sumo logic

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:

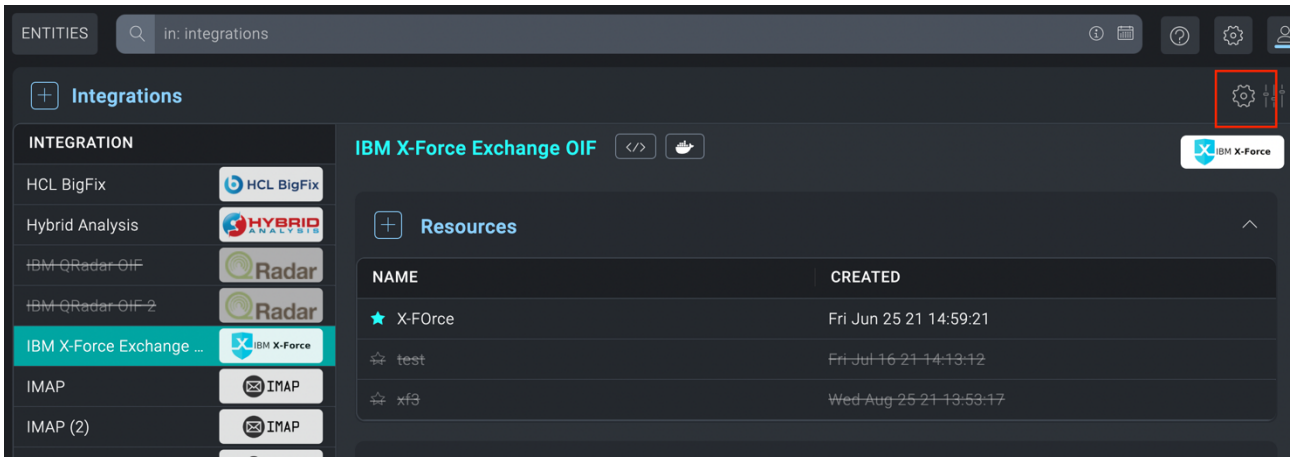
Notice

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.

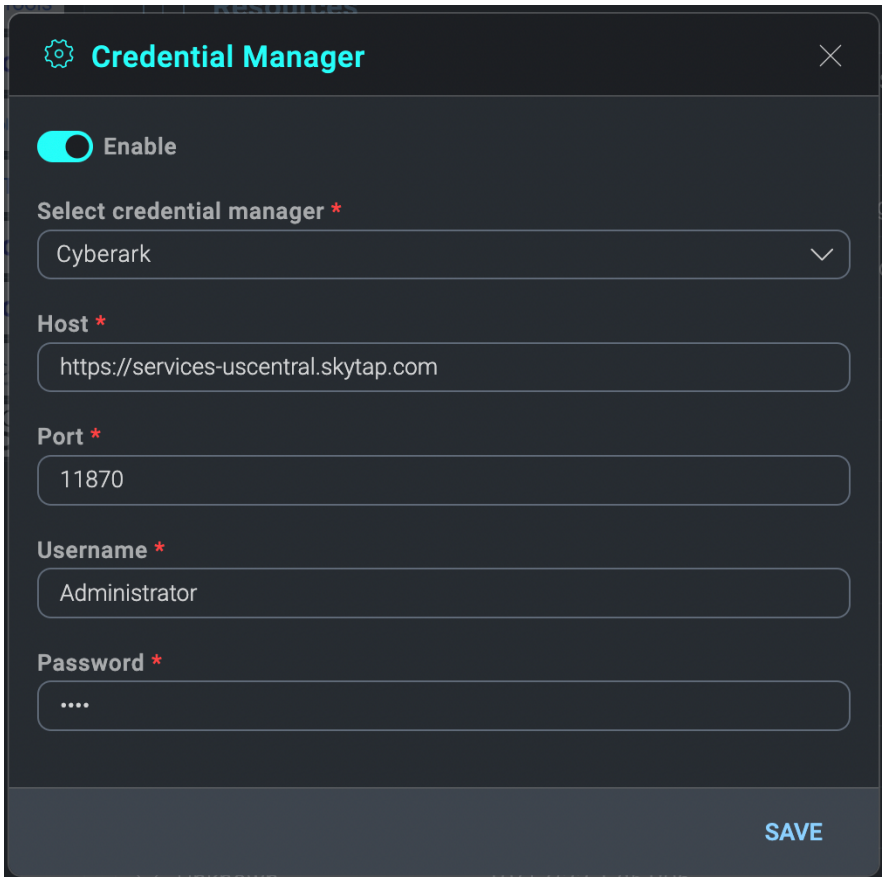
Credential Manager - CyberArk

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.

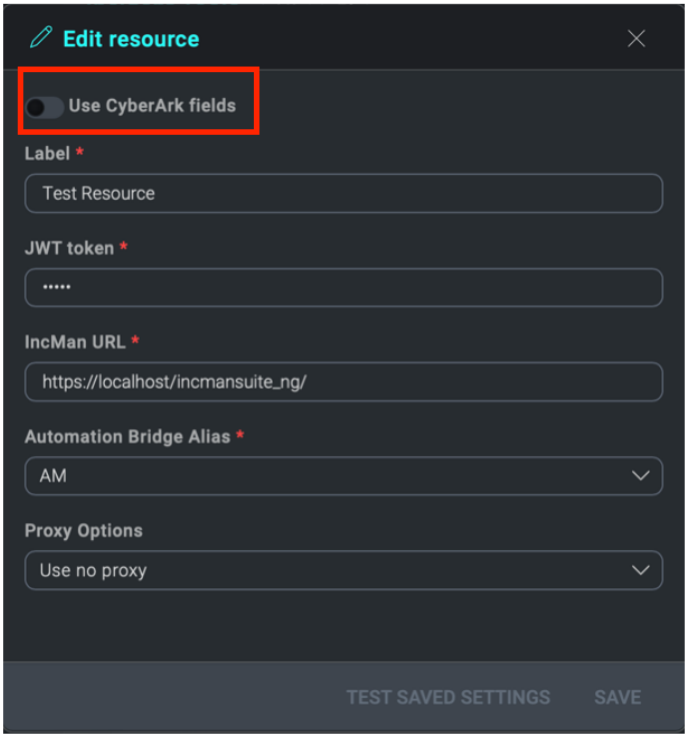


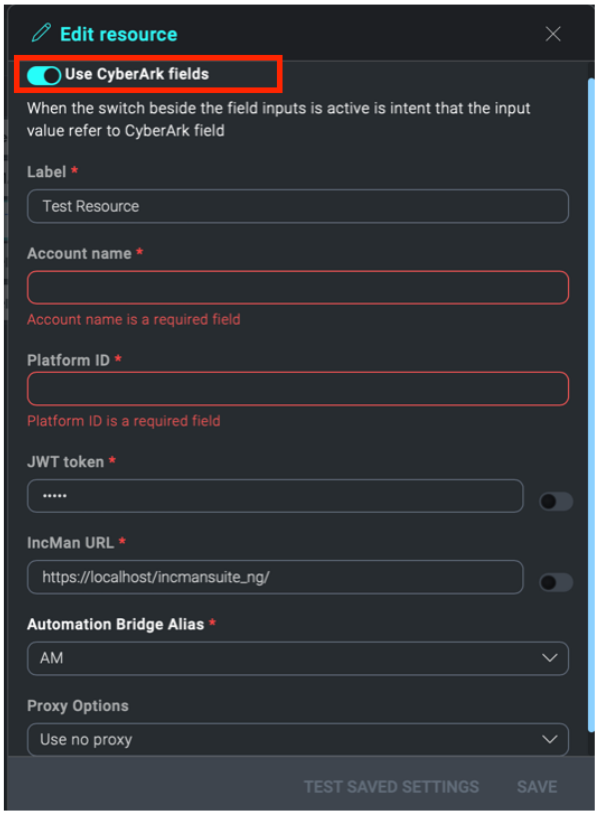
If **enabled** you will be able use CyberArk functionalities.

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

Account Name -> userName in CyberArk

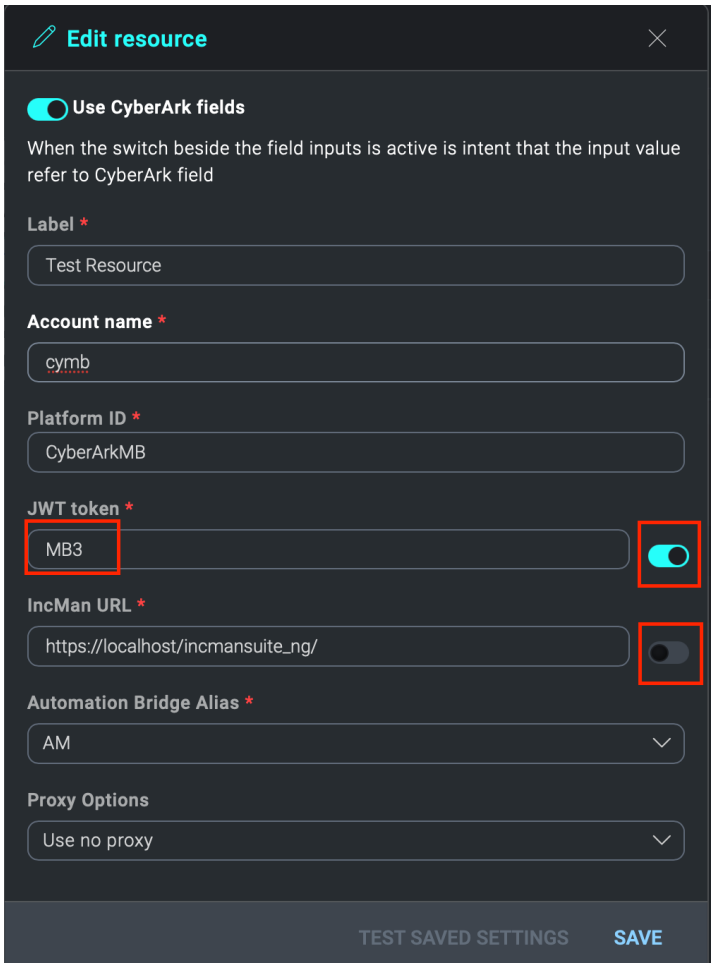
Platform ID -> platformId in CyberArk





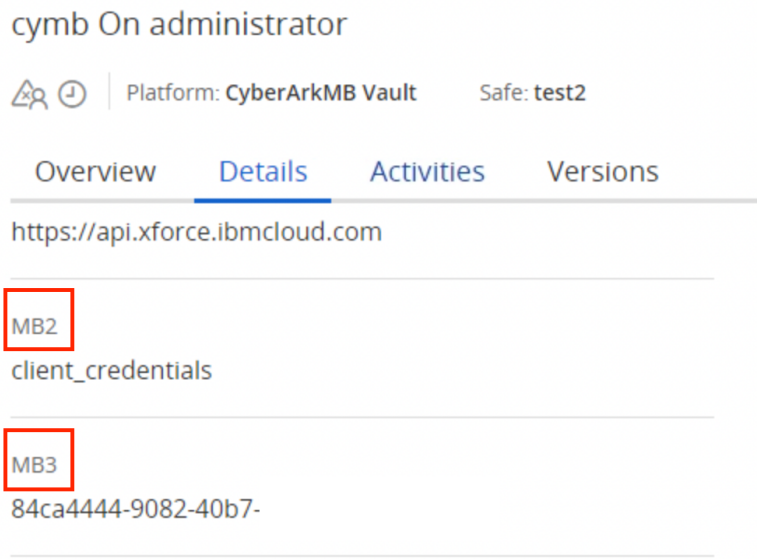
Each field can be activated independently (toggle to the right) and used in CyberArk.

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



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*).



<u>Keep in mind field are case sensitive</u>.

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.

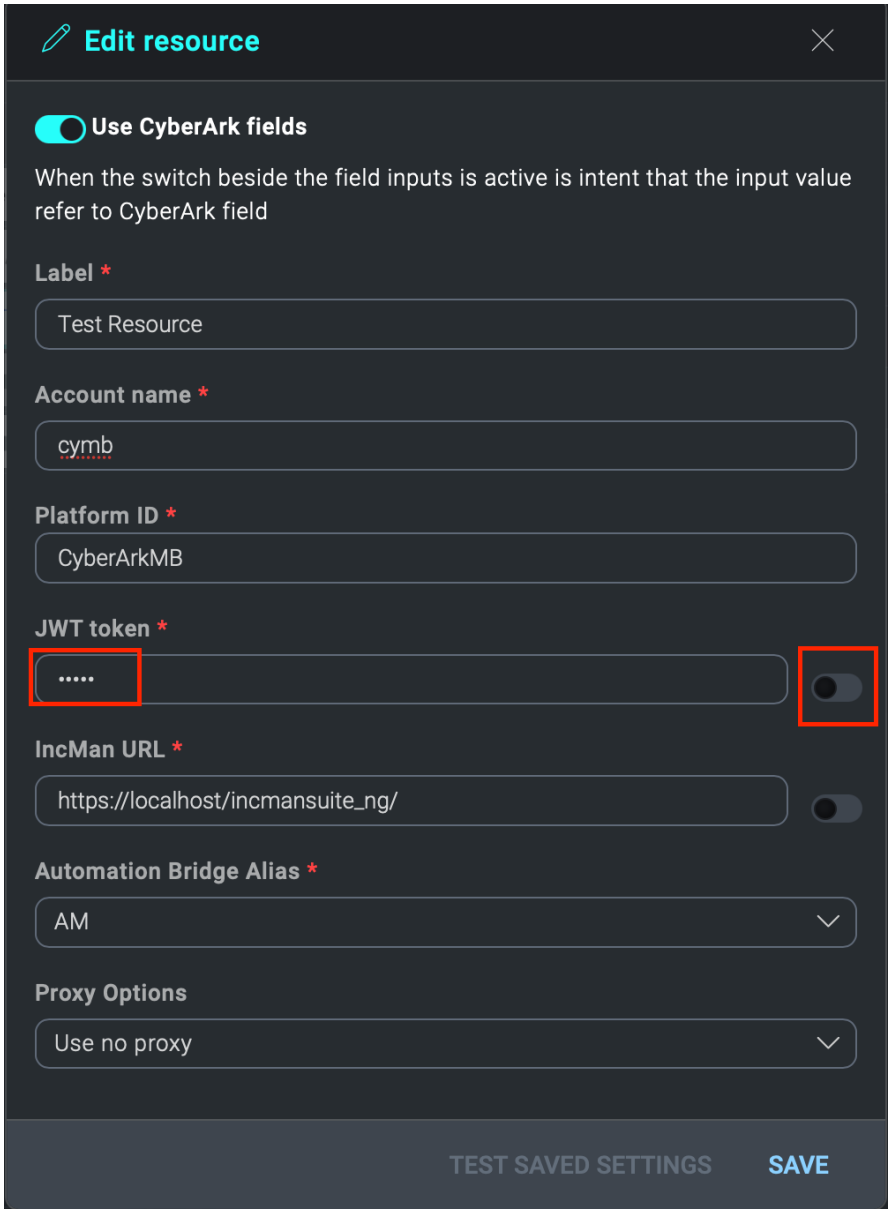
To do this, write the word **Password** in the field

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.



Credential Manager - CyberArk

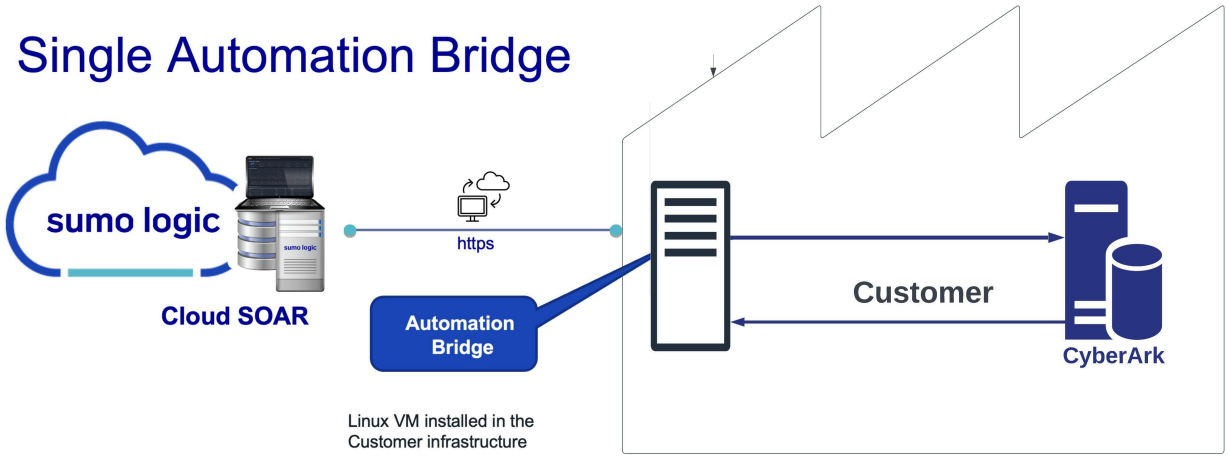
In order to configure the automation bridge for CyberArk you'll need to add the following certificates given by CyberArk:

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