



CYBERARK®



Secrets Manager Agentless CENTRAL Credential Provider (CCP_ Integration

Secrets Manger Integration – Technical Documentation Template

DOCUMENT PURPOSE:

MAKE A COPY OF THIS TEMPLATE FILE BEFORE YOU START WORKING ON YOUR INTEGRATON
DOCUMENTATION

Name of Company: Botprise

Website: <https://www.botprise.com/>

Name of Product: Botprise

Version: V1.6

Date: 03.18.24

Table of Contents

1	Partner solution overview	3
2	Key benefits	3
3	Product diagram & Description of Product Integration	4
3.1	Secrets Manager Integration	4
3.2	Credential Retrieval	4
4	Requirements	4
5	Secrets manager installation	4
6	SEcrets manager configuration	5
6.1	Defining The Application ID (APPID) and Authentication Details	5
6.2	Provisioning Accounts and Setting Permissions for Application Access	7
7	Partner Product installation & integration configuration	10
8	Partner contact info	11





Partner solution overview

>>Describe the Partner Product, providing context of usage and integration.

GenAI-driven Enterprise Operations Automation Platform

Version: V1.5

Platform components:

>>List platform components

Botprise Platform - execute workflows, automations, remediation; and process the result.

Integration Mesh - solution to create inbound and outbound integrations with 3rd party services.

Smart Studio (Drag-n-Drop workflow builder).

Catalog (Automation semantic layer) - library of pre-build Automations.

Gen-AI-workflow creation - solution to create remediation and automation workflows with AI based on users input.

Automation unit Gen-AI creation - creation of Botprise Automation Units with AI based on users input.

Autodiscovery (Autodiscovery - analytic solution to find issues to remediate in infrastructure).

Botprise Units (Botprise Automation Units, Botprise Trigger Units) - building blocks for Botprise workflows.



Key benefits

Benefits of Botprise

>>Benefit 1 | A streamlined integration framework that connects with all applications in minutes, enhancing efficiency and interoperability across your entire operational ecosystem.

>>Benefit 2 | Create automations and remediation with AI, from catalog or from code.

Run automations based on events from any services.

Security remediation

Automation of SecOps, ITOps, CloudOps and others from one source.

Benefits of integrating >> [Product Name] with CyberArk Central Credential Provider:

>>Benefit 1 | CyberArk users will be able to create workflows for remediation of issues detected by CyberArk.

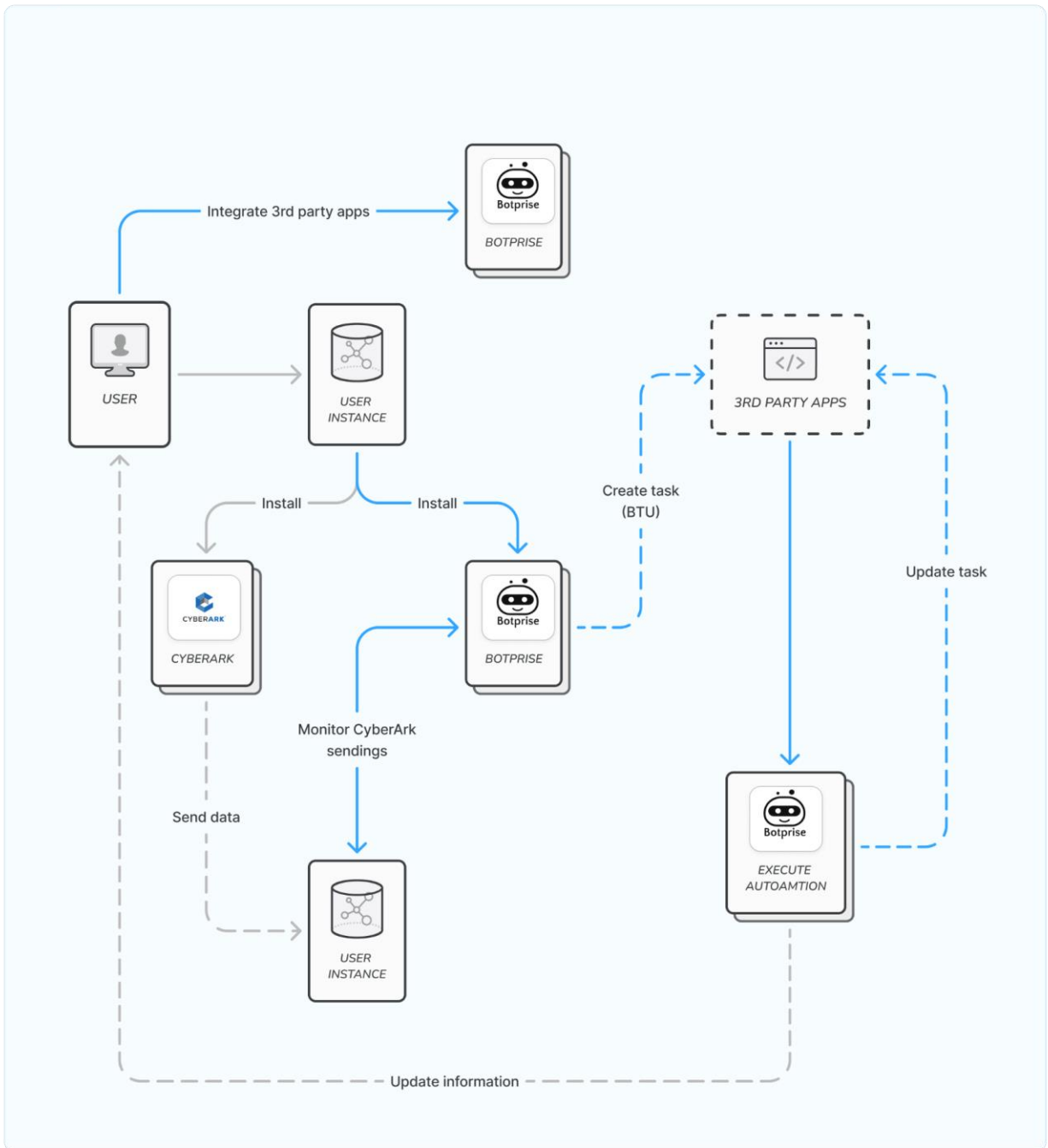
>>Benefit 2 | CyberArk users will be able to create automations with integrations of 3rd party applications.

CyberArk will be ready to be included in the automation chain of Botprise partners, though all applications which are integrated to Botprise will be ready to work with CyberArk.

Product diagram & Description of Product Integration

>>Insert Partner Product architecture diagram.

POS



>>Diagram should depict where the Secrets Manager Central Credential Provider (CCP) integration is located within the Partner Product architecture



Secrets Manager Integration

>>Describe Partner Product and depict where Secrets Manager Central Credential Provider (CCP) integration lies. Description might include:

Botprise provides a “listener” for CyberArk’s user. The listener should be installed on users instance. After setup is completed, the events will be sent to Botprise platform in encrypted format. All the actions could be executed based on the events.

>>Where Secrets Manager is integrated in Partner Product

Botprise does not interact with Secrets Manager.

>>Location of integration: Endpoint or mid-tier or central server

The event sent to Botprise should be used to create a Botprise Trigger Unit. This Trigger Unit is a starting point for workflows.

>>Number of mid-tier servers and number of endpoints in a typical installation

Depending on the amount of created unique instances and unique Botprise trigger units.

Credential Retrieval

>>Describe how the credential retrieval plays a role within the Partner Product.

>>Describe the credential retrieval flow in detail

User should be able to run the package of Botprise Cloud Formation template for the user’s infrastructure.

>>Describe how credential retrieval is triggered

The operations with the user’s credential are totally under the user’s control. Botprise does not work with user credentials.

>>Describe the circumstances under which credentials are retrieved

Inside the admin panel of a user instance, Botprise should get a role with the rights based on the type of integration the user would like to run.

>>Describe the frequency at which credentials are retrieved

The amount of activities connected to the authorization and authentication based on the amount of the CyberArk’s events used as Botprise Trigger Unit.

>>Describe specific properties required for queries on various platforms



>>Unix - Full support

>>Windows - Limited support

Requirements

This section lists the requirements for the integration.

>>List software, network, and hardware requirements. Provide context of requirements and team expertise for user planning needs.

>>Requirement 1 | Internet Connection

>>Requirement 2 | Ability to be online during the process of execution

>>Requirement 3 | The starting point event for running the workflow (To have a event that can e detected and sent to Botprise)

The script to set up an integration.

```
import socket

from ast import literal_eval

import requests

from cloudevents.conversion import to_binary, to_structured

from cloudevents.http import CloudEvent

HOST = " " # Listen on all network interfaces

PORT = 514 # Port number to listen on

attributes = {"type": "user.logon", "source": "services-uscentral.skytap.com"}

# Create a socket object

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:

    # Bind the socket to a specific network interface and port number

    s.bind((HOST, PORT))

    print(f"Listening on port {PORT}...")

    # Listen for incoming connections

    s.listen()

    # Accept incoming connections

    conn, addr = s.accept()

    print(f"Connected by {addr}")

    # Receive data from the client

    while True:

        data = conn.recv(1024)

        if not data:

            break

        data = data.decode("utf-8")
```

```
event = CloudEvent(attributes, literal_eval(data[data.find("{}"):]))
print(event, type(event))

headers, body = to_structured(event)

print(headers, body)

request = requests.request("POST",
"https://demoapi.botprise.com/integrations/Webhook/gAAAAABlBF_HkSpPtGI9FB6WryNv1IYAm-
kIlhgtXWlr1uDCEgJHVZQPMizmLbKurOxaVuk8g4Jg7bXavuNmzBEYB9Ele>

print(request.status_code)

print(f"Received data: {data.strip()}")
```



CENTRAL CREDENTIAL PROVIDER INSTALLATION

To install Central Credential Provider (CCP), see the Central Credential Provider installation documentation. (Based on guys feedback about windows)

CENTRAL CREDENTIAL PROVIDER configuration

The following sections provide details on Central Credential Provider (CCP) configuration with your CyberArk PAM solution (PAM Self-hosted / Privilege Cloud).

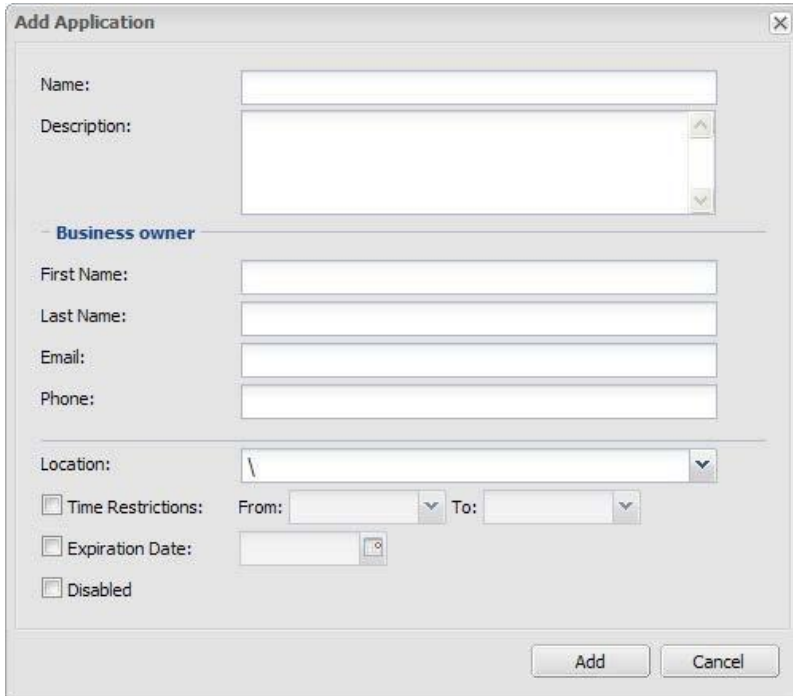
Define the application ID (app ID) and authentication details

To define the application, define it manually through the define it manually through the CyberArk Password Vault Web Access (PVWA) / Privilege Cloud interface:

Log in with a user that has permissions to manage applications (it requires Manage Users authorization).

In the Applications tab, click Add Application. The Add Application page appears.

>>Replace the following screenshot with data filled in (i.e. with the pre-defined APPID the customer should use, specified in the “Name” field)



Specify the following information: ^[1]_[SEP]

In the Name box, provide the unique name (ID) of the application. The recommended application ID for this integration is: ^[1]_[SEP]APP ID = _>>myapp_, for example

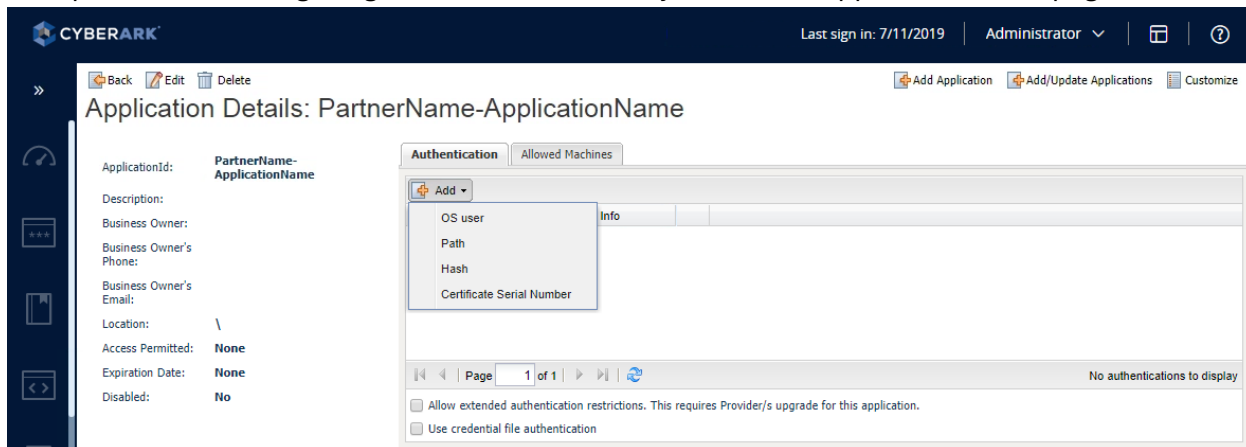
In the Description box, provide a short description of the application that will help you identify it.

In the Business owner section, provide contact information about the application’s business owner.

In the Location box, specify the location of the application in the Vault / Privilege Cloud 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. ^[1]_[SEP]

>>Replace the following image with a screenshot of your Partner Application Detail page



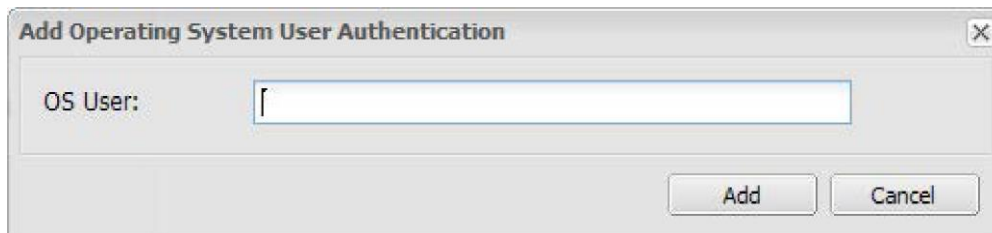
Select the Allowing extended authentication restrictions option. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

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. 

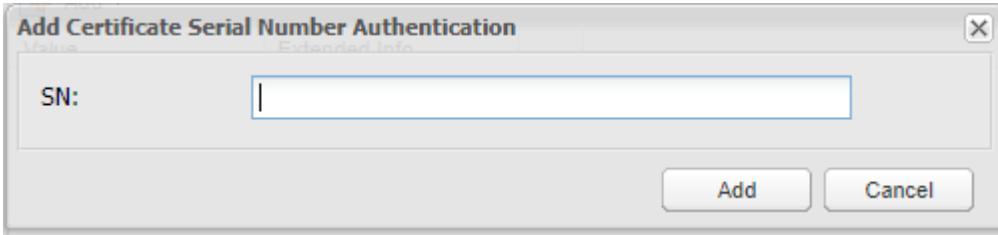
Select the authentication characteristic to specify.

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.

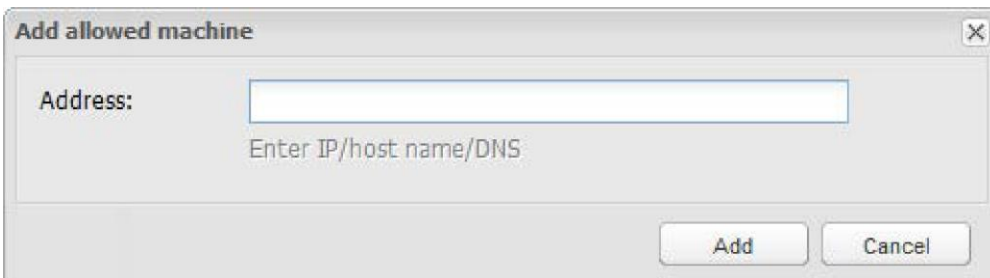
Specify the Certificate Serial Number:



The dialog box titled "Add Certificate Serial Number Authentication" has a close button (X) in the top right corner. It contains a tabbed interface with "Value" and "Extended Info" tabs. The "Value" tab is active, showing a label "SN:" followed by a text input field. At the bottom right, there are "Add" and "Cancel" buttons.

Specify the application's Allowed Machines. This information enables Credential Provider to make sure that only applications that run from specified machines can access their passwords. [SEP]

In the Allowed Machines tab, click Add. The Add allowed machine window is displayed. [SEP]



The dialog box titled "Add allowed machine" has a close button (X) in the top right corner. It contains a label "Address:" followed by a text input field. Below the input field, the text "Enter IP/host name/DNS" is displayed. At the bottom right, there are "Add" and "Cancel" buttons.

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.

Provision accounts and set permissions for application access

For the application to perform its functionality or tasks, the application must have access to particular accounts that already exist, or to new accounts to be provisioned in CyberArk Vault / Privilege Cloud.

In the >>Replace with the name of your password safe: [Password Safe], provision privileged accounts that will be required by the application. You can do this in one of the following ways: [SEP]

Manually – Add accounts manually one at a time, and specify all the account details [SEP]

Automatically – Add multiple accounts automatically using the Password Upload feature

For this step, you need Add accounts permissions in the >>[Password Safe].

For more information about adding and managing privileged accounts, see the documentation for your PAM solution.

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

Add the CCP 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 be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

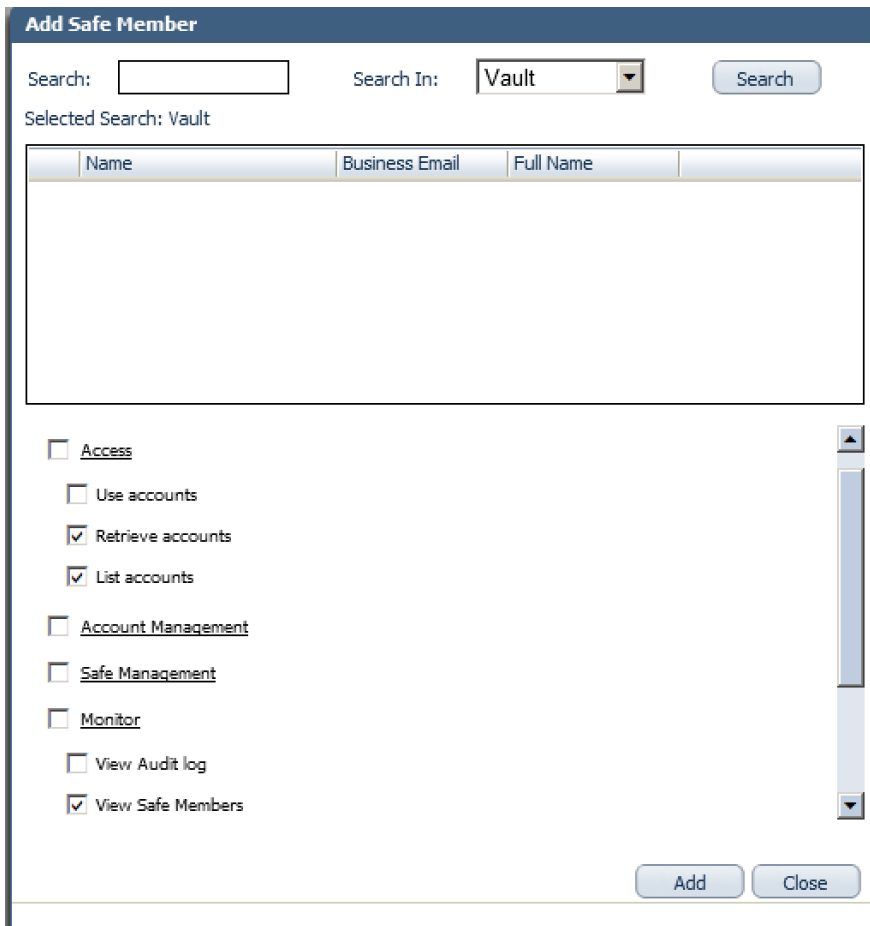
Add the CCP user as a Safe member with the following access:

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**

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 the application (the app ID) as a Safe member with the following access:

Retrieve accounts

Add Safe Member

Search: Search In: **Vault**

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

If the Safe is configured for object level access, make sure that both the CP user and the application have access to the passwords to retrieve.

For more information about configuring Safe members, see the documentation for your PAM solution.

>>[Partner Product]: integration configuration

Partner - please complete

This section describes how to configure the integration between >>[product name] Botprise and Credential Providers.

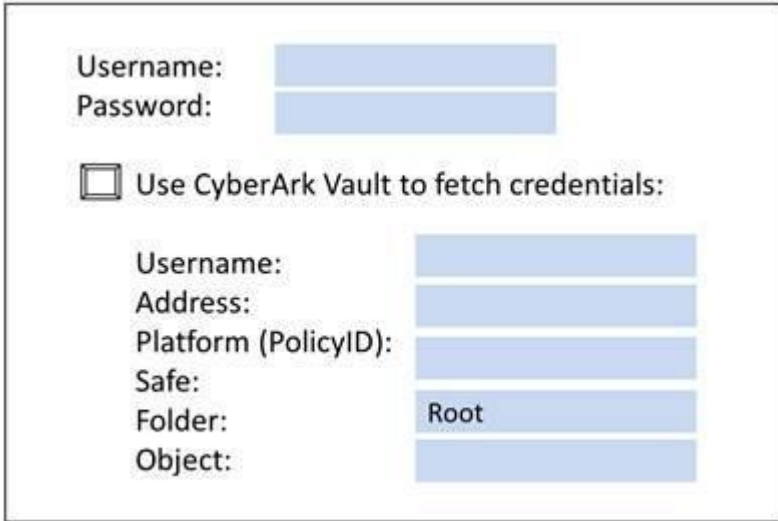
Prerequisite: Install >>[product name] Botprise. For installation instructions, see >> [Hyperlink to Partner Product installation docs] <https://botprise.com/CyberArk> (not created yet 03.18.24) .

>>List specific steps to configuring Partner Product to work with the Credential Provider, including:

Any special configurations within or outside the product

How to specify credentials for scanning, that are stored in the Vault/Privilege Cloud (instead of providing usernames and passwords) – include screenshots and description of steps

>>Replace the following screenshot with your actual integration configuration screenshots Partner Application UI:



The screenshot shows a configuration form for the CyberArk Partner Application UI. It includes the following fields and options:

- Username:** [Text input field]
- Password:** [Text input field]
- ☐ **Use CyberArk Vault to fetch credentials:**
- Username:** [Text input field]
- Address:** [Text input field]
- Platform (PolicyID):** [Text input field]
- Safe:** [Text input field]
- Folder:** [Text input field with "Root" pre-filled]
- Object:** [Text input field]

>>Replace the following with your actual configuration options.

Here are some common use cases:

Windows domain credentials or other standard credentials

The user will specify: username, address, platform

Safe name – optional but recommended for increasing performance

Local accounts (windows/Unix)

The user will specify: username & platform

Safe name – optional but recommended for increasing performance

When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned

Non-standard credentials (can't be unique with username+address+platform)

The user will specify: Safe and object name (folder is usually root by default)

Partner contact info

Business Contact	Name	Oksana Riabichko
	Email	oksana.riabichko@ botprise.com
	Tel	6692924640
Technical Contact	Name	Alex S
	Email	support@ botprise.com
	Tel	
Support Contact	Name	
	Email	
	Tel	