

Automatic rotation of DPA strong accounts

If you have Self-Hosted Vault in your environment, the recommended way to protect your DPA strong accounts is to store your strong accounts in your Self-Hosted Vault and onboard the strong accounts in DPA. With this setup, strong accounts are protected in the Vault and managed by CPM.

High-level overview

The following is a high-level description of the solution steps:

1. Create your strong account in DPA and onboard it to the Vault using the DPA Strong Account platform.
2. While CPM rotates the account in the Self-Hosted Vault, the strong account saved in DPA must also be rotated. Therefore, CPM uses a new platform (**DPA Strong Account**) triggered on each CPM rotation and calls APIs to also rotate the relevant strong account saved in DPA.
3. To call those APIs, a user is needed to be able to authenticate to DPA and you must create a user for that purpose. Each platform that manages one or more strong accounts must be linked to the **DPA Strong Account** platform.

Implement the solution

To implement the solution, do the following steps in order:

Step 1: Create a user to call DPA APIs

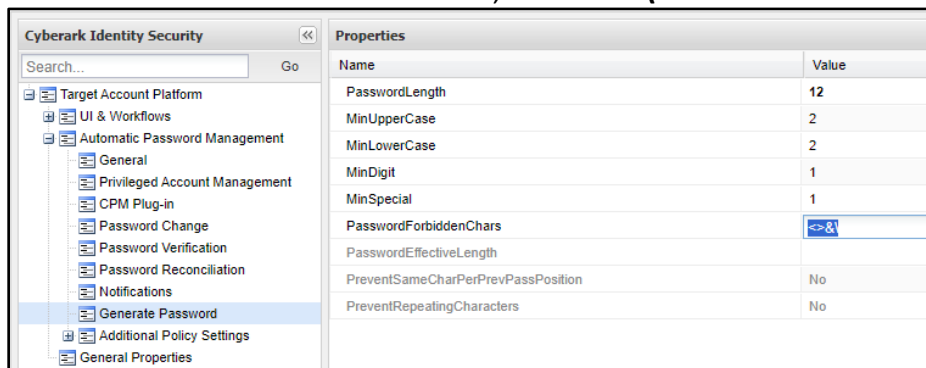
Note: Do this step only once for each tenant.

1. In Identity Administration, [create a new CyberArk Cloud Directory user](#).
 - a) The user must be defined with a password only and no MFA.
 - b) Make sure the option **Require password change at next login (recommended)** is not selected.
 - c) [Add the user](#) as a member to the DPAAdmin role.
2. From the CyberArk Marketplace, download the [CyberArk CPM Identity Administration](#) platform and [import](#) it into PVWA.
3. In PVWA, click **ADMINISTRATION** to display the System Configuration page, then

Automatic rotation of DPA strong accounts

click **Platform Management** to display a list of supported target account platforms.

4. Select the **CyberArk Identity Security** platform, and then click **Edit**. The configuration page for the selected platform appears.
5. Expand **Automatic Password Management**, then select **Generate Password**.
6. In the **PasswordForbiddenChars** field, enter **<>&**



Name	Value
PasswordLength	12
MinUpperCase	2
MinLowerCase	2
MinDigit	1
MinSpecial	1
PasswordForbiddenChars	<>&\
PasswordEffectiveLength	
PreventSameCharPerPrevPassPosition	No
PreventRepeatingCharacters	No

7. Click **OK** to save.
8. Create an account for the CyberArk Cloud Directory in the Vault.
 - a) Click **Add account**.
 - b) For **System type**, select **Application**.
 - c) For **Platform**, select **CyberArk Identity Security**.
 - d) Select the relevant Safe. This should be the Safe that is managed by CPM and has access to **https://<subdomain>.cyberark.cloud**.
 - e) Enter the following properties, duplicating those of the user created in paragraph 1 a) above (in Identity Administration):

Username

Address, in the following format: **<subdomain>.cyberark.cloud**

Password

- f) Click **Add** to add the account.

Step 2: Import the new platform

Note: Do this step only once for each tenant.

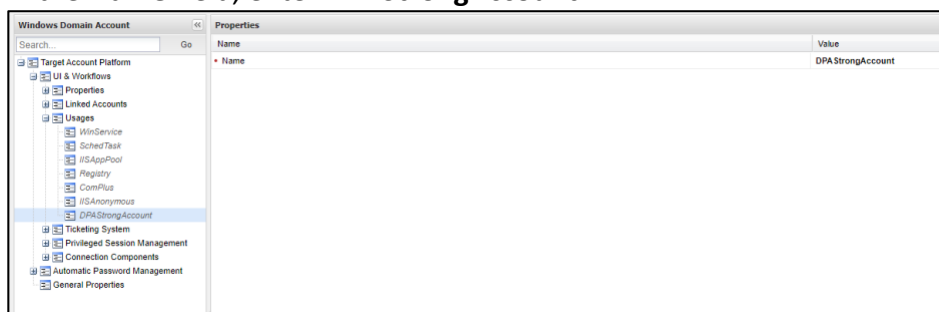
Automatic rotation of DPA strong accounts

From the CyberArk Marketplace, download the [DPA Strong Account platform](#) and [import](#) it into PVWA.

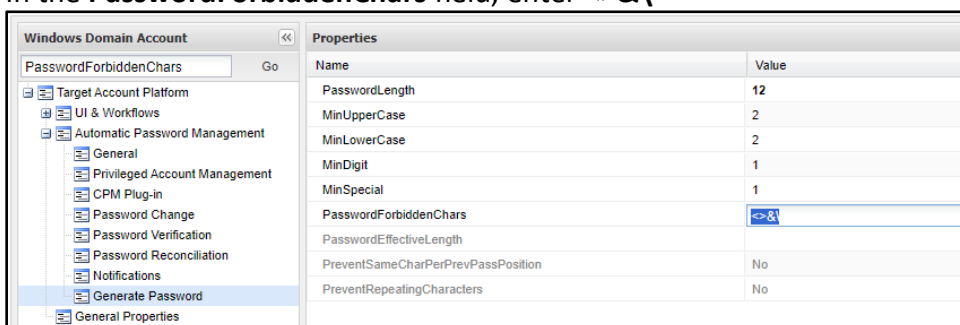
Step 3: Configure usage integration

For each platform that manages one or more strong accounts, configure usage integration with the DPA Strong Account platform.

1. In PVWA, click **ADMINISTRATION** to display the System Configuration page, then click **Platform Management** to display a list of supported target account platforms.
2. Select the relevant target account platform, and then click **Edit**. The configuration page for the selected platform appears.
3. Expand **UI & Workflow**, right-click **Usages**, then select **Add Usage**. The new usage is now created.
4. In the **Name** field, enter **DPAStrongAccount**.



5. Expand **Automatic Password Management**, then select **Generate Password**.
6. In the **PasswordForbiddenChars** field, enter **<>&**



7. Click **OK** to save.

Step 4: Create an account in the Self-Hosted Vault

Automatic rotation of DPA strong accounts

You need to create an account in the Vault related to a strong account in DPA. If the strong account doesn't already exist in DPA, you must first create it. For more information, see [Add and manage strong accounts](#).

1. In DPA, go to the **Strong accounts** page.
2. On the relevant strong account click **More options** (⋮) then **Edit account**. The account details are displayed.



3. Copy the **Account ID**.
4. In PVWA, open the **Accounts View** (classic UI).
5. Open the **Account Details** of the strong account. If the account is not yet stored in the Vault, create it now.
6. Click the **Usages** tab and select **DPA Strong Account**. (If you don't see the tab, navigate to the right with the arrow above the table.)



7. Add a new usage account with the following details:
Subdomain: the tenant's subdomain.
AccountID: paste in the account ID you copied in paragraph number 3.
8. Click **Save**.

Automatic rotation of DPA strong accounts

9. Click on the **AccountID** you just added in paragraph number 7 to display the account details.
10. On the tabs, click **Associate**.
11. Select the user you created in Step 1, then click **Associate**.

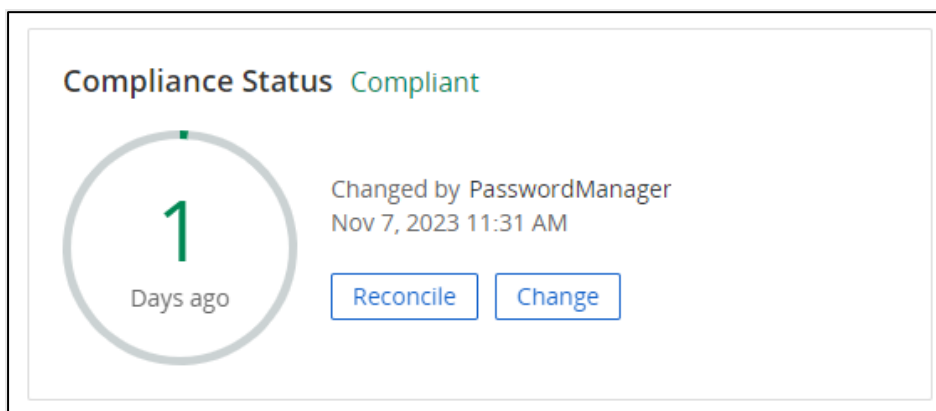
Test the setup

Once you have completed the setup, it is recommended to test it.

To test the setup:

1. Establish a DPA session to make sure the connection works before changing the strong account's password.
2. In PVWA, choose the strong account and click **Change**.

Note: The Compliance Status should record the change.



3. Establish a new DPA session.