# Getting Started with REST Using Postman

# Setting up the Desktop App

Step 1: Accessing the Postman Page Navigate to the CyberArk REST API Postman page <u>https://cybr.rocks/RESTAPIv10</u>

### Step 2: Downloading & Running the App

Select "Run in Postman" and download the required software. The desktop app is recommended as the chrome extension is being deprecated. Once the Postman app has been installed click on the selected method to open the collection under the "Open with..." screen pictured below.

		🛞 Public 🕨 Run in Postman	Cyb
rk R	EST API v10	Language CURL	
C]	Open with	×	
JOFFI	Postman for Chrome V3.1.1 OR HIGHER		
e/CyberAr	Postman for Windows		
services	Don't have the app yet? <u>Get the app</u>		

\*Note sometimes chrome settings won't play nice with this and it may be easiest to use internet explorer.

### Step 3: Navigating to the Collection

Click on collections to display the CyberArk REST Collection

Q Filter	New Tab + •••		
History Collections	GET ∨ Enter request URL		
All Me Team	GET ∨ Enter request URL		
CyberArk REST API v10 [PUBLIC]	Authorization Headers Body Pre-r	equest Script Tests	
83 requests	ТҮРЕ		
Account Groups [v9.9.5+]	Inherit auth from parent $\sim$		
Account/ACL Methods [v9.0+]	The authorization header will be automatically generated when you send the		
Applications [v9.1+]			
Authentication	request. Learn more about authorization		
Central Credential Provider (CCP) [v			
Confirm Requests [v9.10+]	Response		

### Authenticating

In order to begin interacting with the vault, it is necessary to authenticate to obtain a session token.

### Step 1: Selecting a Logon Method

Select the proper logon method below and replace the {{BaseURL}} parameter with your PVWA Address. If you would prefer to set this as a variable, please see <u>Declaring Environment Variables</u> below

Q Filter		CyberArk [v9.0+]/LDA	4 × + •••		No Environment	$\sim$
History	Collections	▶ CyberArk [v9.0+]	/LDAP [v9.7+]/Radius	[v9.7+] Logon		Exan
All Me Team	_+ ↓= →	POST 🗸	{{BaseURL}}/Passwore	Wault/WebServices/auth/Cyberark/CyberArkAuthenticationService.sv	Params Send	✓ Si
Account/ACL Methods Applications [v9.1+]	s [v9.0+]	Authorization -	leaders (1) Body 4	Pre-request Script Tests		Соо
Authentication	000	TYPE				
POST CyberArk [v9.0+]/LD/	AP [v9.7+]/Radius [v9.7+	Inherit auth from	parent 🗸			
POST CyberArk [v9.0+]/LD/	AP [v9.7+]/Radius [v9.7+	The authorization h	neader will be	This request is using an authorization helper from c	ollection CyberArk REST API v10	[PUBLIC].
POST SAML Authentication	n Logon [v9.7+]	automatically gene	rated when you send	1 0 1		
POST SAML Authentication	n Logoff [v9.7+]	the request. Learn authorization	more about			

### Step 2: Specifying Logon Credentials

In the body section, specify the username and password of an account that can authenticate to the vault in place of the {{apiUsername}} & {{apiPassword}} parameters.



# Step 3: Testing Authentication

#### Hit "Send" to test the authentication.

Q Filter		CyberArk [v9.0+]/LDAf  + ••• No Environment	$\sim$
History	Collections	▶ CyberArk [v9.0+]/LDAP [v9.7+]/Radius [v9.7+] Logon	Examp
All Me Team	[]+ ↓= →	POST V components.cyberark.com/PasswordVault/WebServices/auth/Cyberark/CyberArkAuthentica Params	✓ Sav
Account/ACL Methods [ Applications [v9.1+]	v9.0+]	Authorization Headers (1) Body Pre-request Script Tests	Cooki
Authentication POST CyberArk [v9.0+]/LDAR	••• P [v9.7+]/Radius [v9.7+	● form-data ● x-www-form-urlencoded ● raw ● binary JSON (application/json) >	
POST CyberArk [v9.0+]/LDAF POST SAML Authentication I	P [v9.7+]/Radius [v9.7+ Logon [v9.7+]	<pre>2 "username":"SVC_CA_REST", 3 "password":"Cybenark1", 4 "useRadiusAuthentication":"false", 5 "connectionNumber":"1" 6 }</pre>	
POST SAML Authentication I			

Important!! While this method can work for testing, it is highly advised to use a tool such as CyberArk's **Application Identity Manager (AIM)** to pull credentials programmatically from the vault to eliminate any privileged credentials from being hard coded when put into scripts & code.

#### Step 4: Obtaining the Session Token

A successful authentication will yield a token that we can use to perform subsequent actions

Body Cookies (5) Headers (17) Test Results	Status: 200 OK Time: 124 ms Size: 1.15 KB
Pretty Raw Preview JSON V	C Q Save Response
RiYzg3MTg2NzBmBQEAAAAoQ31iZXJBcmsuU2Vydm1jZXMuV2ViL1N1c3Npb	NVpb249OC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZX1Ub2t1bj00MGJ1MW o25JZGVudG1maWVycwQAAAAFVG9rZW4ESW5mbw1TZXNzaW9uSWQEVH1wZQEBAQECAAAAB NVzE1OEU3M0RGNEE2MjZENjNBM0NCNDFDNDgwMjk2NTczMTUzMTg0NkY2OTU1Q0NDNTUw 'jYzhjZmQ4YzYxBgYAAAAACw=="
3 }	

### Performing Additional Vault Functions

In this example, we will look at listing safe members.

### Step 1: Selecting the Desired Function

Select "List Safe Members [v9.7+]" and specify the PVWA address for the {{BaseURL}}, desired safe for {{Safe}}, and the session token from the last step for the {{CyberArkLogonResult}} parameter (no quotes) and hit "Send".

Q Filter		CyberArk [v9.0+]/LE	Ai    List Safe Members [v9 × +		No Environm	nent v 👁 🔅
History	Collections	▶ List Safe Memb	ers [v9.7+]			Examples (0) 🔻
All Me Team Connections [v9.10+]	_+ ↓= →	GET 🗸	{{BaseURL}}/PasswordVault/WebSer	vices/PIMServices.svc/Safes/ <mark>({Safe})</mark> /Members	Params	Send 💙 Save 🗡
Managing Accounts		Authorization	Headers (2) Body Pre-reque	st Script Tests		Cookies Code
Managing Platforms [v9.10+]		Key		Value	Description	••• Bulk Edit Presets 🔻
Monitor Sessions [v9.10+]		Authorizatio	n	{{CyberArkLogonResult}}	Session Authoriza	ation Token
My Requests [v9.10+]		Content-Typ	e	application/json		
Onboarding Rules [v9.8+]		New key				
Policy/ACL Methods [v9.0+]	000	Response				
Safe Management		1/eshouse				
Safe Members						
GET List Safe Members [v9.7+]						

#### Step 2: Viewing the Results

A successful execution will return results as seen below with a status 200

GE	T V	http://components.cyberark.com/Pa eports/Members	asswordVault/WebServices/PIMServices.svc/Safes/PVWA	R Params	Send Y Save
Authoriz	zation	Headers (2) Body Pre-reque	st Script Tests		Cookies Co
Ke	y		Value	Description	••• Bulk Edit Presets
Au	uthorization		AAEAAAD/////AQAAAAAAAAAAMAgAAAFhDeWJlckFy	Session Authorizatio	n Token
Co	ontent-Type		application/json		
Ne					
Body	Cookies Raw	5) Headers (17) Test Result	ts	Status: 200 OK	Time: 168 ms Size: 6.09 k
1 • 2 • 3 • 4 • 5 6 7 8 9 10 11	( "memb	"Permissions": { "Add": true, "Add": true, "AddRenameFolder": true, "BackupSafe": true, "DeleteFolder": true, "DeleteFolder": true, "ListContent": true, "ManageSafe": true,			

### **Declaring Environment Variables**

Declaring environment variables will enable us to call a variable as opposed to manually typing them in

#### Step 1: Navigating to the Environment Manager

Select the gear icon on the top right hand side of the page and choose manage environments. While it is possible to create specific environments, we are just going to add to global variables for our purposes.

	New Tab	-			No Environment	V 💿
Collections	GET 🗸	Enter request URL			Params Se	Manage Environments Shared Environments
[v9.10+]	Authorization	Headers Body Pre	e-request Script Tests			Cookies Code
0+] [v9.8+] Is [v9.0+]	TYPE Inherit auth from The authorization automatically gen the request. Learn authorization	header will be herated when you send	This request is not inheri	ting any authorization helper at the parent's authorization h		ollection to use the
INNAGE ENVIRONMENTS anage Environments Environments are a group of variables ollections.	nt Templates & values, that allow yo	u to quickly switch the conte	X for your requests and			
earn more about environments						
You can declare a variable in an enviro name within curly-braces. <mark>Create an er</mark>			equest by putting the variable			
		Globals	Import Add			

#### Step 2: Declaring the Variables

Declare desired variables and save your changes. You should notice the color change from red to orange if you have done this properly.

