



CSOAR - Procedure for using CyberArk in CSOAR

CSOAR - Procedure for using CyberArk in CSOAR

Name	CSOAR - Internal Change Management procedure.docx
Owner	SumoLogic
Department	CSOAR
Status	Draft
Classification	TRADE SECRET
Version	V0.1
Date	November 15th 2022

Document Classification:

Notice

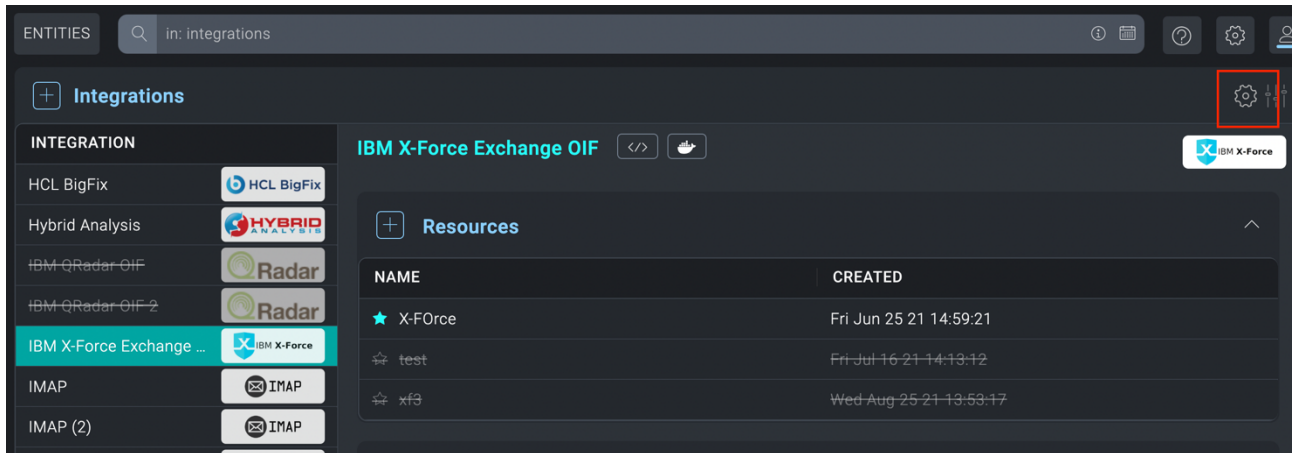
This document is intended only for the use of the individual or entity to which it is provided and contains information that is privileged, confidential, and may be exempt from disclosure under applicable law. This notice serves as warning that any dissemination, distribution, or copying of this document is strictly prohibited without the express written consent of SumoLogic.

What is this guide for?

This guide has been made to describe the procedure in a practical way for CSOAR customers to configure CyberArk Credential Manager and to use CyberArk with CSOAR.

Credential Manager - CyberArk

Using CyberArk Credential Manager you will be able to control integration resources data by using stored information



You can access the integration section by clicking on cogwheel icon on the top right.

In the following modal you can set up the URL, port and credentials needed to connect to CyberArk Components server.

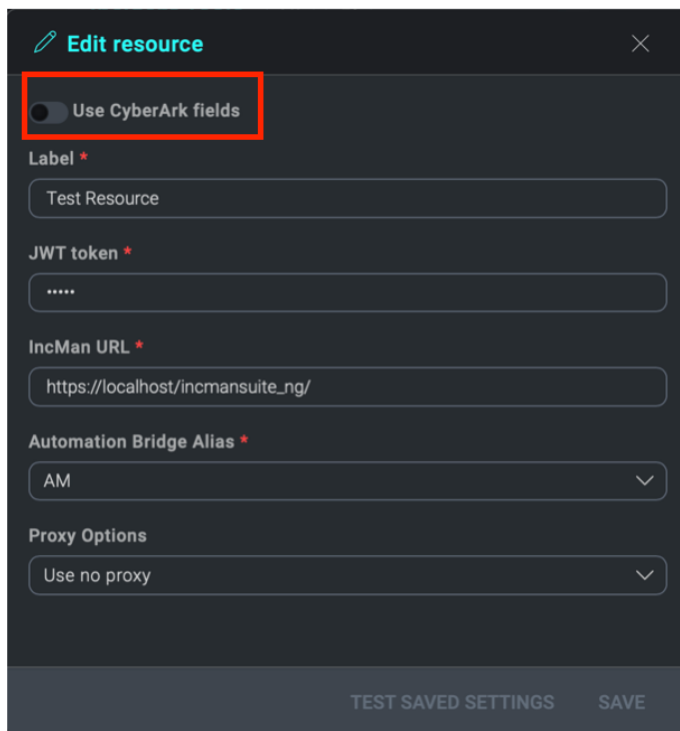
The screenshot shows the 'Credential Manager' configuration modal. It has a title bar with a gear icon and the text 'Credential Manager'. Below the title bar, there is a toggle switch labeled 'Enable' which is currently turned on. Underneath, there is a section 'Select credential manager *' with a dropdown menu showing 'Cyberark'. Below this, there are four input fields: 'Host *' with the value 'https://services-uscentral.skytap.com', 'Port *' with the value '11870', 'Username *' with the value 'Administrator', and 'Password *' with masked characters '....'. At the bottom right of the modal, there is a blue 'SAVE' button.

If **enabled** you will be able use CyberArk functionalities.

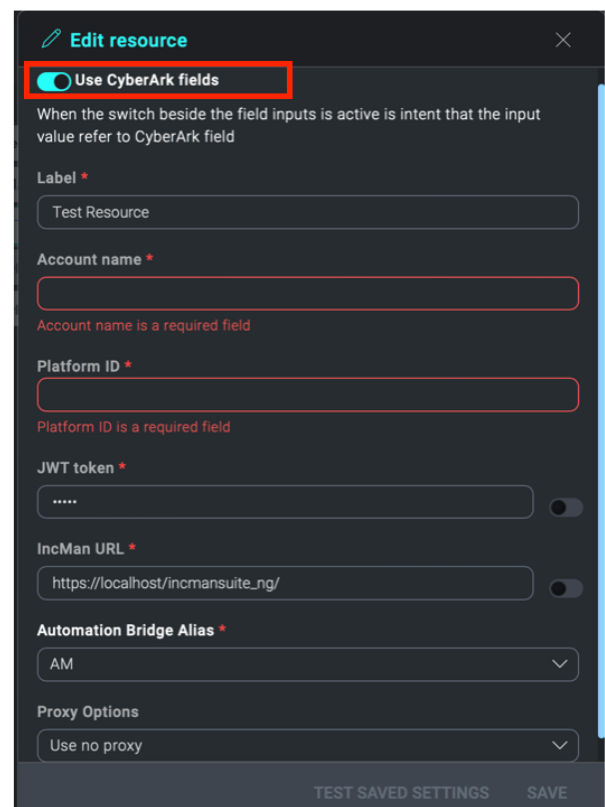
In **Integration resources/Edit resource** two new CyberArk mandatory fields will appear:

Account Name -> **userName** in CyberArk

Platform ID -> **platformId** in CyberArk



The screenshot shows the 'Edit resource' dialog with the 'Use CyberArk fields' toggle switch disabled. The fields are: Label (Test Resource), JWT token (masked), IncMan URL (https://localhost/incmansuite_ng/), Automation Bridge Alias (AM), and Proxy Options (Use no proxy). The 'TEST SAVED SETTINGS' and 'SAVE' buttons are at the bottom.



The screenshot shows the 'Edit resource' dialog with the 'Use CyberArk fields' toggle switch enabled. The fields are: Label (Test Resource), Account name (required field), Platform ID (required field), JWT token (masked), IncMan URL (https://localhost/incmansuite_ng/), Automation Bridge Alias (AM), and Proxy Options (Use no proxy). The 'TEST SAVED SETTINGS' and 'SAVE' buttons are at the bottom.

Each field can be activated independently (toggle to the right) and used in CyberArk.

5

In the image below you can see two different custom fields.

The screenshot shows a dark-themed 'Edit resource' dialog box. At the top, there is a toggle switch labeled 'Use CyberArk fields' which is turned on. Below this, a text box explains: 'When the switch beside the field inputs is active is intent that the input value refer to CyberArk field'. The form contains several fields: 'Label' with the value 'Test Resource'; 'Account name' with the value 'cymb'; 'Platform ID' with the value 'CyberArkMB'; 'JWT token' with the value 'MB3' and a toggle switch that is turned on; 'IncMan URL' with the value 'https://localhost/incmansuite_ng/' and a toggle switch that is turned off; 'Automation Bridge Alias' with a dropdown menu showing 'AM'; and 'Proxy Options' with a dropdown menu showing 'Use no proxy'. At the bottom, there are two buttons: 'TEST SAVED SETTINGS' and 'SAVE'.

The first field (**JWT token**) has been enabled for usage in CyberArk, the second has not (**IncMan URL**).

When activated you'll be able to enter the corresponding CyberArk Platform ID's properties (*see the image below*).

The screenshot shows the 'cymb On administrator' interface. At the top, it says 'cymb On administrator'. Below this, there are icons for a lock and a clock, followed by 'Platform: CyberArkMB Vault' and 'Safe: test2'. There are four tabs: 'Overview', 'Details', 'Activities', and 'Versions'. The 'Details' tab is selected. Below the tabs, there is a text box containing the URL 'https://api.xforce.ibmcloud.com'. Below this, there are two rows of data. The first row has a red box around the value 'MB2' and the text 'client_credentials'. The second row has a red box around the value 'MB3' and the text '84ca4444-9082-40b7-'.

Keep in mind field are case sensitive.

During the execution of the action, the field content (in the above case **MB3**) will be replaced by the correspondent CyberArk value (**84ca4444-9082-40b7-**)

In the enabled fields you can also get the password of the CyberArk account.

To do this, write the word **Password** in the field

Pay attention to uppercase and lowercase letters.

Important: In CyberArk enabled fields the only data type allowed will be strings (even if the same field was configured to accept lists, checkboxes, numbers, etc).

The only property that will be retained is the mandatory nature of the field.

Enabling a field for CyberArk will store previously entered and saved values, the same is not true otherwise.

The screenshot shows a dark-themed 'Edit resource' dialog box. At the top, there is a title bar with a pencil icon and the text 'Edit resource', and a close button (X) on the right. Below the title bar, there is a toggle switch labeled 'Use CyberArk fields' which is currently turned on. Underneath this toggle, a text block explains: 'When the switch beside the field inputs is active is intent that the input value refer to CyberArk field'. The dialog contains several input fields, each with a label and a red asterisk indicating it is mandatory:

- Label ***: A text input field containing 'Test Resource'.
- Account name ***: A text input field containing 'cymb'.
- Platform ID ***: A text input field containing 'CyberArkMB'.
- JWT token ***: A text input field containing '.....'. To the right of this field is a toggle switch that is currently turned off. Both the input field and the toggle switch are highlighted with red rectangular boxes.
- IncMan URL ***: A text input field containing 'https://localhost/incmansuite_ng/'. To the right of this field is a toggle switch that is currently turned off.
- Automation Bridge Alias ***: A dropdown menu showing 'AM'.
- Proxy Options**: A dropdown menu showing 'Use no proxy'.

At the bottom of the dialog, there are two buttons: 'TEST SAVED SETTINGS' and 'SAVE'.

Credential Manager - CyberArk

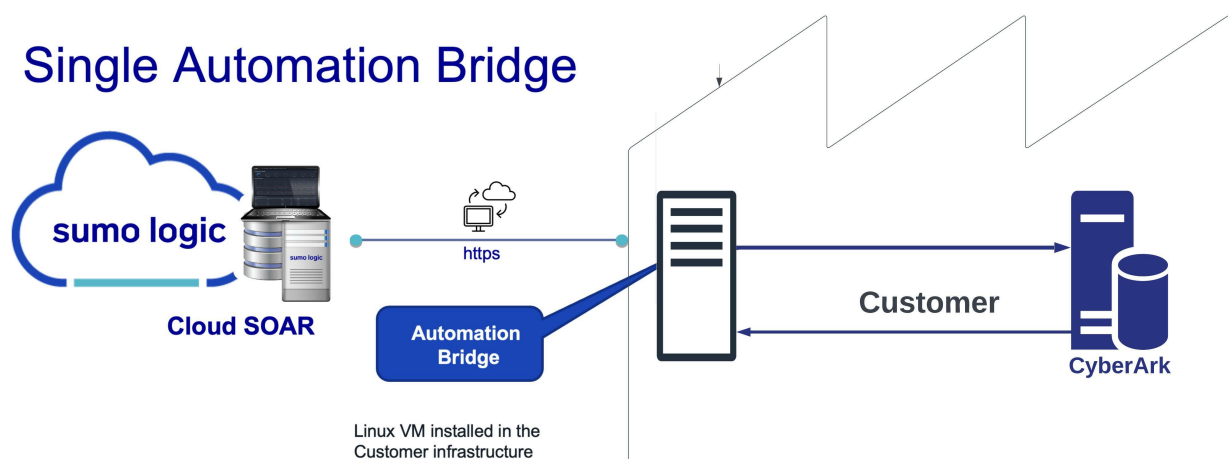
In order to configure the automation bridge for CyberArk you'll need to add the following certificates given by CyberArk:

- RootCA_new.crt
- client_new.crt
- client_new.pem

to the **/opt/automation-bridge/** directory on the server where the bridge is running.

The names must be exactly the same.

Brief explanation of process flow among CSOAR, Bridge and CyberArk



The Automation Bridge process queries CSOAR to check if there are any actions to process.

Bridge checks if that action resource has CyberArk configured fields (as seen above).

It will query CyberArk Component server by using the credentials previously saved on CSOAR.

CyberArk will then respond by returning the value properties, and Bridge will use those information to perform the action.