



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Advanced Systems Concepts, Inc.

Website: www.advsyscon.com

Name of Product: ActiveBatch IT Automation

Version: ActiveBatch® Version 12

Date: 29 January 2019 (Revised 19 October 2020)

ACTIVEBATCH IT AUTOMATION OVERVIEW

ActiveBatch® is an Enterprise IT Automation and Job Scheduling solution that provides reliable workflow development and predictable workload deployment of business processes, IT processes, file transfers, big data (Hadoop) processes, and more within a single unified system that addresses the automation requirements of the enterprise. ActiveBatch offers a low-code and cost-effective approach that addresses the automation of integrated and disparate processes across hybrid IT infrastructures.

While ActiveBatch is a script language independent solution, it also minimizes the requirement for custom scripting. Through its Integrated Jobs Library of prebuilt, drag-and-drop actions and functions, developers can assemble reliable workflows in less than half the time than that of traditional approaches.

The ActiveBatch Service Library complements the Integrated Jobs Library as a dynamic framework that extends integration capabilities, allowing developers to consume APIs (RESTful services, SOAP Web Services, .NET assemblies, stored procedures, and command lines) of applications, platforms and services and turn them into reusable, drag-and-drop job actions within the Integrated Jobs Library without the need for custom coding.

ActiveBatch's powerful date/time scheduling and robust event framework supports the timely execution of cross-platform workloads on and across Windows, Linux, Unix, AIX, NSK, OS X, iSeries, macOS, and other key operating systems.

KEY BENEFITS

ActiveBatch provides for the reliable automation and execution of payloads that encompass Workload Automation, Business Processes, IT Processes, file movements such as Managed File Transfer, Big Data Automation (Hadoop), and more within a single, unified console.

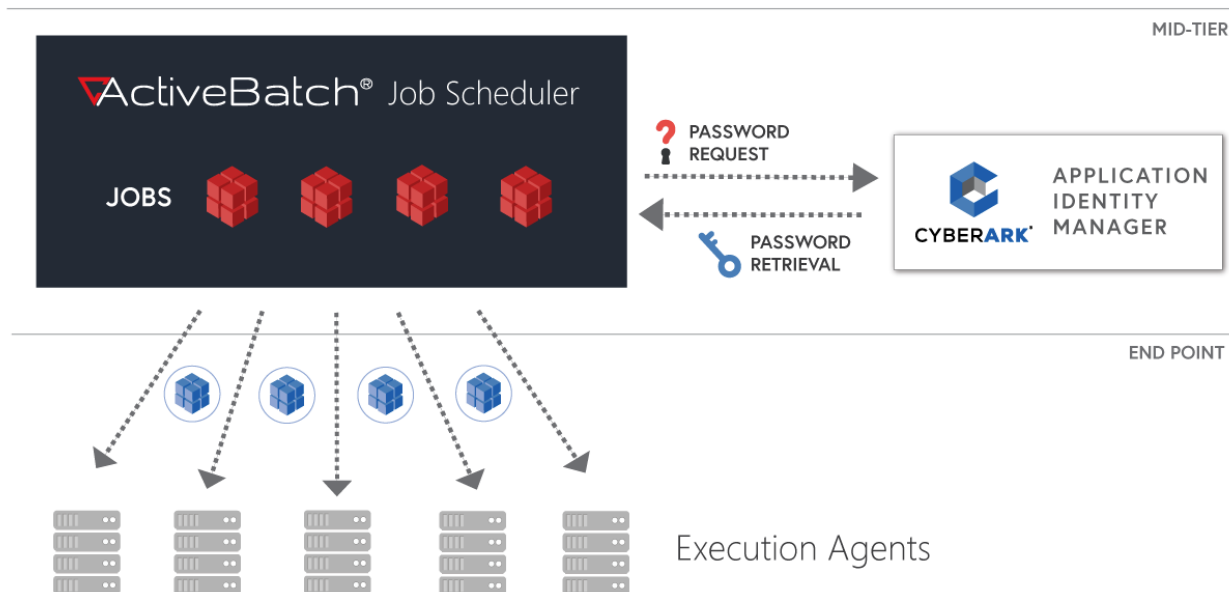
While supporting the automation of all scripts, ActiveBatch takes a Focus on Function, providing for the assembly of prebuilt, drag-and-drop actions and functions into workflows. Such an approach to workflow assembly allows for the development and automation of customized, integrative, end-to-end workflows that seamlessly and reliably pass data and manage dependencies across disparate systems in less than half the time of traditional approaches.

ActiveBatch provides for just-in-time provisioning and deprovisioning of cloud and virtualized systems based on its use of predictive analytics to improve successful completion of executables.

ActiveBatch objects require credentials, usernames and passwords that are stored within the product. The ActiveBatch – CyberArk integration will allow customers to use CyberArk's secure vault, so passwords can be rotated and retrieved at runtime while protecting against cyberattacks and the actions of a rogue employee.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

ActiveBatch IT Automation can be integrated with CyberArk via Credential Provider:



SECRETS MANAGER INTEGRATION

Secrets Manager is integrated within the User Account Object within ActiveBatch. This object allows users to provide credentials that will be used to execute their workflows. Using CyberArk will allow the workflow to dynamically retrieve the credentials from CyberArk at runtime. Using the CyberArk integration makes it much easier for the user to manage username or password changes, since ActiveBatch will not be exposed to the credentials.

The User Account Objects are stored in the Job Scheduler Database, and all API requests to CyberArk are made by the Job Scheduler before dispatching the jobs to a remote agent.

CREDENTIAL RETRIEVAL

The credential retrieval is triggered by running an ActiveBatch Job that has an associated CyberArk user account.

Only Windows Domain Accounts and Local Server accounts (Windows or Unix/Linux) are relevant to the ActiveBatch integration, so only properties required to retrieve those accounts need to be provided in the password retrieval query.

REQUIREMENTS

The ActiveBatch V12 scheduler requires that it be installed on a Microsoft Windows server ranging from Windows Server 2012R2, Windows 10 2019 LTSC, Windows 10 2016 LTSC, Windows Enterprise 10 2015 LTSC, Windows Server 2016, or Windows Server 2019.

SECRETS MANAGER INSTALLATION

Refer to the [“Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.](#)

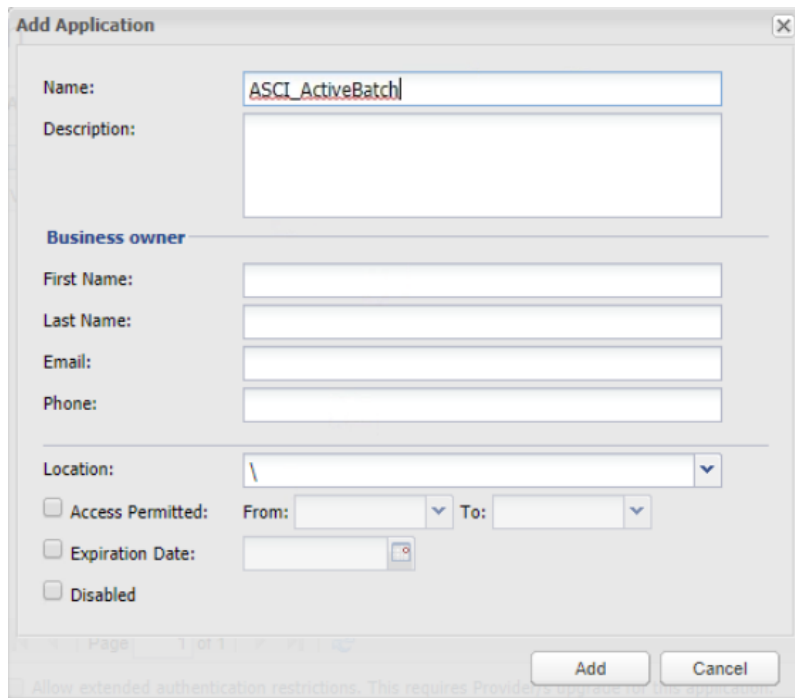
SECRETS MANAGER CONFIGURATION

The following sections provide details on ActiveBatch IT 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:

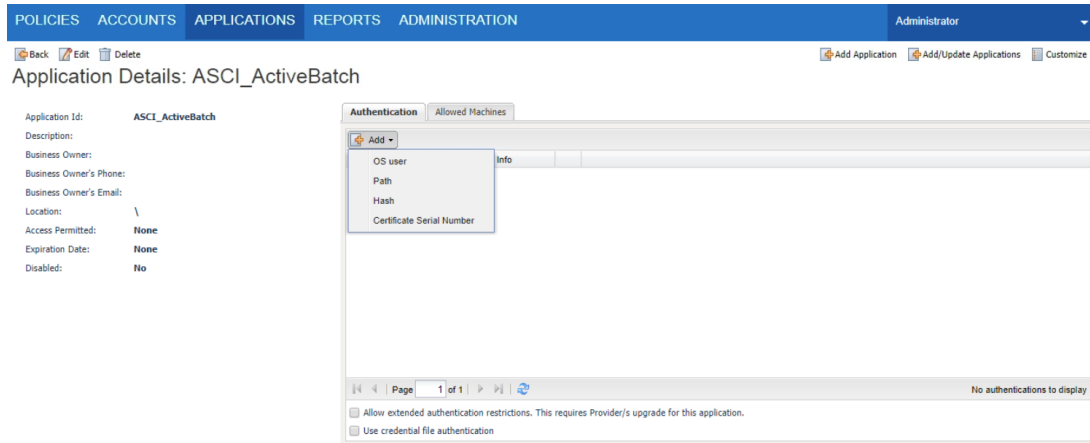
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



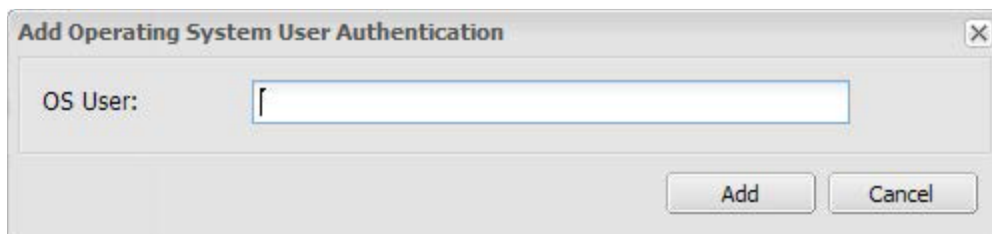
The screenshot shows the 'Add Application' dialog box. The 'Name' field contains the text 'ASCI_ActiveBatch'. The 'Description' field is empty. The 'Business owner' section has fields for 'First Name', 'Last Name', 'Email', and 'Phone', all of which are empty. The 'Location' field is a dropdown menu showing a backslash character. Below this are three checkboxes: 'Access Permitted' (unchecked), 'Expiration Date' (unchecked), and 'Disabled' (unchecked). The 'Access Permitted' checkbox has 'From:' and 'To:' dropdown menus. The 'Expiration Date' checkbox has a date picker. At the bottom right are 'Add' and 'Cancel' buttons. A footer note reads: 'Allow extended authentication restrictions. This requires Provider's approval for the application.'

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

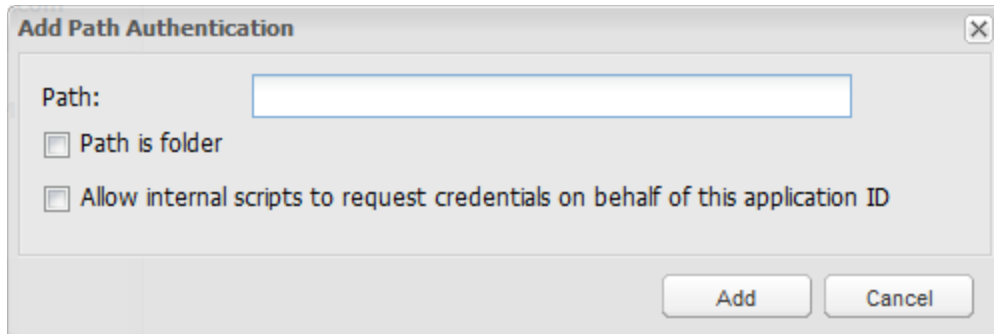
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ 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.

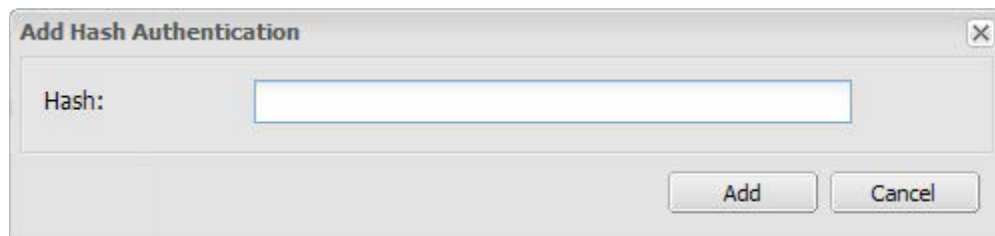


The 'Add Path Authentication' dialog box contains a 'Path:' text input field. Below it are two checkboxes: 'Path is folder' and 'Allow internal scripts to request credentials on behalf of this application ID'. At the bottom right are 'Add' and 'Cancel' buttons.

- ☐ 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.



The 'Add Hash Authentication' dialog box contains a 'Hash:' text input field. At the bottom right are 'Add' and 'Cancel' buttons.

- 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.

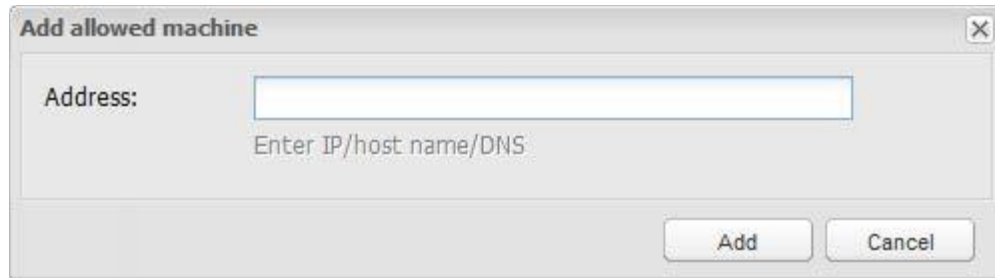
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2

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 a Windows-style dialog box titled "Add allowed machine" with a close button (X) in the top right corner. The dialog contains a label "Address:" followed by a text input field. Below the input field is a placeholder text "Enter IP/host name/DNS". At the bottom right of the dialog 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
ASCI_ActiveBatch		

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

ASCI_ActiveBatch 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.

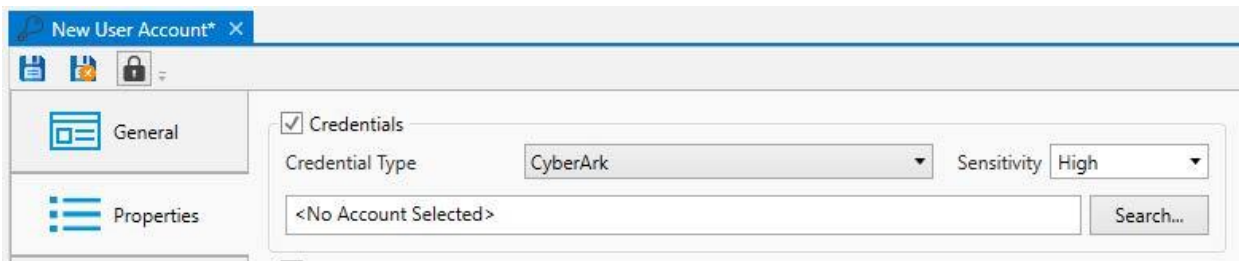
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

ACTIVEBATCH IT AUTOMATION INSTALLATION & INTEGRATION CONFIGURATION

Refer to the ActiveBatch Reference Manual for ActiveBatch IT Automation installation.

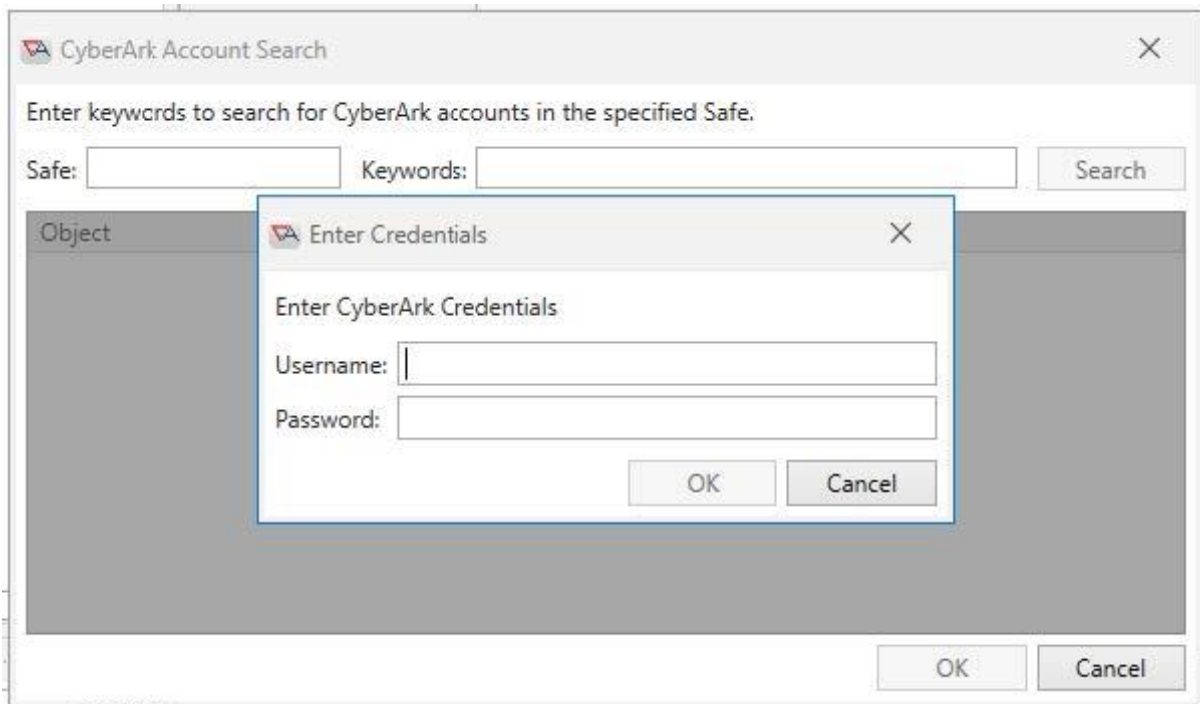
Configuration of an ActiveBatch User Account to retrieve credentials from CyberArk:

1. Select the CyberArk entry from the **Credential Type** drop-down on the **Credential Object Properties** page

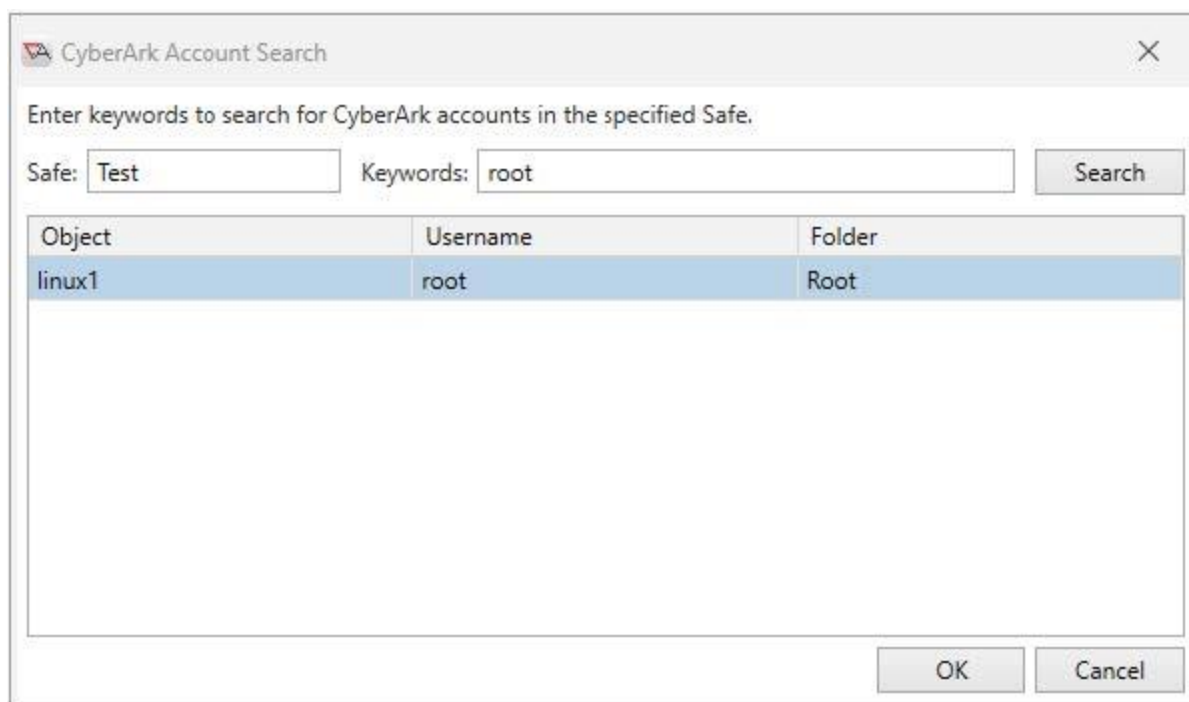


2. Click the **Search** button to search for a CyberArk account. This will open the **Search** dialog. Enter CyberArk credentials that have 'List and Retrieve' access within Secrets Manager to the desired CyberArk object.

Note: These credentials will NOT be stored by ActiveBatch, they are only used to validate that the user creating the ActiveBatch object has the appropriate permissions within CyberArk.



3. Enter the safe to search in and keywords to search for the account, then click the **Search** button. Multiple results may be returned. Select the desired account and click **OK**.



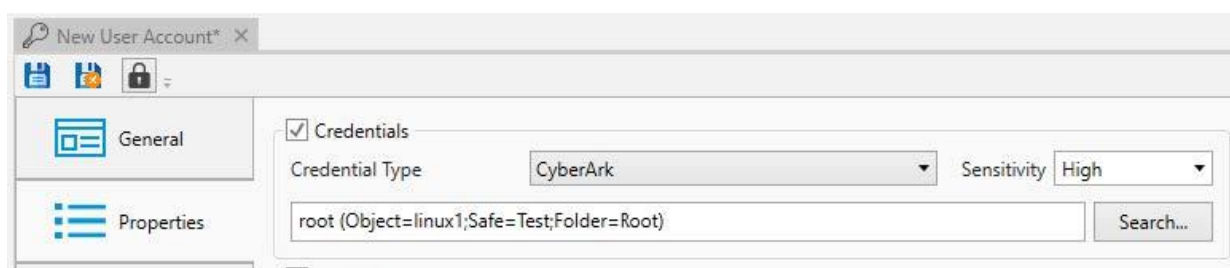
CyberArk Account Search

Enter keywords to search for CyberArk accounts in the specified Safe.

Safe: Keywords:

Object	Username	Folder
linux1	root	Root

- Clicking **OK** will validate that the user has Retrieve permission, and if successful, the account information will be saved into the ActiveBatch User Account Object.
Note: The account's password is NOT saved by ActiveBatch, it will be retrieved at the job's runtime by the Application using either the Local or Central provider.



New User Account*

General

☒ Credentials

Credential Type: Sensitivity:

- Save the ActiveBatch User Account Object, and it is now ready to be associated to Jobs to use.

The following configuration options are available within the ActiveBatch Extensions Manager to allow the user to configure the CyberArk Extension within ActiveBatch:

Central Credential Provider Server: The address of the CyberArk web endpoint to use with the REST API

Connection Timeout: The timeout value (in seconds) to use for the CyberArk API calls.

CyberArk SDK Path: The path to the NetPasswordSDK dll for use with the Local Client API

PVWA Base Address: The server/port to use for accessing the Password Vault Web Access SDK. This is required for permission validation when initially creating the CyberArk account object in ActiveBatch.

Use Local Credential Provider: When checked, ActiveBatch will use the CyberArk local client with the .NET API to retrieve the credentials from CyberArk (requires SDK path to be set). When unchecked, the REST API will be used (requires Webservice Endpoint to be set).

Configuration

CyberArk Service

Central Credential Provider...

https://<central-provider-server>:<port>

Connection Timeout

10

CyberArk SDK Path

C:\Program Files (x86)\CyberArk\ApplicationPasswordSdk\NetPasswordSDK.dll

PWVA Base Address

https://<PWVA-server>:<port>

Use Local Credential Provider

☒

Central Credential Provider Base Address

[Central Credential Provider API Only]: The server/port to use for accessing the CyberArk Central Credential Provider web service. This is required when using the Central Credential Provider
Example: https://<servername>:<port>

Apply

Reset

PARTNER CONTACT INFO

Business Contact	Name	Cassie Doheny
	Email	cdoheny@advsyscon.com
	Tel	973-539-2660
Technical Contact	Name	ASCI Support Team
	Email	www.advsyscon.com/myasci
	Tel	973-539-2660
Support Contact	Name	ASCI Support Team
	Email	www.advsyscon.com/myasci
	Tel	973-539-2660