RSA SECURID® ACCESS
Implementation Guide

CyberArk Password Vault Web Access

Peter Waranowski, RSA Partner Engineering
Last Modified: February 22nd, 2018
Solution Summary

CyberArk Password Vault Web Access can integrate with RSA Cloud Authentication Service using SAML and/or RADIUS. When integrated, CyberArk Password Vault Web Access can challenge users with policy-driven multifactor authentication.

CyberArk Password Vault Web Access can integrate with RSA Authentication Manager using RADIUS. When integrated, CyberArk Password Vault Web Access can challenge users with RSA SecurID.

### RSA SecurID Access Features

<table>
<thead>
<tr>
<th>CyberArk Password Vault Web Access</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On Premise Methods</strong></td>
<td></td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>✔</td>
</tr>
<tr>
<td>On Demand Authentication</td>
<td>✔</td>
</tr>
<tr>
<td>Risk-Based Authentication (AM)</td>
<td>-</td>
</tr>
<tr>
<td><strong>Cloud Authentication Service Methods</strong></td>
<td></td>
</tr>
<tr>
<td>Authenticate App</td>
<td>✔</td>
</tr>
<tr>
<td>FIDO Token</td>
<td>✔</td>
</tr>
<tr>
<td><strong>SSO</strong></td>
<td></td>
</tr>
<tr>
<td>SAML SSO</td>
<td>✔</td>
</tr>
<tr>
<td>HFED SSO</td>
<td>-</td>
</tr>
</tbody>
</table>

### Identity Assurance

| Collect Device Assurance and User Behavior | ✔ |

- 2 -
**Supported Authentication Methods by Integration Point**

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

**CyberArk Password Vault Web Access integration with RSA Cloud Authentication Service**

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>REST</th>
<th>IDR SAML</th>
<th>Cloud SAML</th>
<th>HFED</th>
<th>RADIUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurID</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Authenticate Approve</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Authenticate Tokencode</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Device Biometrics</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>SMS Tokencode</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Voice Tokencode</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>FIDO Token</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CyberArk Password Vault Web Access integration with RSA Authentication Manager**

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>REST</th>
<th>RADIUS</th>
<th>UDP Agent</th>
<th>TCP Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurID</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>AM RBA</td>
<td>-</td>
<td></td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

- Supported
- Not supported
n/t Not yet tested or documented, but may be possible
Configuration Summary

All of the supported use cases of RSA SecurID Access with CyberArk Password Vault Web Access require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

**RSA Cloud Authentication Service** – CyberArk Password Vault Web Access can be integrated with RSA Cloud Authentication Service in the following ways:

SAML via RSA Identity Router (IdP)

- [Cloud Authentication Service -- Identity Router IdP Configuration](#)
- [CyberArk Password Vault Web Access SAML Configuration](#)

SAML via RSA Cloud (IdP)

- [Cloud Authentication Service -- Cloud IdP Configuration](#)
- [CyberArk Password Vault Web Access SAML Configuration](#)

RADIUS Client

- [Cloud Authentication Service RADIUS Configuration](#)
- [CyberArk Password Vault Web Access RADIUS Configuration](#)

**RSA Authentication Manager** – CyberArk Password Vault Web Access can be integrated with RSA Authentication Manager in the following way(s):

RADIUS Client

- [Authentication Manager RADIUS Configuration](#)
- [CyberArk Password Vault Web Access RADIUS Configuration](#)
RSA SecurID Access Configuration

**RSA Cloud Authentication Service Configuration**

**SAML via RSA Identity Router (IdP)**

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for CyberArk Password Vault Web Access in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for CyberArk Password Vault Web Access and click **+Add** to add the connector.

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.

   **Note:** At the time of this testing only IDP work flow is supported. Contact CyberArk for SP login support.

3. Select the **IDP-initiated** radio button in the Initiate SAML Workflow section.
4. Scroll down to SAML Identity Provider (Issuer) section.

SAML Identity Provider (Issuer)

- Identity Provider URL: https://pe108.prod0.pe-lab.com/idPSServlet?Idp_id=PVault

- Issuer Entry ID:
  - Default (idp.Id): PVault
  - Override

SAML Response Signature

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

- Private Key Loaded
- Certificate Loaded
  - CN:ids.local, Valid Until: 12/10/2019

- Include Certificate in Outgoing Assertion

- Take note of the Identity Provider URL, this will be needed to configure the PVWA.
- Select **Choose File** and upload the RSA SecurID Access private key.
- Select the second **Choose File** and upload the RSA SecurID Access public certificate.
5. Scroll to the Service Provider section and enter the PVWA IP address or DNS in place of `<PVWA_IP>` in the Assertion Consumer Service (ACS) URL field.

   **Note:** Your environment may be configured for http; if so change the ACS URL from https to http.

   ![Service Provider section](image)

   **Assertion Consumer Service (ACS) URL**: https://<PVWA_IP>/PasswordVault/auth/saml/

   **Audience (Service Provider Entity ID)**: PasswordVault

6. Scroll to the User Identity section, select **unspecified** from the Identifier Type dropdown list, select the name of your user identity source and select the property value as **sAMAccountName**.

   ![User Identity section](image)

   **Identifier Type**: unspecified

   **Identity Source**: DefaultIdentitySourceGroup

   **Property**: sAMAccountName

7. Select **Show Advanced Configuration**.

8. Scroll down to the Uncommon Formatting SAML Response Options section.

9. Under Sign Outgoing Assertion, select **Assertion within Response**.

   ![Uncommon Formatting SAML Response Options](image)
10. Click the **Next Step** button.
11. On the User Access page, select **Allow All Authenticated Users** radio button.

![Allow All Authenticated Users](image)

12. Click the **Next Step** button.
13. Select the **Display in Portal** checkbox on the **Portal Display** page.
14. Click the **Save and Finish** button.
15. Click the **Publish Changes** button in the top left corner of the page.

![Publish Changes](image)

Refer to the **CyberArk Password Vault Web Access SAML Configuration** section for instructions on how to configure the service provider for SAML SSO.

**SAML via RSA Cloud (IdP)**

To configure a SAML Service Provider in RSA Cloud IdP, you must add a Service Provider for in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

1. Logon to the RSA SecurID Access console and browse to **Authentication Clients > Service Providers**. Click to **Add a Service Provider**.

![Add a Service Provider](image)

2. Click the Add a Service Provider button on the Service Providers page.
3. Enter a name for the Service Provider in the **Name** field on the **Basic Information** page.
4. Click the **Next Step** button.
5. On the Authentication page select RSA SecurID Access manages all authentication.

   **Note:** RSA SecurID Access Cloud IdP does not support the "Service provider manages primary authentication..." setting with CyberArk PasswordVault Web Access.

6. Select your access policy from the **Access Policy for Additional Authentication** drop-down menu and click **Next Step**.

![Authentication](image)

7. Enter the **Assertion Consumer Service (ACS) URL** and Service Provider Entity ID (Audience) and scroll down.

   **Note:** The "http(s)//<hostname>" portion of the ACS URL must match the actual URL CyberArk users use to logon to PasswordVault Web Access.

**Service Provider Metadata**

- **Assertion Consumer Service (ACS) URL**
  - http://<hostname>/PasswordVault/auth/saml

- **Service Provider Entity ID (Audience)**
  - PasswordVault

8. Click **Save and Finish**.
9. In the Message Protection section, select **Choose File** and add the SP signing certificate if required.

10. Select the **Download Certificate** and provide the IdP certificate to the service provider.

11. Click **Save and Finish**.

12. Select the Edit pulldown list and choose **View or Download IdP Metadata**.

13. Make a note of the entityID and click Cancel to close the window. This is the same value as the IdP's SSO Sign-In URL.

Refer to the [CyberArk Password Vault Web Access SAML Configuration](#) section for instructions on how to configure the service provider for SAML SSO.
RADIUS

To configure RADIUS for Cloud Authentication Service for use with a RADIUS client, you must first configure a RADIUS client in the RSA SecurID Access Console.

Logon to the RSA SecurID Access console and browse to Authentication Clients > RADIUS > Add RADIUS Client and enter the Name, IP Address and Shared Secret. Click Publish to push your configuration change to the RADIUS server.

RSA Cloud Authentication RADIUS server listens on port UDP 1812.

RSA Authentication Manager Configuration

RADIUS

To configure your RSA Authentication Manager for use with a RADIUS Agent, you must configure a RADIUS client and a corresponding agent host record in the Authentication Manager Security Console.

The relationship of agent host record to RADIUS client in the Authentication Manager can 1 to 1, 1 to many or 1 to all (global).

RSA Authentication Manager RADIUS server listens on ports UDP 1645 and UDP 1812.
Partner Product Configuration

Before You Begin

This section provides instructions for configuring CyberArk Password Vault Web Access with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All CyberArk Password Vault Web Access components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

CyberArk Password Vault Web Access SAML Configuration

Complete the steps in this section to integrate with RSA SecurID Access using SAML authentication protocol.

Configure Password Vault Web Access Web server

1. In the PasswordVault folder, `inetpub > wwwroot > PasswordVault` open the `web.config` file.
2. In the `appSettings` section, add the following parameters:
   - `IdentityProviderLoginURL` – The Identity Provider URL
   - `IdentityProviderCertificate` – The RSA SecurID Access public certificate
   - `Issuer` – The IDP Entity ID

   ```xml
   <system.webServer>
   <appSettings>
   <add key="VaultFile" value="C:\CyberArk\Password Vault Web Access\VaultInfo\Vault.ini" />
   <add key="GWFFile" value="C:\CyberArk\Password Vault Web Access\CredFiles\gwuser.ini" />
   <add key="HomePage" value="default.aspx" />
   <add key="CustomerLogoURL" value="../images/header_cobrand.gif" />
   <add key="ConfigurationCredentialFile" value="C:\CyberArk\Password Vault Web Access\CredFiles\appuser.ini" />
   <add key="ConfigurationSafeName" value="PWWACconfig" />
   <add key="LogFile" value="c:\windows\temp\PWWA.log" />
   <add key="ValidValues:" value="" />
   <add key="ApplicationID" value="" />
   <add key="MultilingualSupport" value="No" />
   <add key="InternalUsersPasswordChangeInterval" value="3600" />
   <add key="MobileVersionEnabled" value="yes" />
   <add key="FullVersionEnabled" value="yes" />
   <add key="RSADecodeUserName" value="yes" />
   <add key="IdentityProviderLoginURL" value="https://pe100.prod0.pe-la.com/IdPServlet?idp_id=PVault" />
   <add key="IdentityProviderCertificate" value="MIICpDCCAYygAwIBAgIGAvGMiczT1MhETAPBgNVBAMTCGdsLmxvY2FyMDk=
   <add key="Issuer" value="PVault" />
   </appSettings>
   </configuration>
   ```
3. Run `iisreset`. 

- 12 -
Configure Access through PVWA

1. Log onto the PVWA as an Administrator.
2. Click **ADMINISTRATION** to display the System Configuration page.
3. Click **Options**.

4. Expand Authentication methods, select **saml** and verify **Enabled** property is set to **Yes**.
5. Clear the LogoffURL field.

6. Click **Save**.
7. In the Options page, right click **Access Restriction**, then select **Add AllowedReferrer**.
8. In the Allowed Referrer property, in **BaseUrl**, specify the IDP SSO URL.
9. Click **Apply**.
10. Sign out.

<table>
<thead>
<tr>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>BaseUrl</td>
</tr>
<tr>
<td>RegularExpression</td>
</tr>
</tbody>
</table>

CyberArk Password Vault Web Access is now integrate with RSA SecurID Access using SAML.

**CyberArk Password Vault Web Access RADIUS Client Configuration**

**Configure RADIUS connection settings on Password Vault server**

1. Log on to the desktop of the Password Vault server.
2. Open the command prompt and enter the following command:
   ```
   "C:\Program Files (x86)\PrivateArk\Server\CAVaultManager.exe" SecureSecretFiles /SecretType Radius /Secret myradiussecret /SecuredFileName "C:\Program Files (x86)\PrivateArk\Server\myradiussecret.dat"
   ```
3. Open the **DBParm.ini** file and add the following parameters on a single line, separated by semicolons.
   ```
   RadiusServersInfo
   RADIUS Server IP address
   RADIUS Server Authentication Port
   RADIUS Client Name (Vault machine as entered in the RADIUS server)
   Path to SecuredFileName
   ```
   Example:
   ```
   RadiusServersInfo=1.1.1.250;1812;vaulthostname;myradiussecret.dat
   ```
4. (optional) Extend the **DefaultTimeout** value to 60 seconds. This will allow more time for users to complete out of band authentication challenges.
5. Restart the Password Vault server.

**Configure a RADIUS user on Password Vault server**

1. Logon to the vault as an administrative user.
2. Browse to **Tools > Administrative Tools > Users and Groups** and **Add** or **Update** an account to use with RADIUS authentication.
3. Open the **Authentication** tab of the user profile, select **RADIUS Authentication** from the Authentication method drop-down menu and click **OK**.
Configure Access through PVWA

1. Log onto the PVWA as an Administrator.
2. Click **ADMINISTRATION** to display the System Configuration page.
3. Click **Options**.

4. Open the **Authentication Methods** menu and click **radius**.

---

![Image of System Configuration page](image)

![Image of Options page](image)
5. Configure the RADIUS properties and click **OK**.

- **DisplayName** – Enter the value the display name for this authentication method.
- **Enabled** – Set to Yes
- **UseVaultAuthentication** – Set to Yes
- **UseRadius** – Set to Yes
Login Screenshots

Login screen

SIGN IN
Specify your authentication details

<table>
<thead>
<tr>
<th>User name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

Sign in

User-defined New PIN

RADIUS CHALLENGE
ITATS542I Enter a new PIN having from 4 to 8 alphanumeric characters:

<table>
<thead>
<tr>
<th>p_waranowski</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
</tr>
</tbody>
</table>

Post Answer
System-generated New PIN

RADIUS CHALLENGE
ITATS542I Are you satisfied with system generated PIN 77ceOqh? (y/n):

<table>
<thead>
<tr>
<th>p_waranowski</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
</tr>
</tbody>
</table>

Post Answer

Next Tokencode

RADIUS CHALLENGE
ITATS542I Wait for token to change, then enter the new tokencode:

<table>
<thead>
<tr>
<th>p_waranowski</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
</tr>
</tbody>
</table>

Post Answer
RADIUS CHALLENGE

ITATS542! Enter your token code or select another method: 1 for Approve, 2 for Biometrics, 3 for Eyeprint ID, 4 for SMS

Token code

peter

Response

Post Answer
# Certification Checklist for RSA SecurID Access

## Certification Environment Details:
RSA Authentication Manager 8.2 SP1, Virtual Appliance  
CyberArk Enterprise Password Vault v9.9.5  
CyberArk Password Vault Web Access v9.9.5

### RSA Cloud Authentication Service  
Date Tested: February 22, 2018

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>REST Client</th>
<th>RADIUS Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurID</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Authenticate Approve</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Authenticate Tokencode</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Device Biometrics</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>SMS Tokencode</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Voice Tokencode</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>FIDO Token</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

### RSA Authentication Manager  
Date Tested: February 21, 2018

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>REST Client</th>
<th>UDP Agent</th>
<th>TCP Agent</th>
<th>RADIUS Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurID</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>RSA SecurID Software Token Automation</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>On Demand Authentication</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Risk-Based Authentication</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

✔ = Passed, ✗ = Failed, - = N/A