CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Siemplify
Website: http://www.siemplify.co
Name of Product: Siemplify
Version: 4.2
Date: 14 August 2018 (Revised 23 May 2021)

SIEMPLIFY OVERVIEW

Siemplify provides a holistic Security Operations Platform that empowers security analysts to work smarter and respond faster. Siemplify uniquely combines security orchestration and automation with patented contextual investigation and case management to deliver intuitive, consistent, and measurable security operations processes. Leading enterprises and MSSPs leverage Siemplify as their SOC Workbench, tripling analyst productivity by automating repetitive tasks and bringing together disparate security technologies.

Version: 4.2

KEY BENEFITS

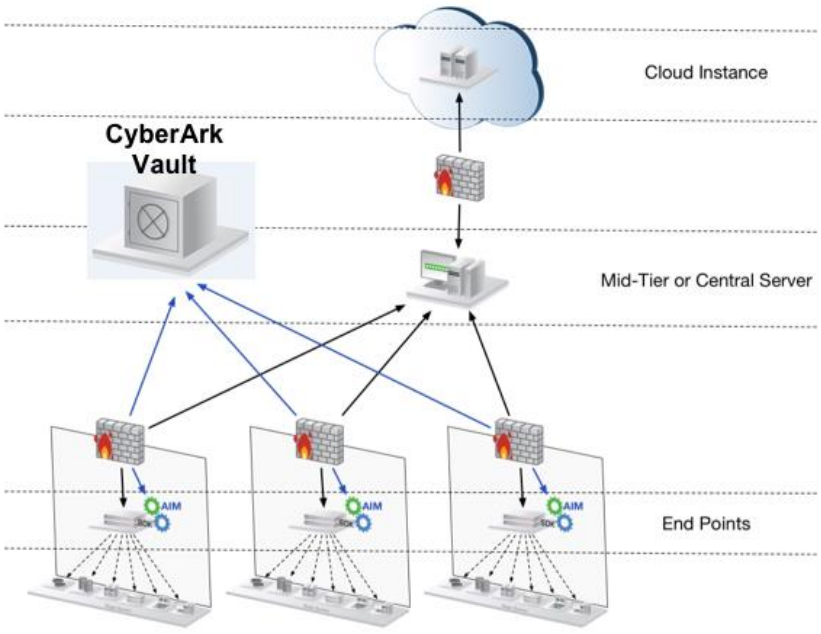
Benefits of Siemplify:

- Reduce alert overload – address cases of related alerts instead of weeding through individual alerts
- Resolve more cases, faster – automate workflows and repetitive tasks
- Gain deeper insight – context applied to alerts illuminates the who, what, and when of a security event
- Work more efficiently – manage and orchestrate disparate tools from a single console
- Create consistent processes – document processes using a drag-and-drop playbook builder
- Track, measure, and improve – define and monitor security operations KPIs and create automated reports

Benefits of integrating Siemplify with CyberArk Secrets Manager:

- Customers are able to easily integrate their full Engineering and IT ecosystems while also levering the full security delivered by CyberArk.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INSTALLATION

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

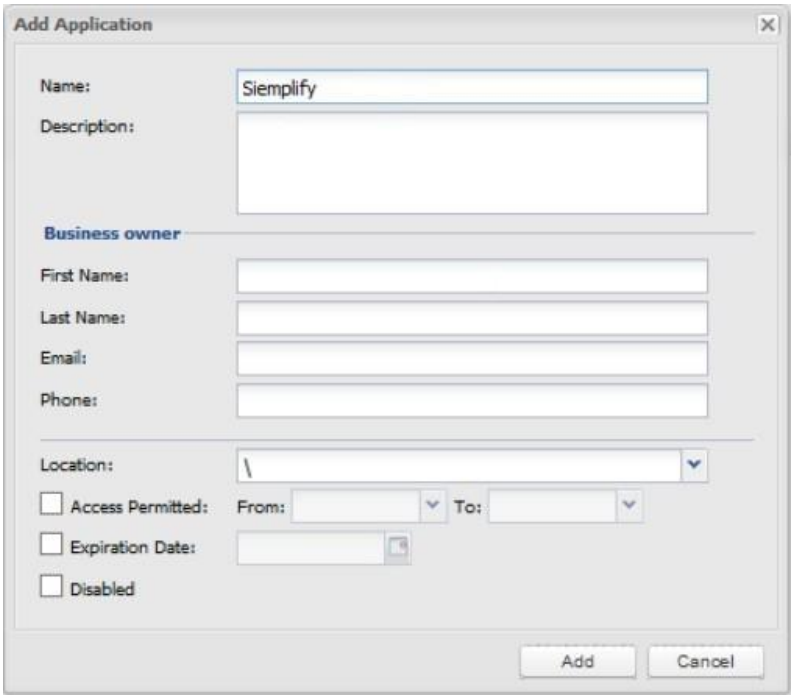
SECRETS MANAGER CONFIGURATION

The following sections provide details on Siemplify 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:

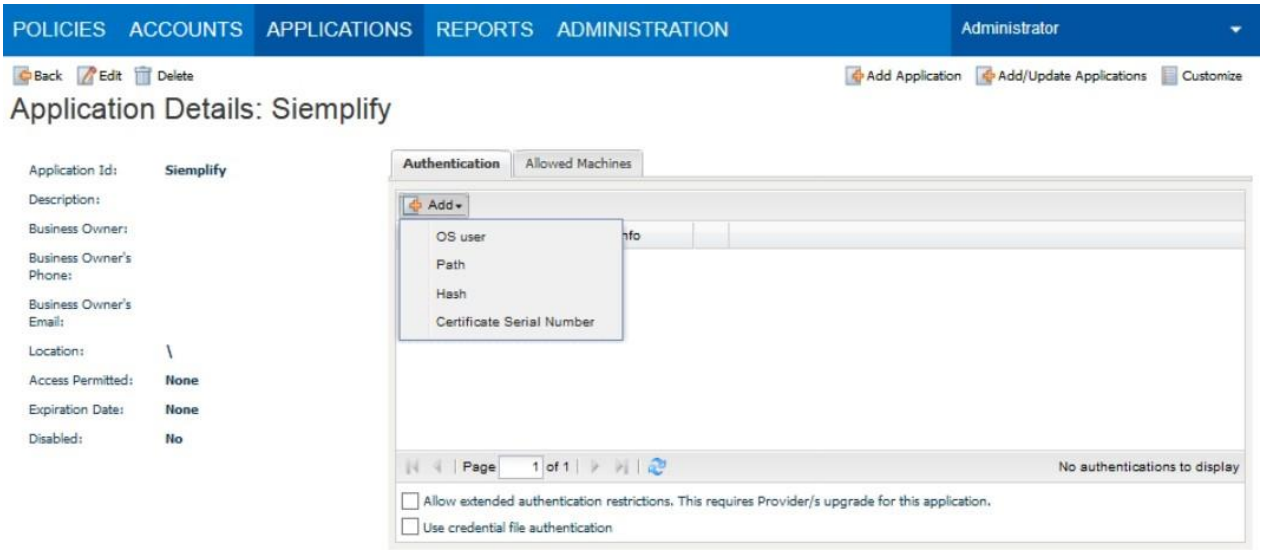
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



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

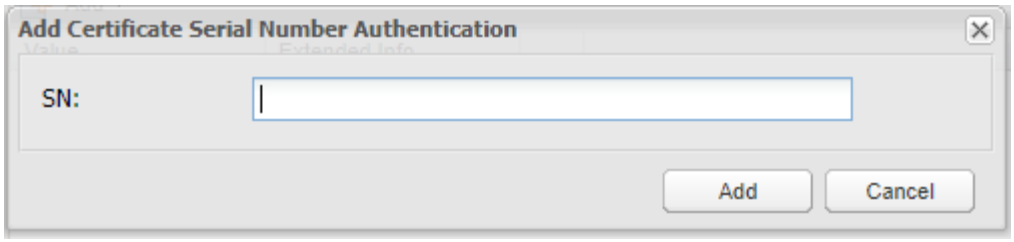
☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

☐ Select the authentication characteristic to specify.

☐ Select **OS user**. The Add Operating System User Authentication window appears.

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

☐ Specify the Certificate Serial Number.



Instructions on how to get the Certificate Serial Number:

Windows:
Start -> certmgr.msc (Current User) -> expand Personal -> select Certificates -> double-click on certificate to open
Start -> certlm.msc (Local Computer) -> expand Personal -> select Certificates -> double-click on certificate to open

If the first two options do not work in your env:
Start -> mmc.msc -> File; Add/Remove Snap-in -> Certificates -> Add -> OK -> you may be prompted to choose Local Computer or Current User -> OK
Expand Certificates -> Personal -> Certificates -> Double-Click on a certificate to open.

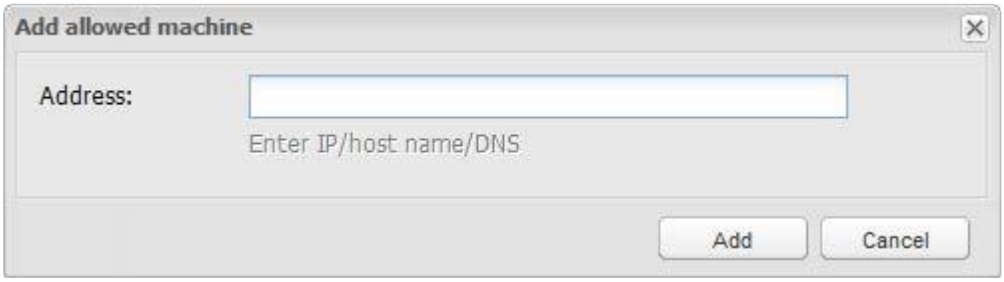
Once the certificate is open -> Details tab -> Serial Number is in the list of values shown

Once the certificate is open
OpenSSL
openssl x509 -in <cert file name> -serial -noout

- This is the most secure way to authenticate the application for CCP
- The following are enhanced ways of authenticating

☐ 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.

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



- 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.**

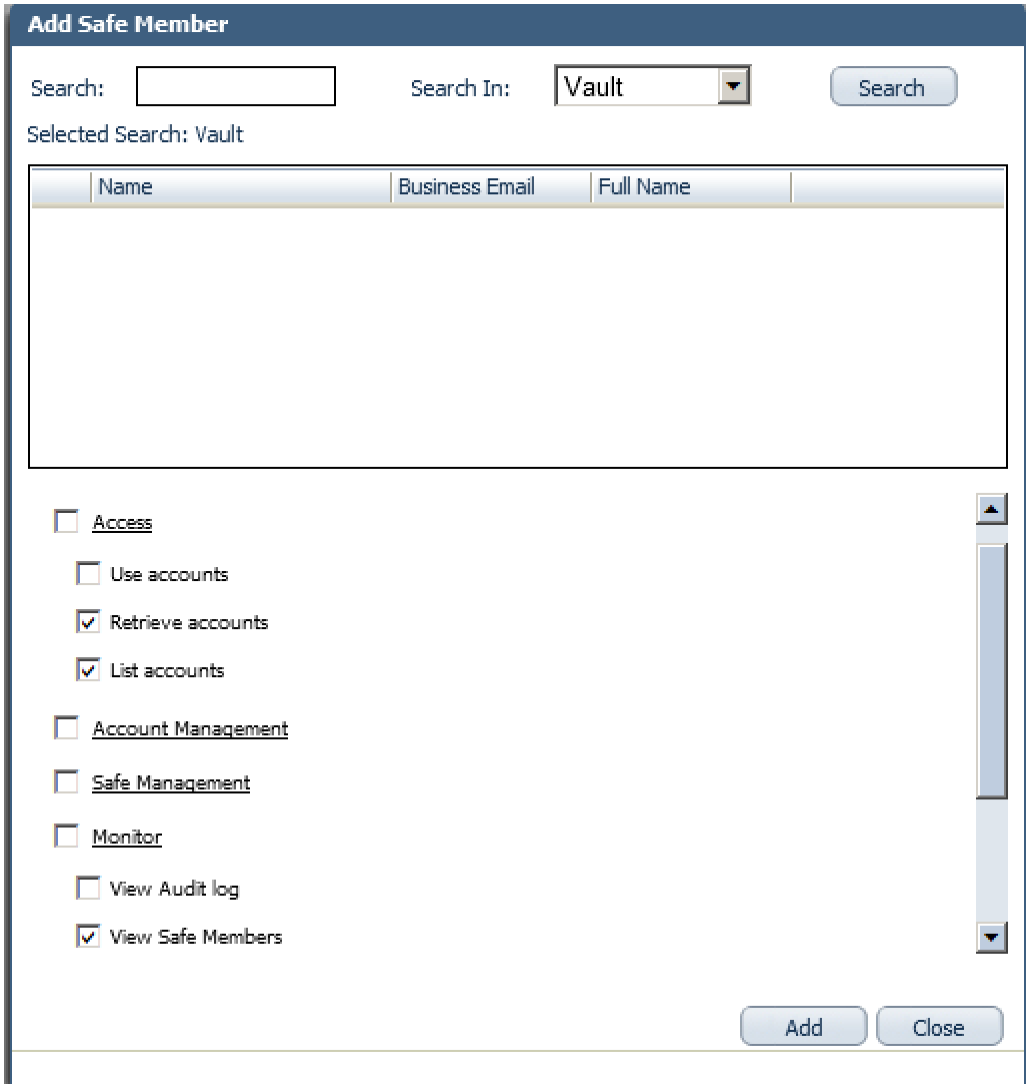
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

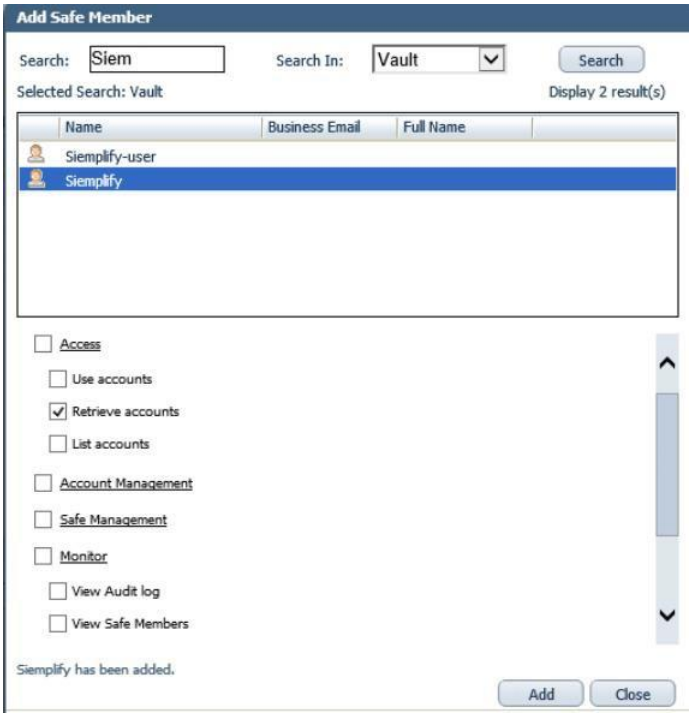
- List accounts
- Retrieve accounts
- View Safe Members

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

- Retrieve accounts



☐ 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.

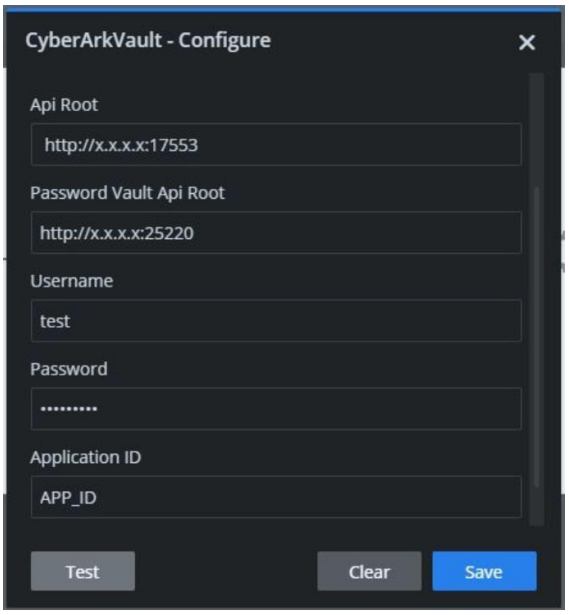
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

SIEMPLIFY INSTALLATION & INTEGRATION CONFIGURATION

Refer to “CyberArk Siemplify Configuration Guide” for Siemplify installation.

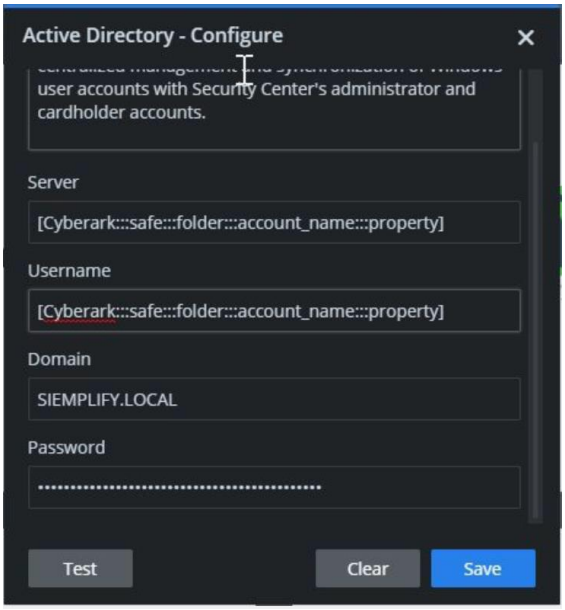
High-Level Use-Cases:

- CyberArk Configuration:



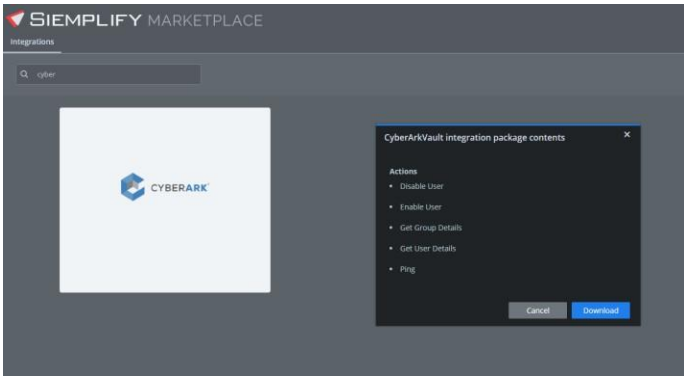
Example: CyberArk Configuration

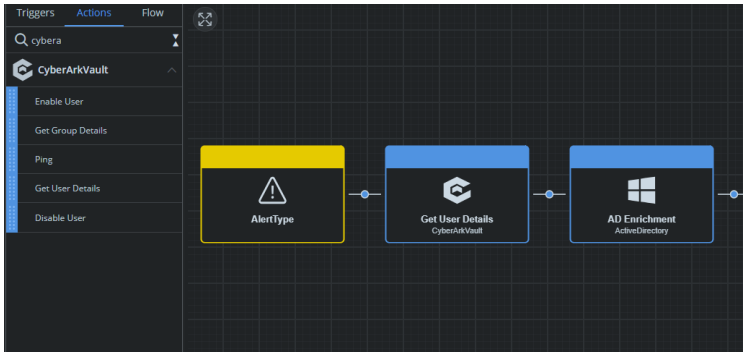
- Utilizing CyberArk to retrieve and utilize credentials to enable automation and responses to any other relevant toolset in the enterprise' infrastructure



Example: AD Integration

- Utilizing CyberArk Integration to provide user context and respond to threats as part of a SOC WorkFlow





Example: WF Automation Utilizing CyberArk

PARTNER CONTACT INFO

Business Contact	Name	Meny Har
	Email	meny@siemplify.co
	Tel	347-209-3431
Technical Contact	Name	Or Gabay
	Email	org@siemplify.co
	Tel	347-209-3431
Support Contact	Name	Or Shafir
	Email	support@siemplify.co
	Tel	