CyberArk Integration Guide (RADIUS)

Introduction

Use this guide to enable multi-factor authentication access via RADIUS to CyberArk Password Vault Server.

Prerequisites

1. Have CyberArk Password Vault Server

2. Configure and test CyberArk Password Vault Server with the PVWA

3. Create, sign, and install a certificate for the Vault Server

> It is not recommended to use a self-signed certificate for RADIUS authentication.

1. From the **C:\Program Files (x86)\PrivateArk\Server** location, run via command line the **CACert utility** with the request parameter.

   Example for Syntax: CACERT request /reqoutfile C:\Requests\VaultCert.req /country “US” /locality “Boston” /org “My Company” /orgunit “Management” /commonname “MyVault.MyCompany.com” /subjalt “IP:1.1.1.250”

   Note: The **commonname** parameter must specify the Vault’s DNS.

2. Retrieve the request file (.req) and sign it with the Certificate Authority.

3. Download the certificate file (.cer) and place it on the Vault Server.

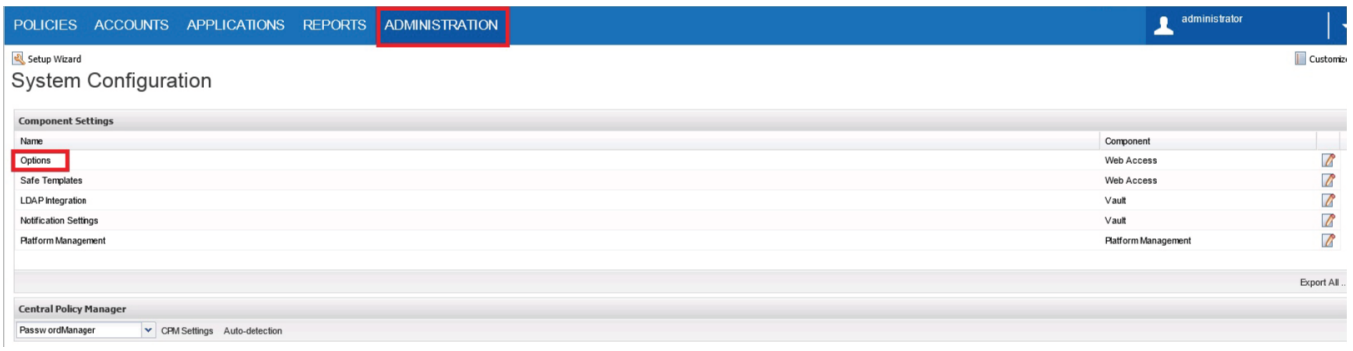
4. From **C:\Program Files (x86)\PrivateArk\Server** location, run via command line the **CACert utility** with the install parameter.

   Example for Syntax: CACERT install /CertFileName C:\certificates\certfile.cer (this is the location chosen during step 3)

4. Configure the Multi-Factor App Enrollment Realm (SecureAuth998) in the SecureAuth IdP Web Admin for the RADIUS OTP authentication requests

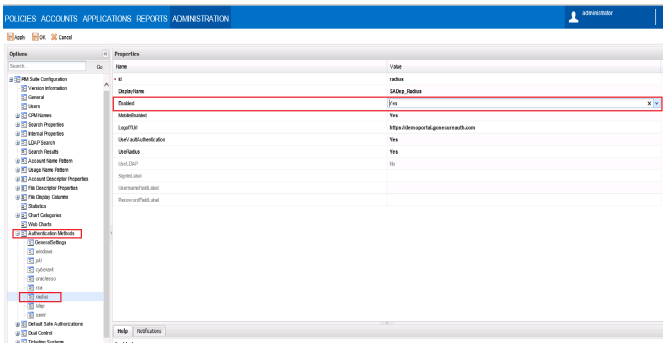
5. Install and configure the SecureAuth RADIUS Server

CyberArk Configuration Steps



1. Log into the CyberArk Password Vault Web Access, and select **Options** under **Administration**.

RADIUS



2. Select **RADIUS** under **Authentication Methods**.

3. Select **Yes** from the **Enabled** options to enable RADIUS.

4. Click **Apply**.

RADIUS Settings

5. To configure the RADIUS settings, stop the Password Vault Server.

6. Generate the RADIUS shared secret file by opening the CMD as an administrator and running **CAVaultManager** to create an encrypted RADIUS shared secret file.

Run this command: **CAVaultManager SecureSecretFiles /SecretType Radius /Secret VaultSecret / SecuredFileName c:\RadiusSecret.dat**

This is a sample of generating a shared secret file with test123 as the shared secret: **C:\Program Files (x86)\PrivateArk\Server>CAVaultManager.exe SecureSecretFiles /SecretType Radius /Secret test123 /SecuredFileName C:\test.dat**

Note that the **RADIUS Secret** has a 14 character limit.

Ensure that the shared secret used for the CyberArk Configuration is the same as in the SecureAuth RADIUS Server settings.

7. Locate the Password Vault Server **DBParm.ini** file at **C:\Program Files (x86)\PrivateArk\Server**, and back up the file.

8. Open the **DBParm.ini** file, and add the RadiusServerInfo key under the [MAIN] section:

CyberArk DBParm.ini Configuration Values

```
RadiusServersInfo=RADIUS_Server_IP;RADIUS_Port;vaulthostname;radiusauth.dat
where;
RADIUS_Server_IP = The IP of the RADIUS server
RADIUS_Port = Port number of the RADIUS
vaulthostname = The name of the RADIUS client
radiusauth.dat = The shared secret file, created in the previous section

Example: RadiusServersInfo=192.168.16.32;1812;SADept;BGRadius.dat
```

Replace the **RadiusServersInfo**, **RADIUS_Server_IP**, **RADIUS_Port**, **vaulthostname**, and **radiusauth.dat** placeholder values with the actual values.

It is critical that the **vaulthostname** value is the exact same as seen in the RADIUS Client. For example, if the hostname is all lower case, then the RADIUS Client must identically reflect that.

Ensure that there is an additional RADIUS Server for authentication (set up an additional RADIUS Server following step 8).

Example of two RADIUS Servers: RadiusServersInfo=192.168.16.32;1812;SADept;BGRadius.dat,10.50.50.10;1812;SADept;BGRadius.dat

9. Save the **DBParm.ini** file.

10. Start the Password Vault Server.

Troubleshooting / Common Issues

1. The RADIUS Configuration can be problematic if the following are not verified:

- Authorization of the Vault Servers as RADIUS Clients
- Capture of the accurate name of the RADIUS Clients entered
- Capture of the accurate RADIUS Secret

2. Network and firewall rules should be made to enable the RADIUS Ports from the Vaults to the RADIUS Servers.

3. When authenticating to the PrivateArk Client with RADIUS Authentication, users fail due to an untrusted certificate.

Refer to the Create, Sign, and Install the Certificate section in the **Prerequisites**.

4. The RADIUS Secret fails if it contains **^** (caret symbol).