



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: AppSphere AG

Website: www.scriptrunner.com

Name of Product: ScriptRunner

Version: 2018 R3

Date: 7 January 2019 (Revised 17 October 2020)

SCRIPTRUNNER OVERVIEW

ScriptRunner is the leading all-in-one solution for PowerShell. It enables organizations to develop, automate, and delegate PowerShell for teams of all sizes. Administrative access is usually necessary for the execution of PowerShell scripts. ScriptRunner manages the information for these credentials with its execution policies.

With the CyberArk Password Vault integration, ScriptRunner customers can now centrally and securely store all necessary credentials.

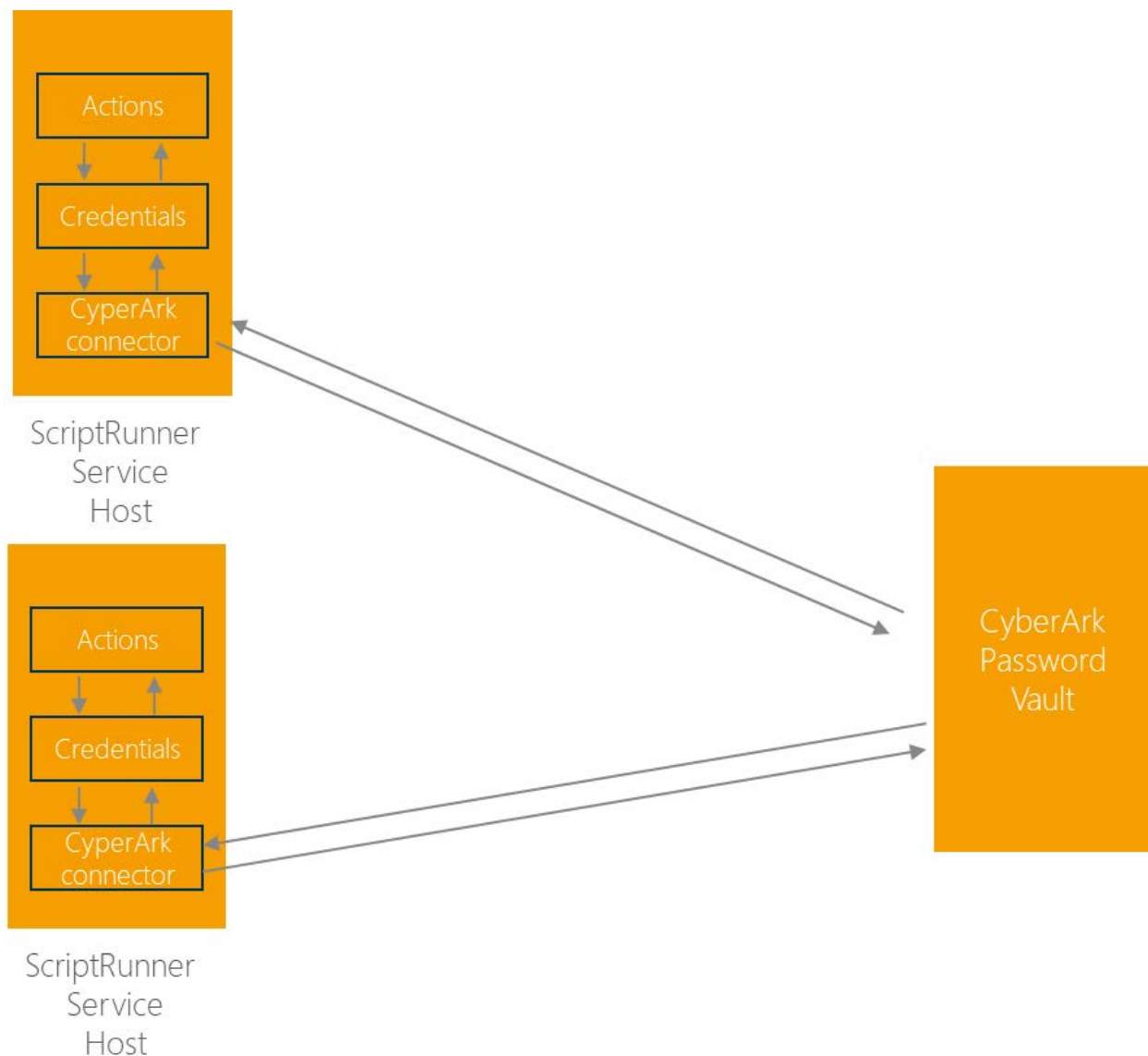
Version: 2018 R3

KEY BENEFITS - ONE INTEGRATED SOLUTION FOR MANAGING POWERSHELL

- Easy-to-use web interface for PowerShell automation and delegation
- Secure task delegation to service desk users
- Retrieved password information are not stored at any time within ScriptRunner
- Create new self-service offers for end users
- Team-based PowerShell script development and testing
- Up and running within less than one day
- Secure and centralized management of ScriptRunner credentials in CyberArk Password Vault
- Support multiple CyberArk password folders
- Dedicated ScriptRunner connector for CyberArk Password Vault
- Flexible selection of folders to retrieve required credentials
- Multiple ScriptRunner hosts share the same secure password repository

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

The combination of ScriptRunner and CyberArk Password Vault offers a unique solution to automate and delegate PowerShell scripts with world class password security.



CREDENTIAL RETRIEVAL

To run PowerShell scripts with ScriptRunner, Users must provide necessary credentials to run PowerShell scripts with ScriptRunner, in order to enable ScriptRunner to work with the CyberArk Password Vault, a new connector has been developed and integrated into ScriptRunner 2018 R3. Customers can now choose between retrieving credentials from the local Windows credential store or from the CyberArk Password Vault.

In the past, the necessary credentials to run PowerShell scripts with ScriptRunner had to be saved in the local Windows credential store of the “Local System” account. This means that customers running multiple ScriptRunner hosts had to maintain the credentials separately for each host. If a customer needed to move a ScriptRunner configuration to a new machine, they would need to re-enter the credentials on the new server.

With the new CyberArk integration, all necessary credentials are stored centrally and can be utilized by multiple ScriptRunner hosts and the credentials are stored a much more secure way.

REQUIREMENTS

Pre-requisites and dependencies:

ScriptRunner release 2018 R3 or higher

- ScriptRunner password connector license
- CyperArk Password Vault

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 ScriptRunner 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.

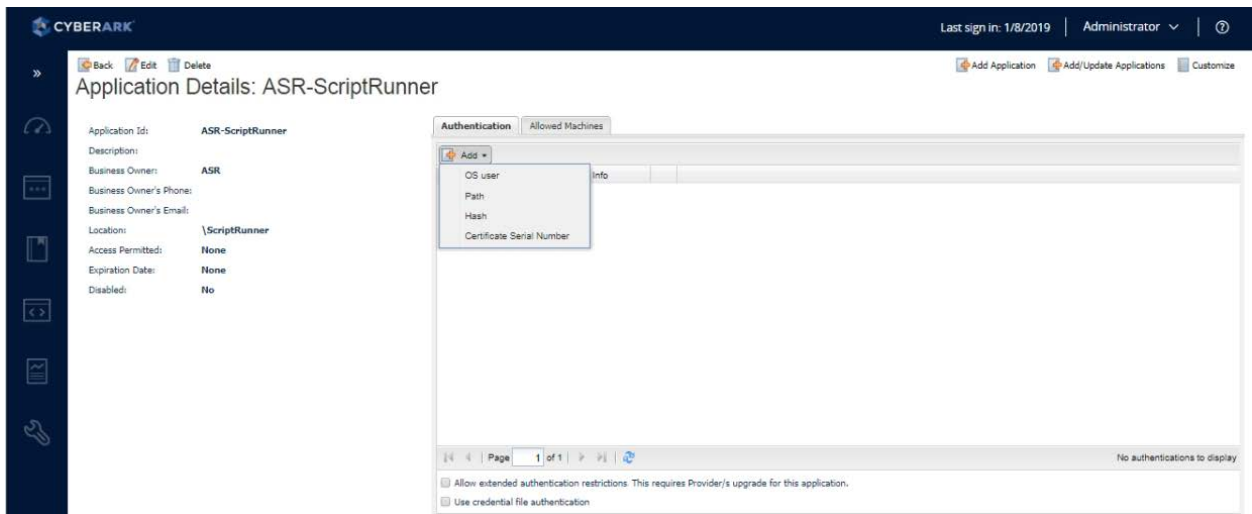
The screenshot shows a dialog box titled "Add Application". It contains the following fields and sections:

- Name:** A text box containing "ASR-ScriptRunner".
- Description:** A large empty text box.
- Business owner:** A section with four text boxes: "First Name", "Last Name", "Email", and "Phone", all of which are empty.
- Locations:** A dropdown menu showing a root path.
- Access Permitted:** An unchecked checkbox followed by "From:" and "To:" dropdown menus.
- Expiration Dates:** An unchecked checkbox followed by a date picker.
- Disabled:** An unchecked checkbox.
- Buttons:** "Add" and "Cancel" buttons at the bottom right.

☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: ASR-ScriptRunner
- 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.

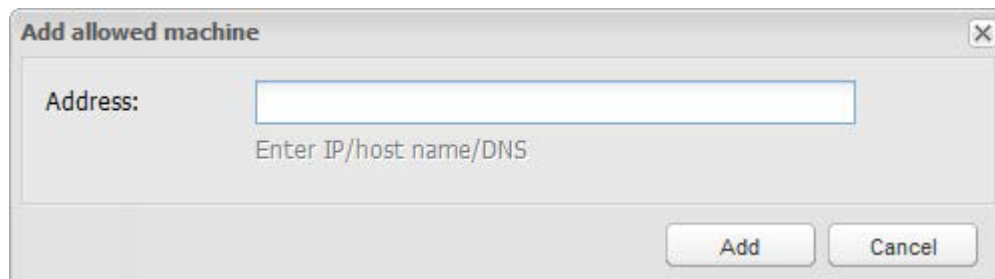


- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain 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**. The OS user is listed in the Authentication tab.
- ☐ Specify the Certificate Serial Number.

- ☐ 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.

A screenshot of a dialog box titled "Add allowed machine" with a close button (X) in the top right corner. The dialog box has a light gray background. Inside, there is a label "Address:" followed by a white text input field. Below the input field, the text "Enter IP/host name/DNS" is displayed in a smaller font. At the bottom right of the dialog box, there are two buttons: "Add" and "Cancel".

Add allowed machine [X]

Address:

Enter IP/host name/DNS

[Add] [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

Add Safe Member

Search: Search In:

Selected Search: Vault Display 3 result(s)

Name	Business Email	Full Name
 ASR-Admin		
 ScriptRunner		ASR Admin
 ASR-ScriptRunner		ASR

☐ Access

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

☐ Account Management
☐ Safe Management
☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

- ☐ If the 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), the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- 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.

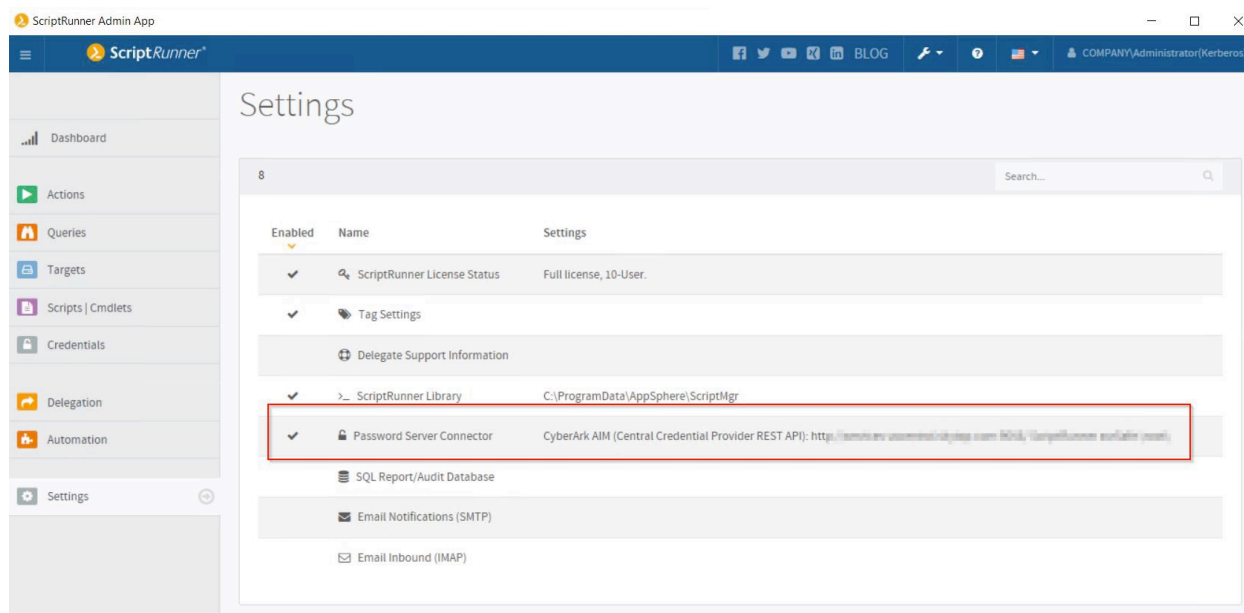
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

SCRIPTRUNNER INSTALLATION & INTEGRATION CONFIGURATION

Create and activate the CyberArk connector on the ScriptRunner service host

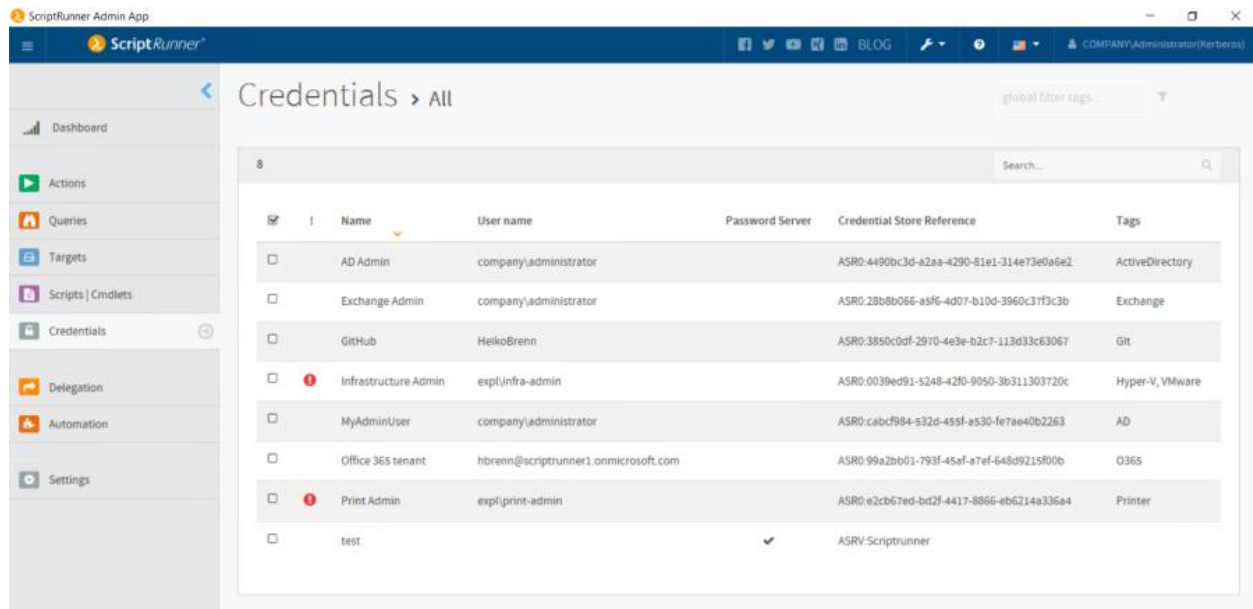
1. Before creating the CyberArk connector make sure you have a valid Password Server Connector license activated on the machine
2. Start Windows PowerShell as Administrator
3. Set-AsrPasswordServerConnector -API 'CyberArk AIM API' -Host 'yourcyberark host' -Port yourcyberarkport -ussl no -On -Restart
4. Set-AsrCyberArkConnector -AppID yourappid -DefaultSafe yourdefaultsafe -DefaultFolder yourdefaultfolder -Restart
5. With Get-AsrPasswordServerConnector -PassThru you can check the current configuration

Open the ScriptRunner AdminApp and go to "Settings" to check the Password Server Connector status.



Create a new credential with the password server connector

1. Go to "Credentials" and click on "Create"



2. Enter the name of the ID for which the password should be retrieved

STORE NEW CREDENTIAL

Credential Properties

Info

Display name:

Credential from CyperArk Password Vault

Password Storage

The initially selected store cannot be changed later. Use the Set-ASRPasswordServerConnector Cmdlet on the ScriptRunner host to enable and configure the Password Server connector.

☒ Retrieve password from the Password Server :

Password Server ID of the password entry:

TestUser

☐ Store password into the local Windows Credential Manager ...

Tags:

Add tag

OK Cancel

Common use cases:

1. Windows domain credentials or other standard credentials
 - a. The user will specify: username, address, platform
 - b. Safe name – optional but recommended for increasing performance
2. Local accounts (windows/Unix)
 - a. The user will specify: username & platform

- b. Safe name – optional but recommended for increasing performance
 - c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned
- 3. Non-standard credentials (can't be unique with username+address+Platform)
 - a. The user will specify: Safe and object name (folder is usually root by default)

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

PARTNER CONTACT INFO

Business Contact	Name	Heiko Brenn
	Email	heiko.brenn@scriptrunner.com
	Tel	+49 (162) 487-9156
Technical Contact	Name	Manfred Böttger
	Email	manfred.boettger@scriptrunner.com
	Tel	
Support Contact	Name	Manfred Böttger
	Email	manfred.boettger@scriptrunner.com
	Tel	