows, improve resource efficiency, and prevent disjointed processes and their associated cost. In addition, it empowers IT leaders to meet the infrastructure and operations needs of their quickly growing business to delight their customers.

Login and password credentials needed in the ASG-Enterprise Orchestrator can be vaulted in the secure CyberArk Vault and retrieved at run time (from CyberArk) eliminating the exposure of storing these credentials in the ASG-Enterprise Orchestrator database.

DIAGRAM & INTEGRATION DESCRIPTION



ASG-Enterprise Orchestrator delivers support for coordinating and orchestrating tasks and workloads on all the major enterprise computing platforms and the most popular business applications. These include: IBM mainframe, Amazon S3, Azure, SAP, Azure DevOps (ADO), Kubernetes, and more. ASG-Enterprise Orchestrator combines all workload automation and consolidates DevOps tasks into dynamic endto-end value streams, which increases output, reduces errors and time-to-market, and improves margins.

To perform these integrations, credentials are often needed to access the applications and those credentials need to be stored within the application. The product uses the concept of a ***login*** to collect the necessary credentials and system information associated with them. To offset the need to store credentials internally, integration with CyberArk was implemented to allow the product to obtain the credentials when needed. Instead of storing the credentials in the product's login elements, the user will specify the necessary key information where the credentials can be found in the CyberArk vault.

When the ASG-Enterprise Orchestrator Server triggers a task to run, it will connect to the CyberArk vault and obtain the credentials. These credentials will then be sent to the agent, along with the task definition, where the agent will perform the requested task. When the task is complete, the status is returned to the server and all associated data relating to that task, including the credentials, are deleted.

The server is the component that handles scheduling and invocation of all tasks. In a typical enterprise there are two (development and production) or three (development, QA and production) ASG-Enterprise Orchestrator environments. Each environment has one active server with optional servers available to automatically become active in the event the active server goes offline.

All connections with the CyberArk vault are done through the CyberArk Secrets Manager web service by the server component. Site administrators can easily control access to the CyberArk vault by configuring the vault to limit access to the necessary server systems.

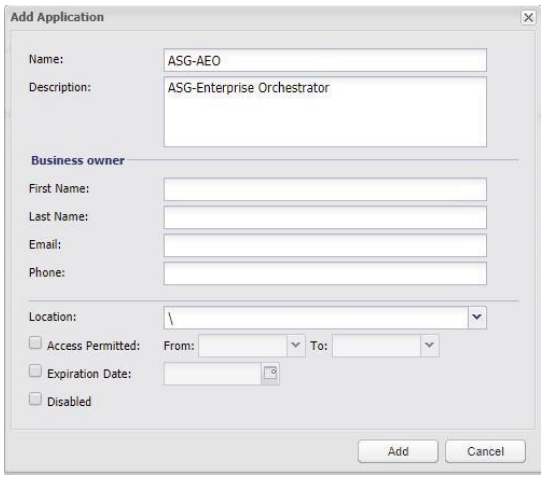
SECRETS MANAGER CREDENTIAL PROVIDER INSTALLATION

Refer to "Central Credential Provider" in the "Secrets Manager Credential Provider" documentation https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-CP/Latest/en/Content/Resources/_TopNav/cc_Home.htm.
For troubleshooting the installation see the CyberArk Technical Community: https://cyberark-customers.force.com/s/

SECRETS MANAGER CREDENTIAL PROVIDER CONFIGURATION

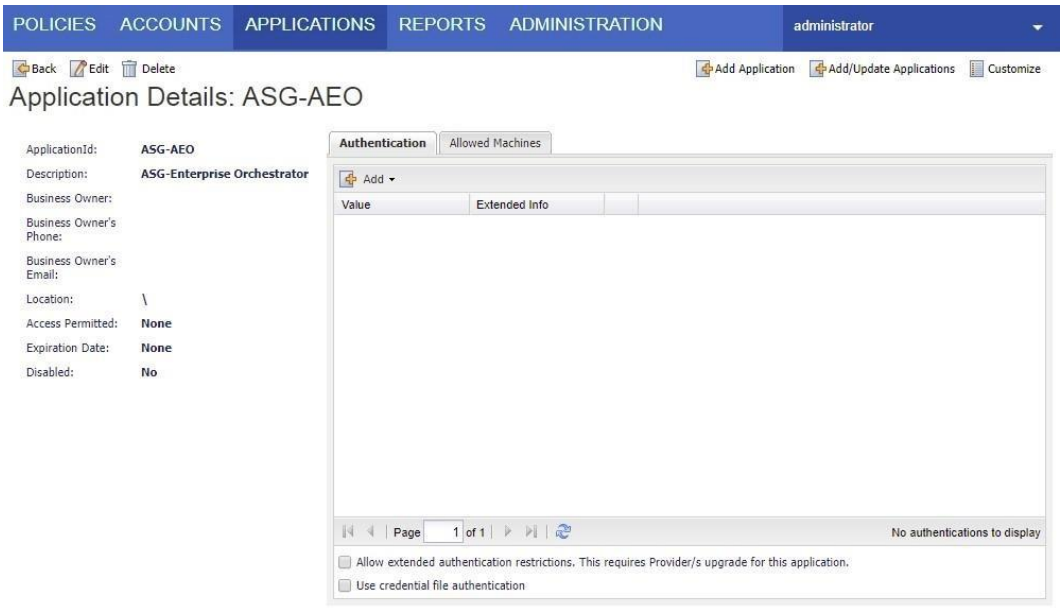
DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

1. Logged in as a user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.



2. Specify the following information:
   - In the Name edit box, specify the unique name (ID) of the application. The default Application ID for this integration is **ASG-AEO**.
   - 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.

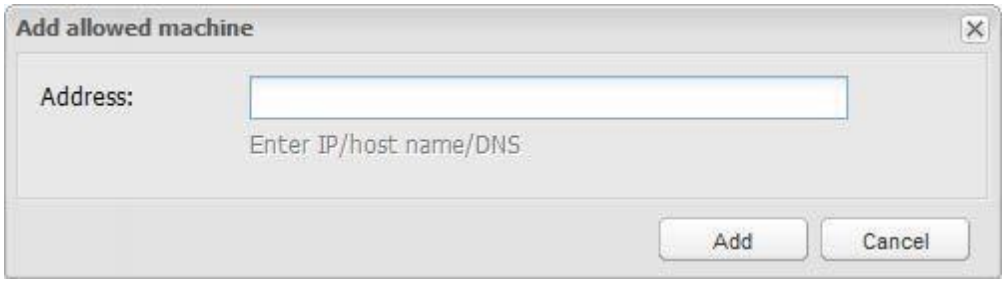


- **Allowing extended authentication restrictions**. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.

4. 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.

5. 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.



- 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 (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).

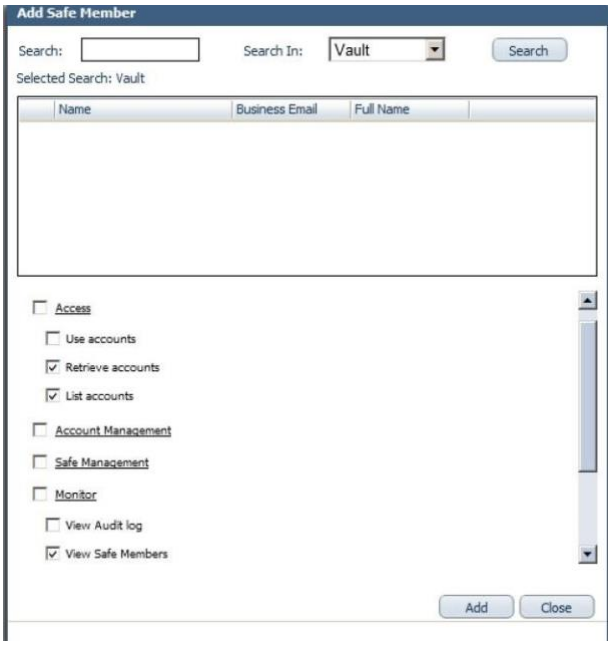
1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
    - **Manually** – Add accounts manually one at a time, and specify all the account details.
    - **Automatically** – Add multiple accounts automatically using the Password Upload feature.

    For this step, you require the **Add accounts** authorization in the Password Safe.

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

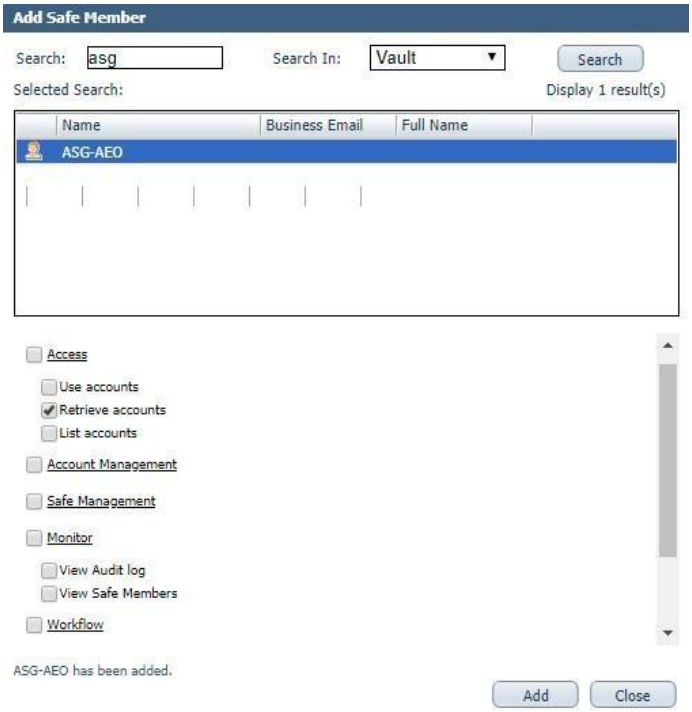
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
    i. Add the Provider user as a Safe 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.



ii. Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve Accounts



iii. If your environment is configured for dual control:

- In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the following permission:
    - Access Safe without Confirmation
- In Privileged Account Security solutions (v8.0 and higher), 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.

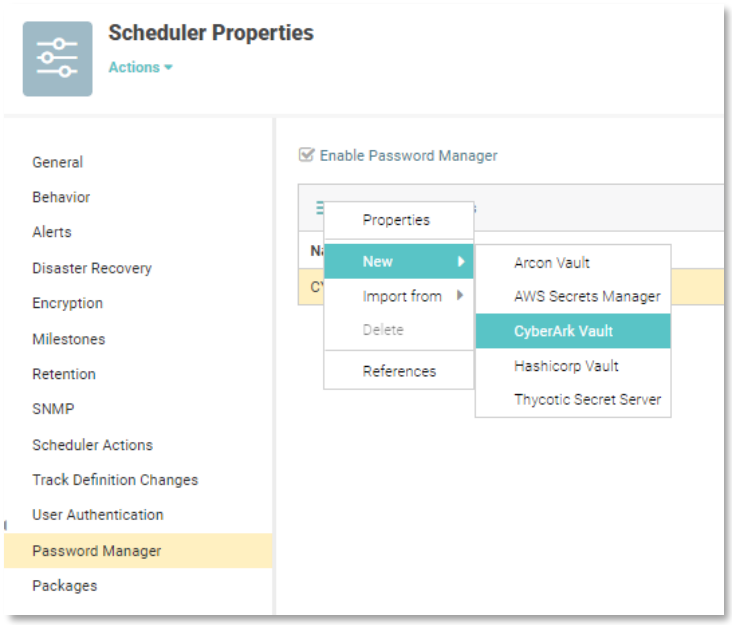
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

ASG-ENTERPRISE ORCHESTRATOR INSTALLATION & INTEGRATION CONFIGURATION

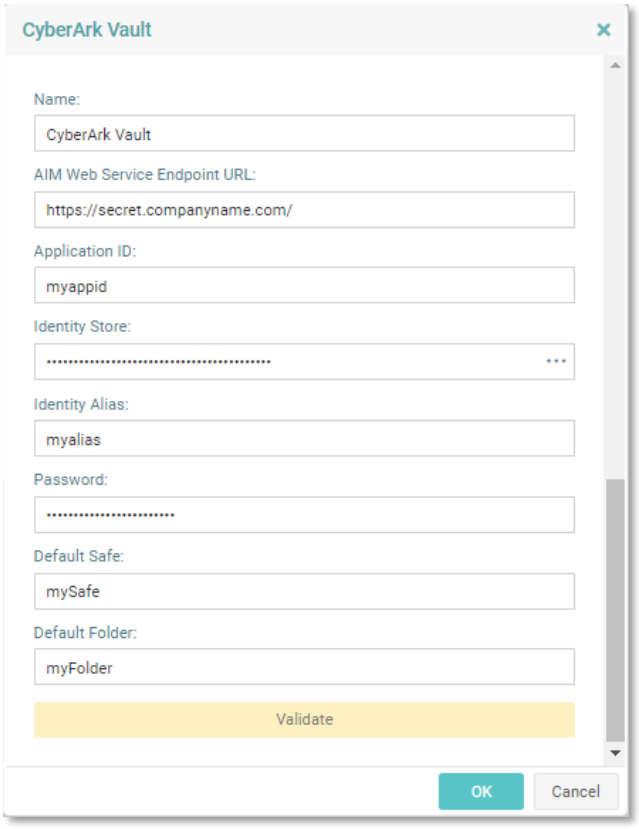
Refer to the ASG-Enterprise Orchestrator online documentation for product installation and configuration of the integration.

The integration must be configured and enabled prior to use. This is done under Authoring → Scheduler Properties → Password Manager.

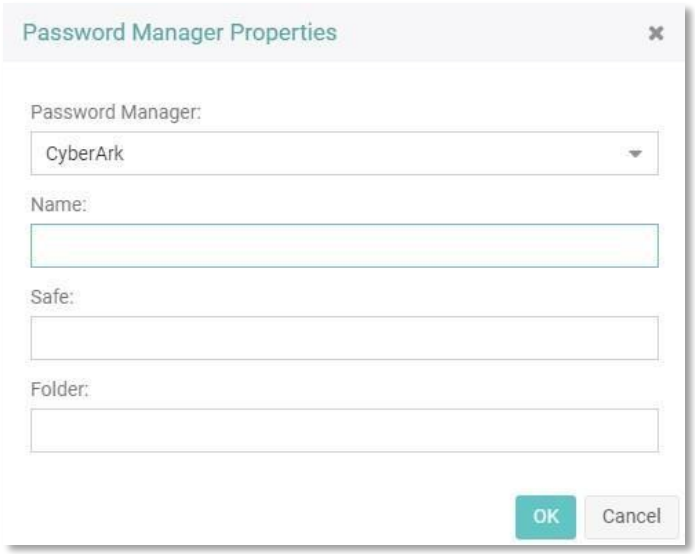
Click the hamburger menu and Select New → CyberArk Vault.



Fill in the fields as required by your installation. Click the Validate button to confirm a good connection, then click the OK button to save the settings.



Usage of the integration is enabled on an as-needed basis. For each login that will retrieve the credentials from the CyberArk vault, click on the ellipsis in the login field. The Password Manager Properties dialog will appear.



Fill in the fields as needed to identify the credential entry in the CyberArk vault that will be used for this login. Press the Ok button to save the settings for this login. The credential fields in the login that will be populated by the data from the CyberArk vault will be disabled in the login definition.

Business Contact	Name	Anna Murray

	Email	amurray2@rocketsoftware.com
	Tel	1.855.577.4323 (USA Only) or 1.781.577.4323
Technical Contact	Name	ASG Customer Support
	Email	asgsupport@asg.com
	Tel	1.800.354.3578
Support Contact	Name	ASG Customer Support
	Email	asgsupport@asg.com
	Tel	1.800.354.3578