

Rapid7 CyberArk Discovery Module

Version 1.1



Pre-Install

The Discovery Module takes results from Rapid7, identify discovered endpoints, apply account templates, normalize the data for CyberArk WebServices SDK, finally input the account in the CyberArk Vault using the WebServices SDK.

Prerequisites

The Discovery Module runs on the same platform as the SCIM Server and utilizes the same functionality and has the same system requirements as the SCIM server. For further information on setting up the SCIM Server please refer to the SCIM Implementation guide:

<https://cyberark-customers.force.com/mplace/s/##a3550000000EiAfAAK-a3950000000jiT7AAI>

Accounts for Discovery Module

- CyberArk account that authenticates to the WebServices SDK with permissions to Add Accounts
- Account to authenticate to Rapid7 solution with permissions to retrieve results

System Requirements

- ** 8 Core Processors
- ** 32GB of RAM
- Microsoft Windows Server 2012 R2 (also supports Server 2016)
- Java Virtual Machine version 1.8

** These are suggested requirements for the SCIM Server but if you are using this exclusively for Discovery this much processing may not be needed.

CyberArk Requirements

- CyberArk SCIM Server 1.1.4
 - CyberArk Vault Server v9.8 or higher
 - AIM Credential Provider v9.8 or higher

NOTE:

Implementation

Now that the SCIM Server is installed and functioning correctly, it will be necessary to build out the configurations for the Discovery module.

Account Objects for Discovery Module

For information regarding the process of adding accounts, here is the link to the CyberArk documentation for this process:

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Onboarding-Accounts-and-SSH-Keys.htm>

WebServiceURL

The Discovery module requires the **baseURL** for both the CyberArk WebServices SDK and the Rapid7 API. The Discovery process will attempt to pull the baseURL from the following three places in this order:

- DiscoveryConfig.yml under connectionAccount
- WebServiceURL file category of the account object
- Address field of the account object

Adding WebServiceURL File Category to Platform

1. Navigate to **Platform Management**
2. Select the Platform used for the WebServices SDK account (CyberArk Vault)
3. Expand **UI & Workflows**
4. Expand **Properties**
5. Right-click **Properties**, select **Add Property**
6. In the Properties window, input the following into the Name parameter:
WebServiceURL
7. Click Apply, OK

WebServices SDK

This account will be used to authenticate to the WebServices SDK and used to create the account objects found in the Discovery process.

1. Select the **Accounts** tab
2. In the **Accounts View**, click **Add Account**
3. In the **Select System Type** window select **Application**, click Next
4. In the **Assign to platform** window, select the **Platform** modified in the last section, click Next

NOTE: If it is a local CyberArk Vault account, assign the CyberArk Vault Platform for proper management of the credential

5. Select or Create a **Safe** to store the object, click Next

NOTE: Storing in the SCIM Config safe provides a centralized location for easier management

6. Provide a **Username**

7. Provide the **Address**

NOTE: If you are using a local Vault account this is going to be the address of the Vault

8. Provide a **Password**

NOTE: You can customize the account name to make it easier for placing it in the config files

9. Scroll down to the **Optional** fields and in the **WebServiceURL** field enter the WebServices SDK **baseURL**:

https://<PVWA_URL>/PasswordVault

10. Select **Add**

Discovery Source

This account will be used to authenticate to the Discovery Source solution to retrieve scan results. Below are links to the available Discovery solutions available.

Rapid7 CPM plugin on CyberArk MarketPlace:

<https://cyberark-customers.force.com/mplace/s/#a352J000000pbWQQAY-a392J000001h4MQQAY>

1. Navigate to the **Platform Management** view
2. Select **Import Platform**
3. In the Windows Explorer window locate and select the zip file downloaded from the MarketPlace link above, click Open
4. The Rapid7 accounts Platform should be imported
5. Select the **Accounts** tab
6. In the **Accounts View**, click **Add Account**
7. In the **Select System Type** window select **Application**, click Next
8. In the **Assign to platform** window, select the **Rapid7** platform, click Next
9. Select or Create a **Safe** to store the object, click Next

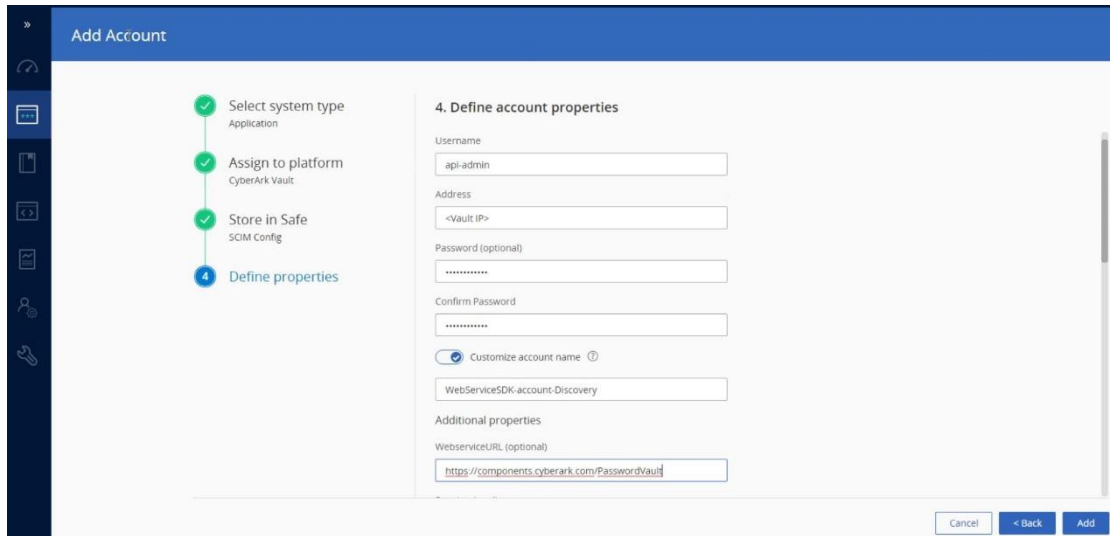
NOTE: Storing in the SCIM Config safe provides a centralized location for easier management

10. Provide the **Username**
11. Provide the **Address** of the **Rapid7** solution
12. Provide a **Password**

NOTE: You can customize the account name to make it easier for entering in the config files

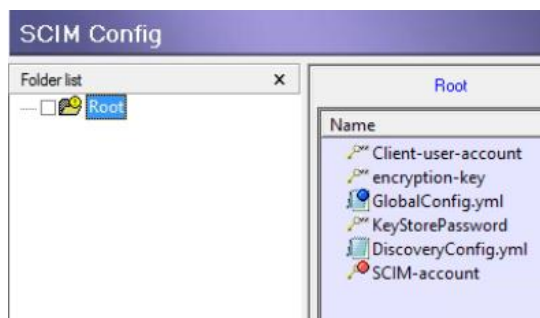
13. Scroll down to the **Optional** fields and if you added the **WebServiceURL** field, enter the Rapid7 API **baseURL**

14. Select **Add**



Discovery Configuration

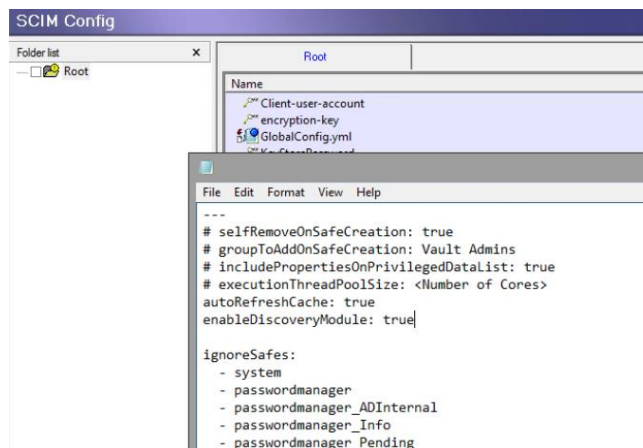
All of the necessary files for the Discovery module are located in the **SCIM Config** safe in the CyberArk Vault.



GlobalConfig.yml

This yaml file is the overall configuration for the entire Discovery/SCIM capability. Add the following syntax to enable the Discovery module:

1. Using the PrivateArk Client authenticate to the Vault navigate to the **SCIM Config** safe.
2. Retrieve the GlobalConfig.yml file and edit it
3. Add the following syntax to towards the top of the file as outlined below
enableDiscoveryModule: true



4. **Save** the file and **Return** it back to the safe

DiscoveryConfig.yml

This yaml file defines the work for the entire Discovery module. In the **Cyberark SCIM** folder in the SCIM installation zip file there is an example DiscoveryConfig.yml to modify. Below is an explanation of the parameters in the Discovery configuration.

webservice – Defines the Vaulted Account to authenticate to the CyberArk WebServices SDK API

connectionAccount	defines the object used for authenticating to the WebServices SDK	
	safe	Safe where the account object will be stored
	folder	Folder where the account object resides
	object	Object Name of the account object
	baseUrl	The base URL for WebServices SDK for example: https://components.cyberarkdemo.com/PasswordVault

discoveryJobs – Defines the Discovery Job for the Rapid7 discovered accounts

name	Name given to the Discovery job	
className	Java class for the Rapid7 Discovery module. It should have the value: com.cyberark.discovery.scheduler.Rapid7Discovery	
connectionAccount	Vaulted account object used to authenticate to Rapid7 API	
	safe	Safe where the account object will be stored
	folder	Folder where the account object resides
	object	Object Name of the account object
	baseURL	The base URL for Rapid7 API.
schedule	Values for how often the Discovery module goes to look for results from Rapid7	
	simple	integer in seconds of how often the Discovery module goes to look for work from Rapid7
	cron	syntax in cron format to define frequency the Discovery module goes to look for work from Rapid7. More information on cron syntax here: http://www.quartz-scheduler.org/documentation/quartz-2.2.2/tutorials/crontrigger
transforms	Configurations for data normalization	
	field	source field that will be normalized
	type	This will be the resulting of the value, and currently we support: - DateTime
	from	data format from the source
	to	data format needed for CyberArk WebServices SDK

rules – Defines the account template applied to the Discovered accounts

name	Name given to the rule		
path	JSONPath syntax to the location of the discovered account to be applied to the template Criteria specified in JSONPath format for the results from Rapid7 that should be considered for the Discovery Job. The syntax follows the standard JSONPath and you can check the syntax from the following links: - https://goessner.net/articles/JsonPath/ - https://github.com/json-path/JsonPath An online tester is available at: https://jsonpath.herokuapp.com		
action	Action to be taken in the WebServices SDK. Currently it supports the following value: - AddPending More actions will be added in upcoming versions.		
templateList	Definitions for the templates applied to Discovered accounts. This is a YAML array object, you can specify multiple templates.		
	description	Brief description of the action of the template	
	mapping	Defines account info to be applied to Discovered accounts. Default mapping.	
	UserName	Username given to discovered account	
	**DiscoveryPlatformType	PolicyID given to manage discovered account	
	OSType	Windows, Unix	
	**AccountCategory	Privileged, Non-privileged	
	AccountCategoryCriteria	Justification of Privilege	
	**AccountType	Local, Domain	
parentMapping	Mapping of properties at the Discovered entity level from Rapid7. This means it will get the field to be applied to the discovered account from the results of the Rapid7 scan. These can be any value that will need to be created for a given account.		
	Address	JSONPath syntax to the location in the discovery results to be applied for the Address field for the account being created	
	AccountDiscoveryDate	JSONPath syntax to the location in the discovery results to be applied for the AccountDiscoveredDate field for the account being created	
pathMapping	Mapping of properties for the resulting subset based on the path specified		
	Port	JSONPath syntax to the location in the discovery results to be applied for the Port field for the account being created	
	Database	JSONPath syntax to the location in the discovery results to be applied for the database field for the account being created	

******If multiple template accounts are listed, these fields can be moved to the **parentMapping** for template information of the entire group of **mapping** entries

Report CyberArk Assets to Rapid7

discoveryJobs – Defines the Discovery Job

name	Name given to the Discovery job	
className	Java class for the Rapid7 Discovery module. It should have the value: com.cyberark.discovery.scheduler.Rapid7Discovery	
endpoint	CyberArkAssets	
connectionAccount	Vaulted account object used to authenticate to Rapid7 API	
	safe	Safe where the account object will be stored
	folder	Folder where the account object resides
	object	Object Name of the account object
	baseURL	The base URL for Rapid7 API.
schedule	Values for how often the Discovery module goes to look for results from Rapid7	
	simple	integer in seconds of how often the Discovery module goes to look for work from Rapid7
	cron	syntax in cron format to define frequency the Discovery module goes to look for work from Rapid7. More information on cron syntax here: http://www.quartz-scheduler.org/documentation/quartz-2.2.2/tutorials/crontrigger
options	Configuration options for interacting with the capability	
	proxyURL	String value for Proxy support
	siteName	Default Rapid7 site name to submit the target assets from CyberArk
	siteSafeMapping	A list of sites with the corresponding regular expressions for the safes to report to the particular site. For example: siteSafeMapping: "TestSite": - "^SAFE.*\$"
enabled	Boolean value for whether the job is enabled or not (true/false)	