

BigID Cloud remote authentication

Updated on 09 Jun 2022 • 4 Minutes to read • Contributors 

In Short

BigID provides a method for storing credentials to your data sources so that they're managed within the BigID environment. You can also connect to credential management tools, such as CyberArk and HashiCorp.

This document describes how to connect to CyberArk and HashiCorp for your BigID Cloud environment.

This document will be useful for Admins.

See More: [Credentials](#), [BigID Cloud FAQs](#), [BigID Managed Services FAQ](#), [Cloud-Supported Applications](#), [BigID Cloud Upgrades](#)

Credentials allow you to manage users and passwords for connecting BigID to data sources. Create a connection from your data source to an external authentication management system, such as CyberArk or Hashicorp.

For more information about setting up Credentials in BigID, see [Credentials](#).

See below for connecting BigID Cloud to:

- [CyberArk](#)

CyberArk for BigID Cloud

Create a credential that uses your on-prem CyberArk to authenticate your BigID Cloud connection to any data source that authenticates using usernames and passwords.

1. Set up BigID Cloud in CyberArk

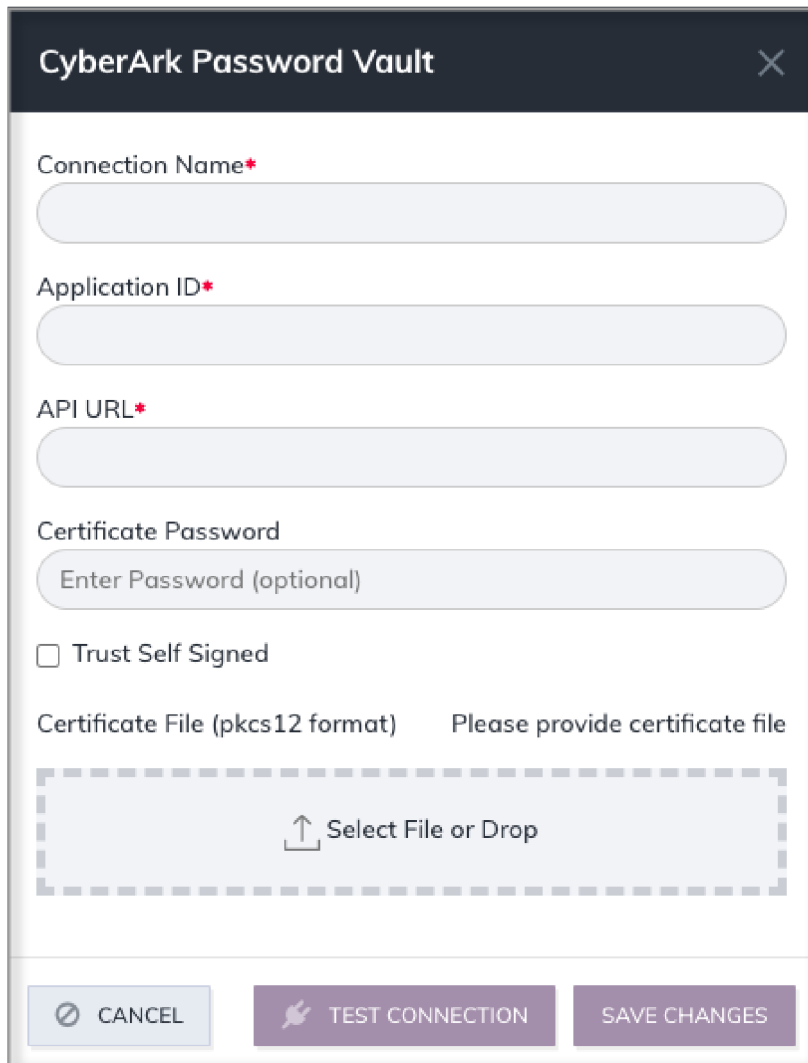
Create objects inside your CyberArk safe containing the connection details needed to access your data sources. In each object, define the username in

the UserName field and password in the Content field.

Create an Application ID/Account in CyberArk for BigID Cloud with permissions to access the required objects.

2. Connect to CyberArk in BigID Cloud

In BigID Cloud, click **Applications Management** > **CyberArk Configuration** > **Open** to display the CyberArk configuration dialog.



The image shows a configuration dialog titled "CyberArk Password Vault" with a close button (X) in the top right corner. The dialog contains several input fields and a checkbox:

- Connection Name***: A text input field.
- Application ID***: A text input field.
- API URL***: A text input field.
- Certificate Password**: A text input field with the placeholder text "Enter Password (optional)".
- ☐ **Trust Self Signed**: A checkbox.
- Certificate File (pkcs12 format)**: A label followed by the text "Please provide certificate file". Below this is a dashed rectangular box containing an upward arrow icon and the text "Select File or Drop".

At the bottom of the dialog, there are three buttons: "CANCEL" (with a close icon), "TEST CONNECTION" (with a lightning bolt icon), and "SAVE CHANGES".

Element	Description
Connection Name	A free text descriptive name for the BigID Cloud / CyberArk connection.
Application ID	A free text Application ID or Account configured for BigID Cloud in CyberArk.
API URL	The URL of your CyberArk server. Format: https://ip:port
Certificate Password	The password of your Password Vault.
Trust Self Signed	Select this checkbox to allow self-signed certificates.
Certificate File	Select or drag and drop the CyberArk Password Vault pkcs certificate file defined for the Application ID. To use CyberArk certificates that already exist on the CyberArk PVWA server: 1. Log in to the CyberArk PVWA server. 2. Open Windows Certificate manager. 3. Export the CyberArk certificate from the Personal folder. Select the certificate that has been signed by the CA root certificate. Include the private key in the export and save the certificate in the p12/pfx format. 4. Upload the p12/pfx file using the BigID UI. Note that only one file can be uploaded at a time.
Test Connection	Click to test that BigID Cloud successfully connects to CyberArk. This test validates that BigID Cloud successfully connects to its Application ID in CyberArk, as follows: • Connect to Password Vault using certificate and password. • Connect to Application ID via CyberArk API.

Click **SAVE CHANGES** to save your CyberArk configuration in BigID Cloud.

Error "Unable to verify the first certificate" when testing the connection.

If you get this error, check that SSL is enabled for the AIMWebService:

1. Open **IIS Manager** on the CyberArk PVWA server.
2. Navigate to **Default Web Site > AIMWebService**.
3. Explicitly enable SSL (set to required).

These changes are implemented dynamically; there's no need to reboot the Windows server.

3. Enable Remote CyberArk credentials type

1. In the left navigation bar, click **Advanced Tools**, and select **Services Configuration**.

2. In the Variable Name field, enter

`SHOW_REMOTE_CYBERARK_CREDENTIALS_TYPE` .

3. Set the value of `SHOW_REMOTE_CYBERARK_CREDENTIALS_TYPE` to true.

A notification appears instructing you to log out for the change to take effect.

4. Re-login

Log out of BigID Cloud, and then log back in.

5. Create CyberArk Credentials in BigID Cloud

Set up credentials for your data sources.

1. In the left navigation bar, navigate to **Administration > Credentials**, and click **Add New Credential**.
2. Enter a descriptive name in **BigID Credential ID** and select credential type **RemoteCyberArk**. Available fields display accordingly.
3. Enter the CyberArk query that connects to the specific object, and click **Save**.

Example of a CyberArk query:

`Safe=Test;Folder=root;Object=Postgres` , which specifies the object called "Postgres" inside a folder called "root" inside a safe called "Test".

4. Enter the Scanner Group that includes a scanner that can reach the CyberArk vault. The scanner group can be a different group than the data source configured with the credentials.
5. Enter the **Scopes** for this data source.

6. Configure the BigID Cloud data source connection

1. In BigID Cloud, **create a new data source connection** or **edit an existing one**.
2. Enable **Use Credential** and select the appropriate CyberArk credential.