



APPLICATION ACCESS MANAGER

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Microsoft

www.microsoft.com

Power Automate Desktop

Version: 2.6.28.21069 and later

April 2021

MICROSOFT POWER AUTOMATE SOLUTION OVERVIEW

Power Automate Desktop broadens the existing robotic process automation (RPA) capabilities in Power Automate and enables you to automate all repetitive desktop processes. It's quicker and easier than ever to automate with the new intuitive Power Automate Desktop designer using the prebuilt drag-and-drop actions or recording your own desktop flows to run later.

KEY BENEFITS

Leverage automation capabilities in Power Automate Desktop. Create flows, interact with everyday tools such as email and excel and work with modern and legacy applications. Examples of simple and complex tasks you can automate are:

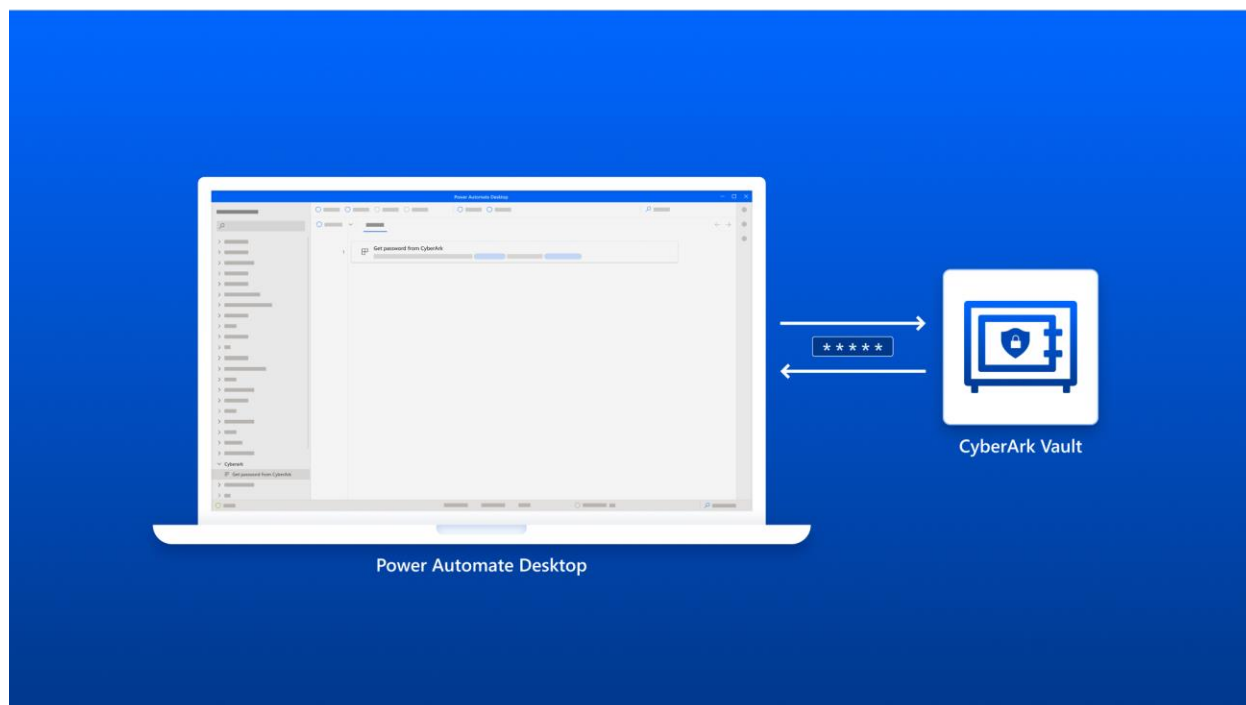
- Quickly organize your documents using dedicated files and folders actions
- Accurately extract data from websites and store them in excel files using Web and Excel automation
- Apply desktop automation capabilities to put your work on autopilot

Power Automate Desktop is addressed to home users, small businesses or larger enterprise companies. It's addressed essentially to everyone who is performing simple or complex rule-based tasks on their workstations.

It allows you to automate both legacy applications, such as terminal emulators and modern web and desktop applications, Excel files, and folders. Interact with the machine using application UI elements, images, or coordinates.

The CyberArk functionality as part of Power Automate Desktop, enables an extra layer of security for end-user sensitive data and credentials, particularly for when this data is used in processes to access web or desktop applications. User authentication takes place through the secure enterprise's CyberArk vault to safely retrieve usernames and passwords when and if needed.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



The integration lies in the Runtime of the application at the execution level of the processes at End Point or Mid-Tier or Central Server

Power Automate Desktop includes a dedicated action in its standard action library called “Get Password from CyberArk”. Through this action a request to retrieve a password from the secure vault is initiated through the CyberArk’s API. This is stored into a secure value which can be used in all other actions that require a password, like email actions, ftp actions, web actions, etc.

The Credentials retrieval is triggered through a dedicated Power Automate Desktop action called “Get Password from CyberArk”. When this action is used within a desktop flow, then upon its execution the credentials will be asked from the CyberArk’s Secure Vault.

The frequency under which the credential retrieval is done depends on the frequency that the desktop flows need to run. Every time a desktop flow, which is requesting credentials, is executing, the retrieval will take place.

AAM INSTALLATION

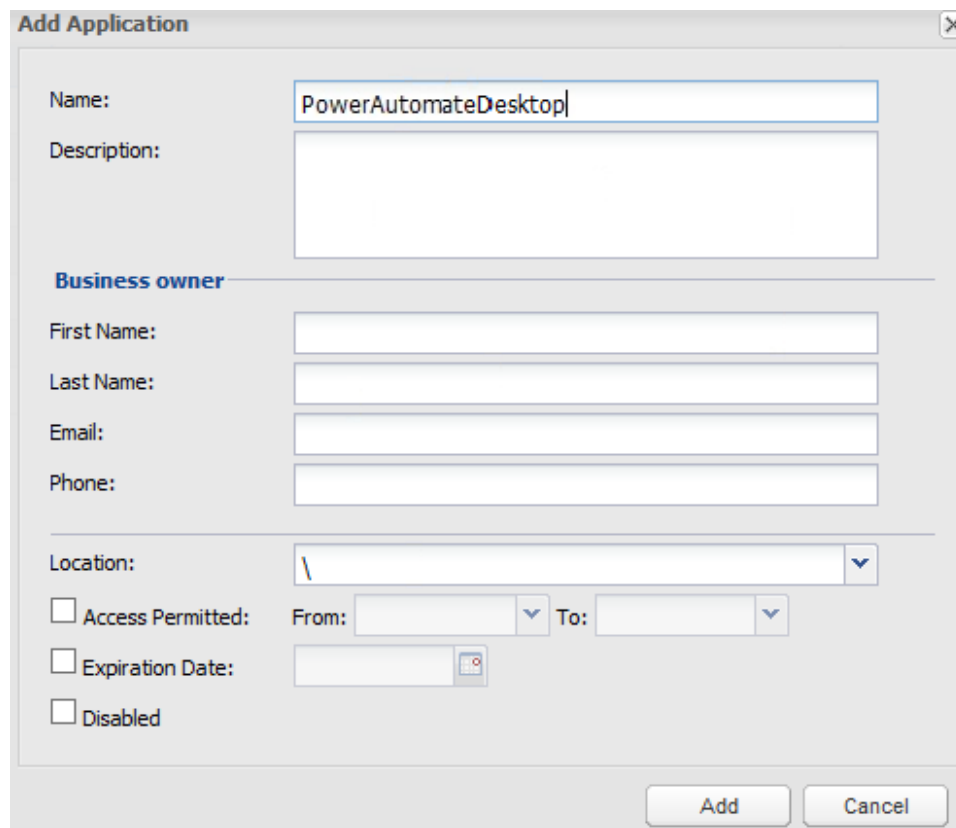
Refer to the “Central Credential Provider Implementation guide” for CyberArk Agentless installation and configuration.

AAM CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the Application, here are the instructions to define it manually via CyberArk's PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed 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. It contains the following fields and sections:

- Name:** A text box containing 'PowerAutomateDesktop'.
- Description:** A large empty text area.
- Business owner:** A section header followed by four text boxes for:
 - First Name:**
 - Last Name:**
 - Email:**
 - Phone:**
- Location:** A dropdown menu showing a backslash character (\).
- Access Permitted:** A checkbox followed by 'From:' and 'To:' dropdown menus.
- Expiration Date:** A checkbox followed by a date picker.
- Disabled:** A checkbox.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

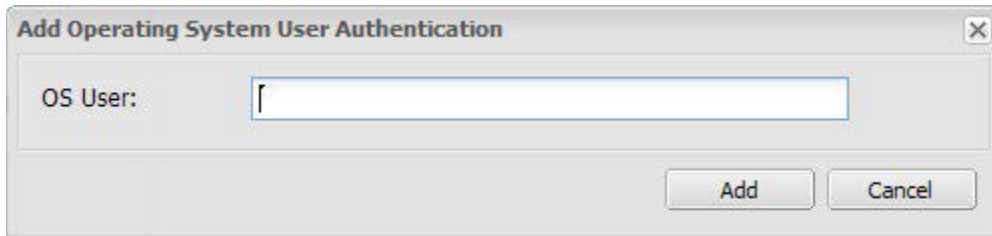
2. Specify the following information:
 - In the Name edit box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: **PowerAutomateDesktop**
 - In the Description, specify a short description of the application that will help you identify it.
 - In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

The screenshot shows the 'Application Details: PowerAutomateDesktop' page. On the left, there is a sidebar with application metadata: ApplicationId: PowerAutomateDesktop, Description: (empty), Business Owner: (empty), Business Owner's Phone: (empty), Business Owner's Email: (empty), Location: \, Access Permitted: None, Expiration Date: None, and Disabled: No. On the right, the 'Authentication' tab is active. It features an 'Add' button with a dropdown menu that lists 'OS user', 'Path', 'Hash', and 'Certificate Serial Number'. Below the dropdown is a table with columns 'Info' and 'Add'. At the bottom of the page, there are two checkboxes: 'Allow extended authentication restrictions. This requires Provider/s upgrade for this application.' and 'Use credential file authentication'.

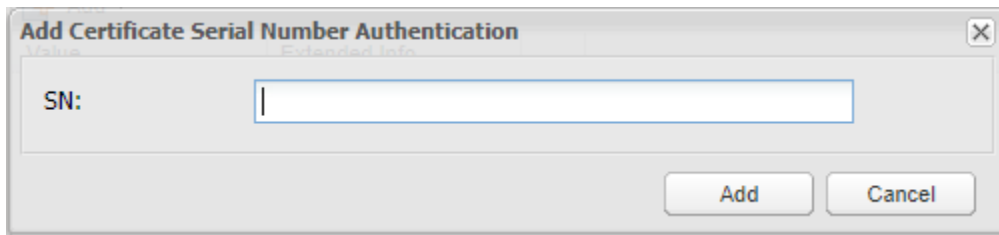
- **Allowing extended authentication restrictions.** This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.
4. Specify the application's **Authentication** details. This information enables the Credential Provider to check 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 OS user:
- a. Select **OS user**; the Add Operating System User Authentication window appears.



The dialog box is titled "Add Operating System User Authentication". It contains a label "OS User:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

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

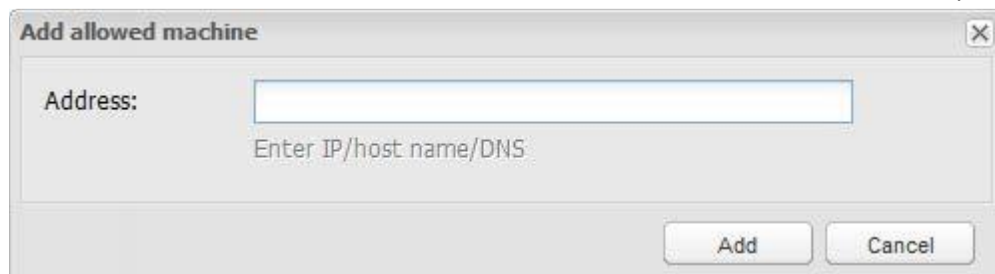
6. Specify the Certificate Serial number:



The dialog box is titled "Add Certificate Serial Number Authentication". It has two tabs: "Value" (selected) and "Extended Info". Under the "Value" tab, there is a label "SN:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

7. Specify the application's **Allowed Machines**. This information enables AAM 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.



The dialog box is titled "Add allowed machine". It contains a label "Address:" followed by a text input field. Below the input field, there is a hint text: "Enter IP/host name/DNS". At the bottom right, there are two buttons: "Add" and "Cancel".

- 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 (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 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.

- 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.

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

- ii. 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
 PowerAutomateDesktop		

☐ Access

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

☐ Account Management
☐ Safe Management
☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

- iii. 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**.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to [Install Power Automate Desktop on your device - Power Automate | Microsoft Docs](#) for Microsoft Power Automate Desktop installation.

Power Automate Desktop UI:

Get password from CyberArk



 Retrieves a password for a specific application from CyberArk [More info](#)

Select parameters

Server address:	{x}	
Application ID:	{x}	
Safe:	{x}	
Folder:	{x}	
Object:	{x}	
Extra data:	{x}	
Accept untrusted certificates:	<input checked="" data-bbox="570 1060 647 1102" type="checkbox"/>	
Certificate location:	Don't use certificate ▼	

Advanced

Timeout:	30	
----------	--	---

Variables produced

- ☒

JSONResponse {x}

The API response result
- ☒

CyberArkPassword {x}

The password retrieved from CyberArk

 On error

Save

Cancel



Configuration Options:

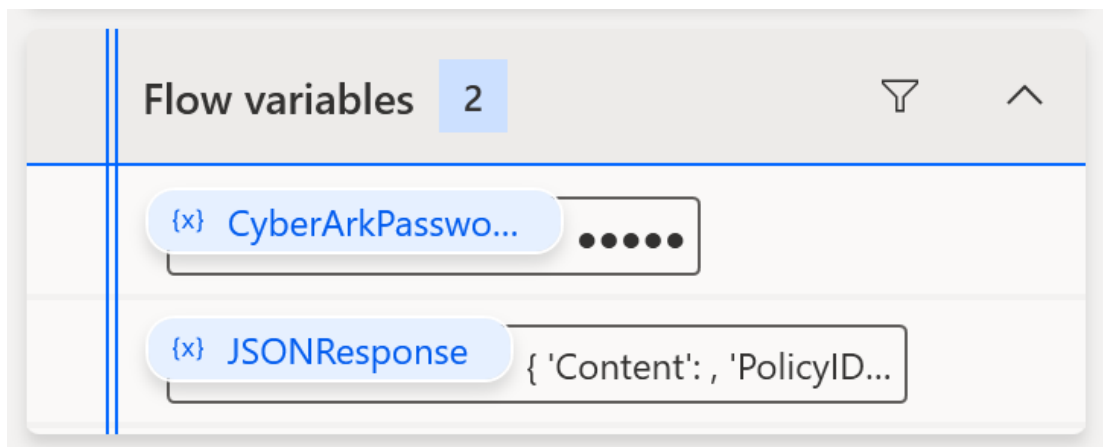
The user will enter the Server Address, Application ID, and Safe, Folder and Object names, as well as any optional Extra Data. Next, they will specify whether a Certificate will be used.

1. Don't use Certificate
2. Load Certificate from Windows Store
 - a. The user should select the certificate to be used from the Windows Store using the "Find Certificate" button; an option allows them to only choose from Valid Certificates.
 - b. The chosen Certificate's Path will be displayed under "Certificate Path".
3. Load Certificate from File
 - a. The user should select the Certificate File to be used or enter its path.
 - b. Optionally, if the Certificate requires a Password, it should be entered in the "File Password" field.

Note: It is advised that a method requiring a certificate is preferred.

You can find all the input parameters in detail, [here](#).

After the Action is executed, the resulting retrieved Credentials and JSON response are stored in two separate Variables of the "Encrypted value" and "Custom object" type, respectively.



You can find all the variables produced in detail, [here](#).

These can then be used in subsequent Actions like for example “Retrieve Emails” action that required a password and a username, adding the *CyberArkPassword* variable as input for the password field.

Retrieve email messages

Retrieves email messages from an IMAP server [More info](#)

Select parameters

IMAP Server

IMAP server:

imap.servername.com

{X}

i

Port:

993

{X}

i

Enable SSL:

☒

i

User name:

%Username%

{X}

i

Password:

%CyberArkPassword%

{X}

i

Accept untrusted certificates:

☐

i

> Email Filters

> Variables produced

RetrievedEmails

 On error

Save

Cancel

For more information please see here: [CyberArk - Power Automate | Microsoft Docs](#)

PARTNER CONTACT INFO

- Join the Microsoft Power Automate community:
[Microsoft Power Automate Community - Power Platform Community](#)
- Support for Power Automate Desktop:
[Power Automate Desktop - Power Platform Community \(microsoft.com\)](#)